CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
ESCOLA TÉCNICA DE CUBATÃO
Curso de Ensino Técnico em Informática

Eric Vieira dos Santos
Larissa Cavalcante dos Santos
Oswaldo Leite Santos Grillo
Ryan Ferreira da Silva

CONFORMIDADE COM A LGPD NA EMPRESA COM SEGMENTO NA ÁREA CONTÁBIL, LOCALIZADA EM SANTOS: UMA ANÁLISE DOS PROCESSOS ORGANIZACIONAIS COM FOCO NO SETOR DE RECURSOS HUMANOS

Cubatão
2026

Eric Vieira dos Santos
Larissa Cavalcante dos Santos
Oswaldo Leite Santos Grillo
Ryan Ferreira da Silva

CONFORMIDADE COM A LGPD NA EMPRESA COM SEGMENTO NA ÁREA CONTÁBIL, LOCALIZADA EM SANTOS: UMA ANÁLISE DOS PROCESSOS ORGANIZACIONAIS COM FOCO NO SETOR DE RECURSOS HUMANOS

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática da Etec de Cubatão, orientado pelo Prof. Marcelo Batista Onuki, como requisito parcial para obtenção do título de técnico em Informática.

Cubatão
2026

“Se você acha que sabe tudo sobre cibersegurança, provavelmente lhe explicaram mal o assunto.”

Stéphane Nappo.

RESUMO

O presente trabalho teve como objetivo geral analisar o nível de conformidade de uma empresa com segmento na área contábil, localizada em Santos/SP, com os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n.º 13.709/2018), com foco no setor de Recursos Humanos e nas práticas de segurança da informação adotadas pela organização. Para tanto, foram definidos como objetivos específicos identificar falhas e não conformidades nos processos de tratamento de dados pessoais, avaliar o nível de conhecimento dos colaboradores sobre a LGPD e a segurança digital por meio de instrumentos de coleta e de uma ação de capacitação, e propor intervenções que contribuíssem para a adequação das práticas organizacionais à legislação vigente. A pesquisa caracteriza-se como de finalidade aplicada e, quanto aos objetivos, como exploratória, com abordagem quali-quantitativa. Adotou-se o método indutivo, partindo da observação da realidade concreta da organização para a formulação de conclusões mais amplas sobre seu nível de conformidade, e os procedimentos técnicos de estudo de caso e levantamento bibliográfico. A coleta de dados contemplou entrevistas semiestruturadas com o sócio-administrador, também responsável pela função de Encarregado de Proteção de Dados (DPO), e com os profissionais dos setores de Recursos Humanos e Tecnologia da Informação, além da aplicação de formulário aos colaboradores, de questionário avaliativo gamificado via plataforma Kahoot e da realização de uma capacitação sobre segurança digital e LGPD nas dependências da empresa. Os resultados confirmaram, em graus distintos, as hipóteses formuladas, evidenciando um cenário de conformidade parcial: a organização apresenta boas práticas consolidadas, como maturidade na continuidade de negócios e conscientização geral dos colaboradores sobre a legislação, ao lado de lacunas relevantes, entre elas a ausência de senhas individuais em parte das estações de trabalho, o desconhecimento do canal de reporte de incidentes por mais da metade dos colaboradores e a inexistência de políticas formalizadas de segurança da informação. Como contribuição prática, foi elaborado e entregue à gestão um Plano de Intervenção estruturado em oito ações distribuídas em quatro fases ao longo de doze meses, fundamentado nos princípios da LGPD e nos requisitos da norma ABNT NBR ISO/IEC 27001:2022, cuja adoção permanece a critério da organização.

Palavras-chave: LGPD. Segurança da Informação. Proteção de Dados.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIAÇÕES E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ANPD – Autoridade Nacional de Proteção de Dados

CPF – Cadastro de Pessoa Física

DAMA-DMBOK – Data Management Body Of Knowledge

DPO - Data Protection Officer / Encarregado de Proteção de Dados

DP – Departamento Pessoal

ETEC – Escola Técnica Estadual

GDPR - General Data Protection Regulation / Regulamento Geral de Proteção de Dados da União Europeia

LGPD – Lei Geral de Proteção de Dados

LTDA - Sociedade de Responsabilidade Limitada

ISO - Organization for Standardization / Organização Internacional de Padronização

IEC – Comissão Elétrica Internacional

RH – Recursos Humanos

SI – Sistema de Informação

SGSI - Sistema de Gestão de Segurança da Informação

SIRH – Sistema de Informação de Recursos Humanos

S/S – Sociedade Simples

NBR – Norma Brasileira

TCC – Trabalho de Conclusão de Curso

TI – Tecnologia da Informação

RIPD - Relatório de Impacto à Proteção de Dados

PDCA - Planejar, Executar, Checar e Agir

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

No contexto organizacional, a adequação à Lei Geral de Proteção de Dados (LGPD) abrange todas as áreas da empresa que realizam o tratamento de dados pessoais, exigindo a adoção de políticas, controles e boas práticas voltadas à segurança da informação e à privacidade. Nesse cenário, diversos setores, como o administrativo, financeiro e de tecnologia da informação, lidam direta ou indiretamente com dados de clientes, fornecedores e colaboradores, tornando a conformidade com a legislação uma responsabilidade institucional ampla.

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709, de 14 de agosto de 2018), com vigência plena a partir de 2020 e aplicação de sanções administrativas desde agosto de 2021, representou um marco regulatório no tratamento de dados pessoais no Brasil, alinhando o país aos padrões internacionais de privacidade, como o GDPR europeu. A lei estabelece princípios, direitos dos titulares e obrigações aos agentes de tratamento, impactando diretamente todos os setores organizacionais, em especial o setor de Recursos Humanos, que lida diariamente com dados pessoais e sensíveis de colaboradores, como CPF, dados bancários, informações de saúde e biometria, entre outros.

Apesar da importância da norma, muitas empresas, sobretudo de pequeno e médio porte, ainda enfrentam dificuldades na adequação efetiva, seja pela escassez de profissionais especializados (como o Encarregado de Proteção de Dados – DPO), pela ausência de políticas internas claras ou pela falta de transparência no tratamento das informações. Tais lacunas expõem as organizações a riscos jurídicos, financeiros (multas de até R$ 50 milhões por infração) e reputacionais.

A pesquisa parte da seguinte problemática: em que medida os processos e as boas práticas adotados tanto pelo setor de Recursos Humanos quanto pela empresa estão em conformidade com os requisitos da LGPD, especialmente no que se refere ao tratamento de dados pessoais e dados sensíveis de seus colaboradores?

Nesse contexto, o presente trabalho tem como objetivo geral analisar o nível de conformidade da empresa com os requisitos da Lei Geral de Proteção de Dados Pessoais, com foco no setor de Recursos Humanos e nas práticas de segurança da informação adotadas pela organização. Para alcançá-lo, foram definidos os seguintes objetivos específicos: identificar falhas e não conformidades nos processos de tratamento de dados pessoais; avaliar o nível de conhecimento dos colaboradores sobre a LGPD e a segurança digital por meio de instrumentos de coleta e de uma ação

de capacitação; e propor intervenções concretas que contribuam para a adequação das práticas organizacionais à legislação vigente.

Como hipóteses, considera-se que: a pouca aderência dos colaboradores à cultura de segurança da informação potencializa a ocorrência de incidentes no manuseio diário de dados; a existência de fragilidades nos controles de acesso e na gestão de dados pessoais aumenta os riscos de não conformidade com a LGPD; e a ausência ou insuficiência de capacitação compromete a qualidade das práticas institucionais de proteção de dados.

A escolha do tema justifica-se pela relevância da LGPD no contexto da área de Informática, especialmente no que se refere à segurança da informação, ao controle de acesso e ao tratamento de dados pessoais em sistemas. Além disso, o estudo se mostra pertinente pela sua aplicação prática em uma empresa real, contribuindo para a identificação de falhas e para a proposição de melhorias nos processos relacionados à proteção de dados.

Para o desenvolvimento do trabalho, bem como para a validação dos objetivos e das hipóteses estabelecidas, foi adotada uma pesquisa de finalidade aplicada, visto que visa desenvolver e aplicar conhecimentos práticos voltados à adequação organizacional à Lei Geral de Proteção de Dados (LGPD). Quanto aos objetivos, classifica-se como exploratória, pois realiza uma sondagem sobre um fenômeno ainda pouco explorado no contexto da organização estudada. No que se refere à abordagem, optou-se pela quali-quantitativa, contemplando tanto a análise interpretativa das entrevistas realizadas com o sócio-administrador e com os profissionais das áreas de Recursos Humanos e Tecnologia da Informação (qualitativa), quanto o tratamento dos dados coletados por meio de formulário aplicado aos colaboradores (quantitativa). O método utilizado foi o indutivo, uma vez que a investigação partiu da observação de uma situação concreta e particular, a realidade organizacional da empresa estudada, para, a partir da análise dos dados coletados, alcançar conclusões mais amplas sobre o nível de conformidade com a LGPD. Por fim, quanto ao procedimento técnico, adotaram-se o estudo de caso, com análise aprofundada da organização em questão no tocante à sua conformidade com a LGPD, e o procedimento bibliográfico, por meio do levantamento de literatura especializada que fundamentou teoricamente a investigação. Foi também implementado um treinamento voltado à conscientização em segurança digital e ao aprofundamento do conhecimento acerca da legislação junto aos colaboradores.

O desenvolvimento da pesquisa seguiu uma sequência estruturada de etapas. Iniciou-se pelo levantamento do referencial teórico e pela requisição formal de acesso à empresa, acompanhada da coleta de documentação de apoio. Em seguida, foram realizadas as entrevistas com o sócio-administrador e com a responsável pelo setor de Recursos Humanos. Posteriormente, foi conduzida a capacitação em segurança digital e LGPD junto aos colaboradores, seguida da entrevista com o profissional de Tecnologia da Informação. O trabalho foi encerrado com a elaboração e entrega do Plano de Intervenção à gestão da empresa.

2 REFERENCIAL TEÓRICO

O referencial teórico deste trabalho está estruturado em quatro eixos temáticos que fundamentam a análise desenvolvida ao longo da pesquisa. O primeiro aborda a proteção de dados e a privacidade, com ênfase na evolução histórica do direito à privacidade e nos fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). O segundo trata do setor de Recursos Humanos, com foco em suas rotinas, subsistemas e no fluxo de informações gerado pela área. O terceiro apresenta a norma ABNT ISO/IEC 27001, discutindo os princípios de segurança da informação, a tríade CIA e a gestão de riscos no contexto organizacional. Por fim, o quarto eixo aborda a gestão e a governança de dados, explorando o dado como ativo estratégico e sua interface com as exigências da LGPD.

2.1 Introdução à Proteção de Dados e Privacidade

Para compreender o estudo de caso sobre a conformidade com a LGPD, é necessário aprofundar o conceito da Lei Geral de Proteção de Dados. Nesse contexto, destaca-se que o dado pessoal está diretamente ligado à pessoa, podendo até substitui-la em determinadas situações, ao refletir aspectos de sua identidade. Assim, conforme Danilo Doneda, os dados representam uma espécie de “corpo eletrônico”, devendo ser verídicos e protegidos, pois seu uso inadequado pode resultar em prejuízos e perda de direitos.

A proteção de dados pessoais e o direito à privacidade representam pilares fundamentais na sociedade da informação contemporânea. Conforme Doneda (2020), a privacidade não é mais apenas um “direito a ser deixado só”, mas um instrumento de autodeterminação existencial e informacional da pessoa humana. O autor destaca que, na era digital, a proteção de dados pessoais transcende o indivíduo e assume dimensão coletiva, afetando grupos sociais e a própria democracia. Já Donda (2020) enfatiza que a adequação à LGPD vai além de aspectos técnicos: exige governança, conscientização e integração de controles de segurança da informação em todos os processos empresariais.

Segundo Laura Mendes, a proteção de dados deve começar desde o início do processo, para evitar problemas que possam sair do controle. Antes de coletar qualquer informação, é importante definir claramente sua finalidade e objetivo. Isso porque os dados devem ser utilizados de forma adequada e na medida certa, buscando sempre coletar apenas o necessário para atender ao propósito proposto.

Figura 1 - Princípios da Lei

Fonte: serpro.gov.br, 2018

2.1.1 Evolução Histórica do Direito à Privacidade

O direito à privacidade possui raízes históricas profundas, mas sua configuração moderna surgiu como resposta às transformações sociais, tecnológicas e jurídicas dos séculos XIX e XX. Inicialmente associada à ideia de isolamento e proteção contra intromissões físicas, a privacidade evoluiu para uma disciplina complexa de proteção de dados pessoais, especialmente com o advento da informática e da internet.

Doneda (2020, p. 13) explica que, tradicionalmente, a tutela da privacidade destinava-se à proteção contra “intromissões indesejadas na esfera pessoal”. Todavia, o progresso tecnológico e a intensificação do fluxo de informações alteraram quantitativa e qualitativamente essa noção. O autor cita como marco clássico o artigo seminal de Warren e Brandeis (1890), intitulado The Right to Privacy, publicado na Harvard Law Review. Nesse trabalho, os juristas norte-americanos cunharam a expressão “right to be let alone” (direito de ser deixado em paz), defendendo que a privacidade não se limitava à propriedade, mas derivava da inviolabilidade da personalidade. Doneda (2020, p. 90) ressalta que o artigo foi motivado por escândalos midiáticos envolvendo a família Warren e representou uma ruptura: a privacidade

deixou de ser vista apenas como direito patrimonial para tornar-se um direito da personalidade.

Ao longo do século XX, a privacidade ganhou contornos mais amplos. Nos Estados Unidos, a jurisprudência constitucional (casos como Griswold v. Connecticut e Roe v. Wade) expandiu o conceito para incluir decisões íntimas (aborto, contracepção). Na Europa, a Convenção Europeia dos Direitos Humanos (1950, art. 8) e a Diretiva 95/46/CE (1995) consolidaram a proteção de dados como direito fundamental. Doneda (2020, p. 31) observa que, com o surgimento dos bancos de dados e da informática, surgiu a necessidade de “exorbitar os cânones tradicionais” da privacidade, dando origem à disciplina específica de proteção de dados pessoais.

No Brasil, a Constituição Federal de 1988 (art. 5º, X) garantiu a inviolabilidade da intimidade, vida privada, honra e imagem. No entanto, foi apenas com a era digital que se percebeu a insuficiência dessa proteção. Doneda (2020, p. 267) afirma que a privacidade no ordenamento brasileiro “encontra abrigo certo em várias declarações internacionais”, mas carecia de normatização específica até a LGPD. O autor destaca que a proteção de dados pessoais é “a continuação por outros meios” da privacidade tradicional, funcionalizando-se para garantir o livre desenvolvimento da personalidade em um ambiente de processamento massivo de informações.

Essa evolução é crucial para o TCC. Na empresa, o RH lida com dados que, historicamente, eram tratados de forma manual ou em planilhas sem controles. Hoje, a privacidade informacional exige mapeamento, consentimento e segurança — temas que serão analisados no estudo de caso.

2.1.2 A Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD) representa o marco regulatório brasileiro para o tratamento de dados pessoais. Promulgada em 14 de agosto de 2018, ela altera o Marco Civil da Internet (Lei nº 12.965/2014) e inspira-se diretamente no Regulamento Geral de Proteção de Dados (GDPR) europeu. Donda (2020, p. 10) explica que a LGPD entrou em vigor em 3 de maio de 2021 (após sucessivas prorrogações devido à pandemia de Covid-19), com sanções administrativas previstas para agosto de 2021. A lei já produzia efeitos desde dezembro de 2018 em relação à criação da Autoridade Nacional de Proteção de Dados (ANPD).

A LGPD aplica-se a qualquer operação realizada com dados pessoais, seja por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio (digital ou manual). Donda (2020, p. 16) destaca que a lei possui alcance extraterritorial: aplica-se quando os dados são tratados no Brasil ou coletados em território nacional, mesmo que a empresa esteja sediada no exterior.

Os conceitos centrais definidos no artigo 5º da Lei Geral de Proteção de Dados (LGPD) incluem o dado pessoal, entendido como qualquer informação relacionada a uma pessoa natural identificada ou identificável, e o dado pessoal sensível, que abrange informações como origem racial ou étnica, convicção religiosa, opinião política, dados genéticos, biométricos e aspectos relacionados à saúde ou à vida sexual. Além disso, o tratamento de dados refere-se a toda e qualquer operação realizada com dados pessoais, como coleta, uso, armazenamento, compartilhamento e eliminação.

Donda (2020, p. 12) ressalta que a LGPD é dividida em dez capítulos, com ênfase nos princípios (art. 6º): finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização

Doneda (2020) complementa que a LGPD não é apenas uma lei de “segurança da informação”, mas uma ferramenta de tutela da pessoa humana. O autor (2020, p. 316) afirma que a proteção de dados pessoais assume “caráter de direito fundamental”, harmonizando privacidade com desenvolvimento econômico. No contexto do TCC, a empresa deve implementar um comitê LGPD, mapear dados de RH, elaborar Política de Privacidade e realizar Relatório de Impacto à Proteção de Dados (RIPD) — temas que serão aprofundados no estudo de caso.

A LGPD não se aplica a dados tratados para fins exclusivamente jornalísticos, artísticos, de segurança pública ou por pessoa natural para uso privado (art. 4º). No entanto, no RH empresarial, praticamente todos os processos caem no âmbito da lei, exigindo adequação imediata para evitar multas de até 2% do faturamento (limitado a R$ 50 milhões por infração).

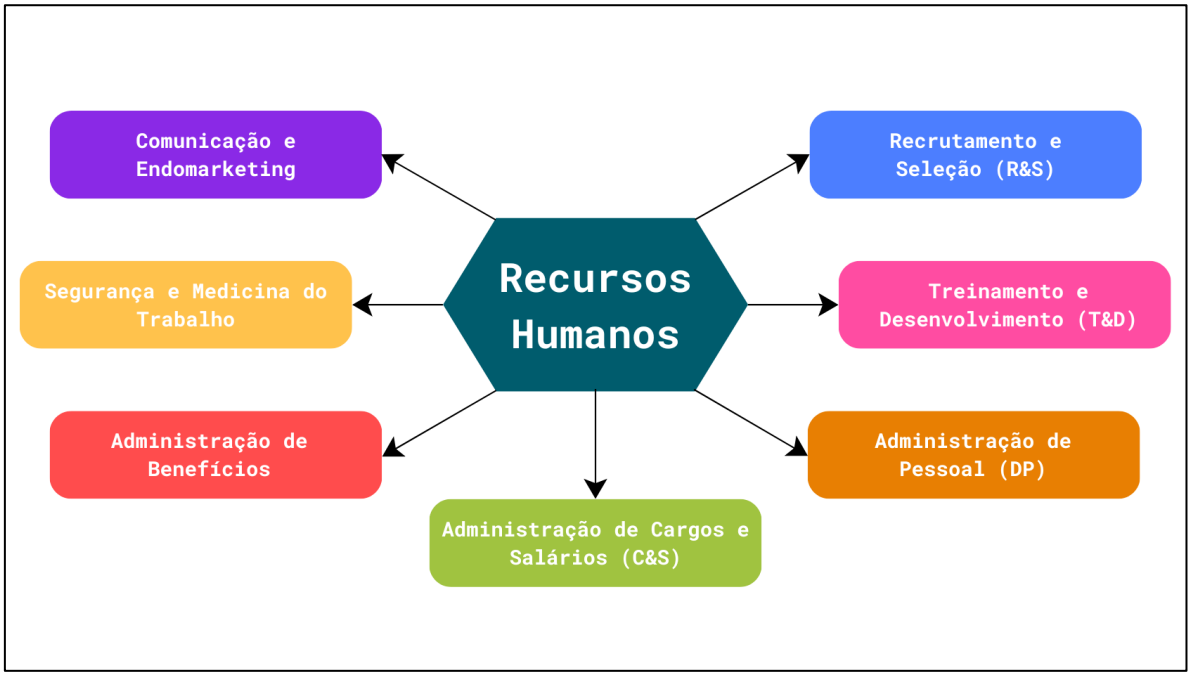
2.2 O Departamento de Recursos Humanos

O departamento de Recursos Humanos, em uma visão mais tradicional, é o setor responsável pelo gerenciamento do capital humano dentro de uma organização, sendo responsável por atividades relacionadas às pessoas na empresa, que vão desde aspectos de cultura organizacional até rotinas administrativas e trabalhistas, como folha de pagamento, gestão de benefícios e cumprimento da legislação trabalhista (CHIAVENATO, 2014).

O setor de Recursos Humanos, também denominado Gestão de Pessoas, é considerado estratégico dentro das organizações, pois está diretamente relacionado à missão, visão e aos objetivos organizacionais. Nesse contexto, o cumprimento das metas depende diretamente da atuação dos colaboradores, uma vez que são eles que executam as atividades necessárias para o funcionamento e desenvolvimento da organização. Dessa forma, as organizações não poderiam existir sem a participação ativa das pessoas, que contribuem para o alcance dos objetivos institucionais (CHIAVENATO, 2022).

A Figura abaixo demonstra os subsistemas estratégicos presentes no setor de Recursos Humanos. Esses subsistemas representam as principais áreas de atuação da gestão de pessoas dentro das organizações, sendo divididos em sete segmentos, cada um com funções específicas que contribuem para o gerenciamento do capital humano. Dessa forma, cada subsistema possui um papel distinto e relevante para o funcionamento e desenvolvimento da gestão de pessoas na organização.

Figura 2 - Subsistemas do RH



Fonte: Gestão de Pessoas, 2014.

A análise dos subsistemas de Recursos Humanos permite compreender as diferentes áreas que compõem a gestão de pessoas nas organizações. Entre esses subsistemas, destaca-se o Departamento Pessoal, responsável pelas rotinas administrativas e pelo gerenciamento de informações dos colaboradores, aspecto relevante para a presente pesquisa.

2.2.1 O Departamento Pessoal

De acordo com Holmes, “O Departamento Pessoal é responsável pela movimentação econômico-financeira laboral do trabalhador, conduzindo essa movimentação através da interpretação e aplicação da legislação trabalhista, previdenciária e fiscal” (HOLMES, 2019).

Dessa forma, o Departamento Pessoal não é apenas um setor burocrático, mas sim um elo fundamental para o cumprimento da legislação trabalhista e para a correta gestão das relações entre empregador e empregado dentro da organização.

Devido à complexidade das rotinas administrativas e trabalhistas, o Departamento Pessoal necessita de ferramentas adequadas para a execução de suas atividades. Processos como folha de pagamento, controle de benefícios, registro de horas extras e demais obrigações legais demandam organização e precisão, tornando

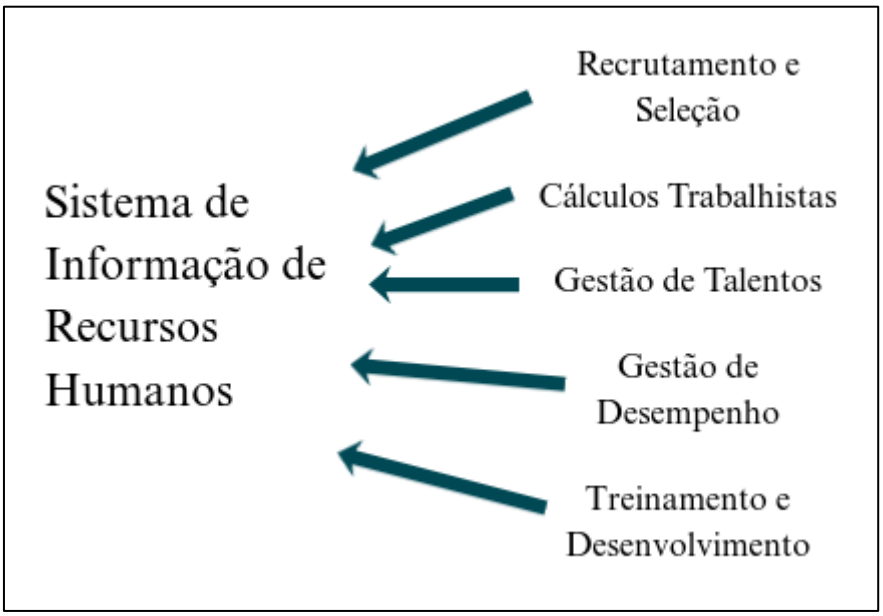
essencial o uso de sistemas de gestão capazes de armazenar, processar e gerenciar as informações dos colaboradores.

2.2.2 Sistemas de Informação de Recursos Humanos

Sendo o setor de Recursos Humanos considerado estratégico dentro das organizações, torna-se necessário acompanhar os avanços da tecnologia da informação. Diante da complexidade das rotinas e processos envolvidos na gestão de pessoas, faz-se necessário o uso de softwares e sistemas informatizados que auxiliem na execução dessas atividades. Esses sistemas, conhecidos como e-RH ou Sistemas de Informação de Recursos Humanos, utilizam recursos tecnológicos e redes de comunicação para apoiar as atividades do setor e automatizar processos administrativos relacionados aos colaboradores (COSTA, 2005).

A Figura abaixo demonstra a integração de diferentes atividades do setor de Recursos Humanos em um Sistema de Informação de Recursos Humanos, no qual diversos processos da gestão de pessoas se conectam a um sistema central responsável pela organização dessas informações.

Figura 3 - Integração do RH



Fonte: Grupo, 2026.

A unificação dos subsistemas de Recursos Humanos em um único sistema apresenta-se como uma vantagem estratégica para as organizações, proporcionando

benefícios como redução de custos, maior facilidade de acesso às informações e melhor controle e integração dos processos. Entretanto, essa centralização também exige maior atenção em relação ao fluxo e ao tratamento dos dados gerenciados pelo sistema, uma vez que a tecnologia da informação tem sido utilizada pelas organizações para apoiar processos administrativos, melhorar a eficiência organizacional e facilitar a gestão das atividades empresariais (ALBERTIN, 2001).

2.2.3 Fluxo de Informações no RH

O setor de Recursos Humanos contemporâneo tem passado por processos de automação que buscam reduzir atividades operacionais e permitir maior foco em atividades estratégicas relacionadas à gestão de pessoas. De acordo com pesquisa da McKinsey & Company, organizações que automatizaram processos administrativos de RH conseguiram reduzir entre 20% e 40% do tempo gasto em atividades operacionais.

Nesse sentido, alguns profissionais da área destacam que a automação também permite maior atenção a ações simples de engajamento com os colaboradores. Como observa a especialista em RH Isis Borge, “quando você automatiza processos, fica mais fácil fazer coisas simples que encantam: lembrar aniversário, tempo de casa ou pequenas celebrações, o que contribui para fortalecer o vínculo entre colaborador e organização”.

Ao tornar o setor de Recursos Humanos mais estratégico, surge também a necessidade de maior atenção ao fluxo de informações geradas pelo próprio setor. Nesse contexto, os profissionais da área precisam desenvolver competências relacionadas à gestão de dados e ao tratamento adequado dessas informações. Como exemplo dessa mudança, a especialista em Departamento Pessoal Rafaela Lucena destaca que “o DP agora é um gerador de dados. Tem muita informação, então precisa haver uma biblioteca de dados muito forte, para que informações como fluxogramas e responsabilidades não fiquem apenas na cabeça das pessoas”. Dessa forma, observa-se que a organização e a gestão estruturada dessas informações tornam-se fundamentais para o funcionamento eficiente do setor.

Diante do grande volume de dados gerenciados pelas organizações, especialmente no setor de Recursos Humanos, torna-se necessária a adoção de práticas voltadas à proteção dessas informações. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais estabelece diretrizes obrigatórias para o tratamento de

dados pessoais no Brasil. Além disso, a segurança dessas informações depende também da atuação dos profissionais que lidam diretamente com esses dados, uma vez que a proteção da informação envolve políticas, processos e comportamentos adotados dentro da organização (SÊMOLA, 2014).

2.3 Introdução à Norma ABNT NBR ISO/IEC 27001:2022

No cenário de intensificação do uso de tecnologias digitais, a informação passou a ser um dos principais ativos organizacionais, exigindo mecanismos de proteção capazes de reduzir riscos e sustentar a continuidade das atividades. Nessa direção, a literatura nacional destaca que a segurança da informação deve ser compreendida de forma sistêmica, considerando ativos, vulnerabilidades, ameaças e riscos como elementos interdependentes do ambiente organizacional (MASCARENHAS NETO; ARAÚJO, 2019). Em órgãos públicos, a adoção de práticas estruturadas de segurança também foi associada ao fortalecimento dos controles internos, ao aumento da resiliência dos serviços e à melhoria da imagem institucional (NUNAN; COSTA FILHO; LIMA, 2016).

Diante desse contexto, a ISO/IEC 27001 assume papel central por estabelecer requisitos para a criação, implementação, manutenção e melhoria contínua de um Sistema de Gestão da Segurança da Informação (SGSI). A norma orienta a organização a definir o escopo do sistema, promover liderança e comprometimento, planejar ações para tratar riscos e oportunidades, prover recursos, monitorar o desempenho e assegurar a melhoria contínua (ABNT, 2022). A versão 2022 incorporou formalmente ao título as dimensões de segurança cibernética e proteção à privacidade, estreitando o alinhamento com a LGPD. Dessa forma, a ABNT NBR ISO/IEC 27001:2022 ultrapassa a dimensão puramente técnica e consolida uma abordagem de gestão orientada ao risco e à governança da informação.

2.3.1 Segurança da Informação e Sistema de Gestão

A segurança da informação não se restringe à instalação de ferramentas tecnológicas, pois envolve políticas, processos, pessoas e controles que atuam de maneira integrada. Mascarenhas Neto e Araújo (2019) apresentam a informação como ativo estratégico e destacam que sua proteção exige visão sistêmica, uma vez que ameaças e vulnerabilidades devem ser analisadas em conjunto com os objetivos organizacionais. Nessa perspectiva, a segurança da informação passa a ser

entendida como parte da gestão da organização e não como um elemento isolado do setor de tecnologia.

A implantação de um SGSI pressupõe estrutura formal, responsabilidades definidas e monitoramento contínuo. Nunan, Costa Filho e Lima (2016) demonstram que a Norma ABNT NBR ISO/IEC 27001 organiza o sistema em lógica semelhante ao ciclo PDCA, articulando planejamento, execução, verificação e ação corretiva. Esse modelo favorece a adaptação constante dos controles às mudanças do ambiente interno e externo, o que é essencial em cenários marcados por riscos cibernéticos, exigências regulatórias e dependência crescente de sistemas informacionais.

2.3.2 A ISO/IEC 27001 e a Gestão de Riscos

A norma ISO/IEC 27001 estrutura requisitos que permitem identificar riscos, definir tratamentos, estabelecer responsabilidades e controlar informações documentadas. Sua lógica é compatível com a necessidade de governança, pois os riscos de segurança da informação devem ser tratados de forma sistemática e proporcional ao contexto da organização (ABNT, 2022). A versão 2022 introduziu o requisito 6.3 (Planejamento de mudanças), que formaliza a exigência de que alterações no SGSI sejam conduzidas de forma estruturada (ABNT, 2022). Em estudos brasileiros, essa abordagem é apresentada como fundamental para alinhar a política de segurança, o planejamento estratégico e a operação cotidiana das instituições, preservando a confiança nas informações e nos processos.

Mendes et al. (2013) reforçam que a implantação de um SGSI baseado nas normas ABNT NBR ISO/IEC 27001 e 27002 exige processos gerenciados e decisões orientadas por controles adequados às necessidades do negócio. Na mesma direção, materiais institucionais e acadêmicos mostram que a adoção da norma tende a melhorar a capacidade da organização de prevenir incidentes, responder a falhas e sustentar a continuidade das atividades essenciais (MENDES et al., 2013; NUNAN; COSTA FILHO; LIMA, 2016).

2.3.3 A Tríade CIA na Segurança da Informação

O núcleo conceitual da segurança da informação é tradicionalmente representado pela tríade CIA, formada por confidencialidade, integridade e disponibilidade. Hintzbergen et al. (2018) explicam que a segurança da informação consiste na preservação simultânea desses três atributos, os quais orientam a escolha de políticas, controles e mecanismos de proteção. A própria ABNT NBR ISO/IEC 27001 também associa o SGSI à preservação desses princípios, ao vincular a gestão de riscos à proteção da informação em sua totalidade (ABNT, 2022).

A confidencialidade relaciona-se ao acesso restrito da informação, assegurando que apenas pessoas autorizadas possam consultar ou utilizar determinados dados. A integridade diz respeito à manutenção da exatidão, consistência e estado esperado da informação, evitando alterações indevidas, acidentais ou intencionais. Já a disponibilidade garante que os dados e sistemas permaneçam acessíveis quando necessários, inclusive em situações de falha, interrupção ou ataque. Em conjunto, esses três elementos sustentam a credibilidade das informações e a confiabilidade dos processos organizacionais (HINTZBERGEN et al., 2018; MASCARENHAS NETO; ARAÚJO, 2019).

2.3.4 Relevância Organizacional e Continuidade

A efetividade da segurança da informação depende da formalização de políticas, da definição de responsabilidades, da conscientização dos usuários e do tratamento consistente dos riscos. Em pesquisas aplicadas ao setor público, observou-se que a implementação da segurança da informação fortalece os controles internos, aumenta a resiliência dos serviços e contribui para a melhoria do desempenho organizacional (NUNAN; COSTA FILHO; LIMA, 2016). Assim, a adoção da ISO/IEC 27001 deve ser compreendida como uma iniciativa estratégica, pois viabiliza maior controle sobre os ativos informacionais e apoio às decisões institucionais.

Além de proteger informações e reduzir incidentes, o SGSI contribui para a continuidade dos negócios e para a melhoria contínua dos processos. Quando a organização integra política, riscos, controles e monitoramento, cria melhores condições para responder a ameaças, corrigir falhas e aprimorar seu nível de

maturidade em segurança da informação. Por esse motivo, a norma é frequentemente adotada como base para programas de governança da informação e para a construção de uma cultura organizacional voltada à proteção de dados.

2.4 Gestão e Governança de Dados

2.4.1 O Dado como Ativo de Valor

Segundo Bergson Lopes Rego (2013), as organizações contemporâneas atravessam uma mudança de paradigma na qual o dado deixa de ser um subproduto tecnológico para assumir o papel de ativo estratégico. Nesse contexto, os dados passam a ser reconhecidos como elementos fundamentais para a geração de valor, inovação e vantagem competitiva.

Ainda de acordo com o autor, para que esse valor seja efetivamente alcançado, os dados devem ser geridos com o mesmo nível de rigor aplicado a ativos financeiros ou físicos. Assim, a Gestão de Dados pode ser compreendida como o conjunto de práticas voltadas ao desenvolvimento, execução e supervisão de planos, políticas e programas que visam controlar, proteger e potencializar o valor dos ativos de dados (Bergson Lopes Rego, 2013).

2.4.2 O Framework DAMA-DMBOK

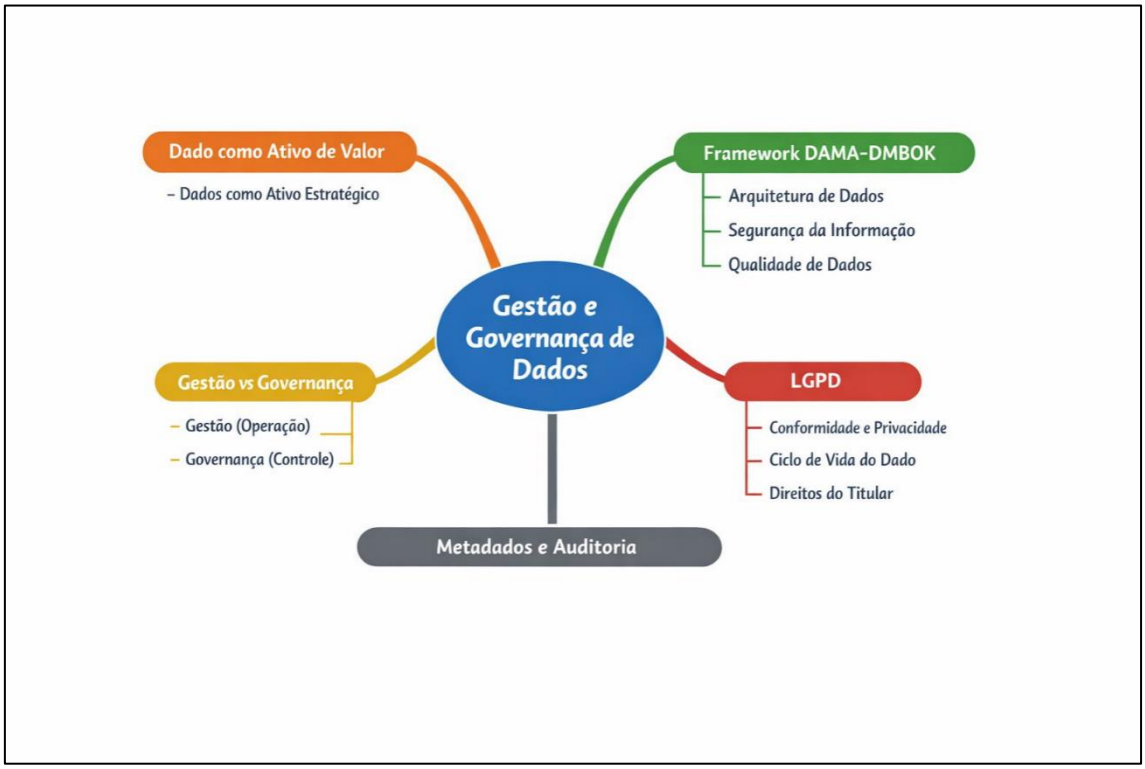
A abordagem apresentada por Rego (2013) está alinhada ao Data Management Body of Knowledge (DAMA-DMBOK), que organiza a gestão de dados em diferentes áreas de conhecimento integradas (DAMA INTERNATIONAL, 2017). Nesse contexto, a Arquitetura de Dados é responsável por definir a estrutura e os modelos necessários para atender às demandas organizacionais, enquanto a Segurança de Dados visa garantir a confidencialidade, integridade e disponibilidade das informações. Paralelamente, a Qualidade de Dados dedica-se à implementação de processos que assegurem a precisão, completude e consistência dos dados. Essas funções, quando integradas, sustentam ambientes informacionais seguros, confiáveis e alinhados aos objetivos estratégicos das organizações.

2.4.3 Diferença entre Gestão e Governança de Dados

Um ponto central na literatura de Rego (2013) é a distinção entre Gestão de Dados e Governança de Dados. Enquanto a gestão está relacionada às atividades operacionais e técnicas, ou seja, ao “fazer”, a governança exerce um papel estratégico

ao estabelecer diretrizes, regras e mecanismos de controle sobre os dados. Nesse sentido, a Governança de Dados define papéis e responsabilidades, como o do Data Steward, além de assegurar que as práticas de gestão estejam alinhadas aos objetivos organizacionais e às exigências regulatórias (Bergson Lopes Rego, 2013; DAMA INTERNATIONAL, 2017).

Figura 4 - Mapa Mental



Fonte: Grupo, 2026

2.4.4 Interface entre Gestão de Dados e a LGPD

A promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), introduziu um conjunto de exigências legais que tornam indispensável a adoção de práticas estruturadas de gestão e governança de dados (BRASIL, 2018). Nesse contexto, observa-se que a conformidade regulatória depende diretamente da implementação de mecanismos de governança, em consonância com o princípio da responsabilização e prestação de contas (accountability), o qual exige que as organizações demonstrem controle sobre o tratamento de dados pessoais.

Além disso, a segurança da informação deve ser tratada como um processo contínuo ao longo de todo o ciclo de vida dos dados, abrangendo etapas como classificação, armazenamento, uso e eliminação após o término do tratamento,

conforme previsto na legislação. A qualidade dos dados também desempenha papel fundamental, uma vez que viabiliza o atendimento aos direitos dos titulares, especialmente no que se refere à correção de informações incompletas, inexatas ou desatualizadas.

Adicionalmente, a gestão de metadados entendidos como dados sobre os dados contribui para a rastreabilidade e transparência das informações, facilitando o atendimento a requisições de órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD). Por fim, destaca-se que as práticas de segurança da informação adotadas na gestão de dados encontram respaldo em normas como a ABNT NBR ISO/IEC 27001, que estabelece requisitos para a implementação de sistemas de gestão da segurança da informação, reforçando a proteção dos ativos informacionais.

3 DESENVOLVIMENTO

Neste capítulo, apresenta-se um estudo de caso sobre a adequação à Lei Geral de Proteção de Dados (LGPD) na empresa utilizada como objeto de estudo. O objetivo é verificar o nível de conhecimento da organização sobre a LGPD e analisar seu grau de conformidade com a legislação nas práticas relacionadas ao tratamento de dados pessoais e sensíveis.

Considerando que escritórios contábeis lidam com grande volume de dados de clientes, fornecedores e colaboradores, como informações financeiras, registros de folha de pagamento, admissões, demissões e rescisões, torna-se importante compreender como esses ambientes adotam boas práticas de segurança da informação e proteção de dados em seu cotidiano.

Para isso, realiza-se a análise das práticas internas da instituição por meio de entrevistas e aplicação de formulários, buscando identificar as medidas atualmente adotadas, possíveis fragilidades e o nível de conhecimento dos colaboradores sobre a LGPD. Com base nesse diagnóstico, propõem-se intervenções e recomendações voltadas à melhoria da proteção de dados e à redução de riscos relacionados à segurança da informação.

Por fim, apresentam-se sugestões de adequação à LGPD, cuja implementação fica a critério da empresa, destacando também a importância da conscientização dos colaboradores quanto ao tratamento adequado de dados pessoais e sensíveis.

3.1 Elaboração dos Documentos de Apoio

Inicialmente, foram elaborados os documentos necessários para a realização dos questionamentos, os quais foram organizados em formato de checklist. Esses documentos foram segmentados de acordo com as áreas das quais se pretendia coletar informações: Sócio, Tecnologia da Informação (TI) e Recursos Humanos (RH).

Os documentos elaborados para a aplicação das entrevistas foram baseados na Lei Geral de Proteção de Dados (LGPD) e na norma ISO 27001, incluindo também a criação dos termos de consentimento, com o objetivo de evidenciar e registrar a autorização dos entrevistados.

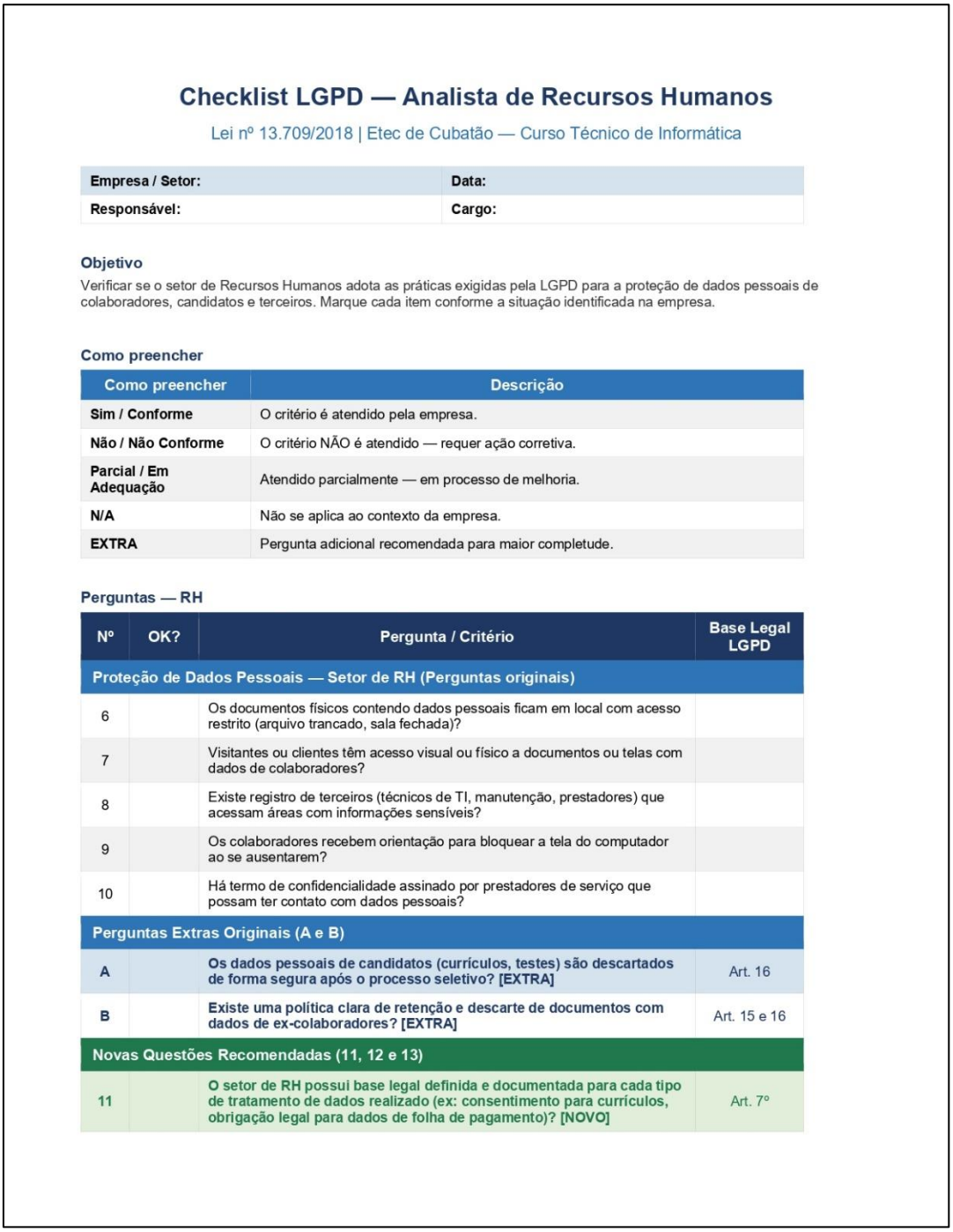
Figura 5 - Modelo 1 de Checklist

Tabela X – Checklist de Conformidade com LGPD e ISO 27001 em Empresa de Contabilidade

Nº	Categoria	Item de Verificação	Status	Evidência	Responsável
1	Controle de Acesso	Funcionários utilizam crachá de identificação			
2	Controle de Acesso	Existe controle de entrada/saída de pessoas			
3	Controle de Acesso	Computadores possuem login individual			
4	Controle de Acesso	Há política de senhas definida			
5	Controle de Acesso	Acessos são removidos após desligamento			
6	Níveis de Acesso	Sistemas possuem acesso por perfil (RBAC)			
7	Níveis de Acesso	Usuários acessam apenas o necessário (menor privilégio)			
8	Níveis de Acesso	Existe segregação de funções			
9	Níveis de Acesso	Há registro de logs de acesso			
10	Níveis de Acesso	Acessos são revisados periodicamente			
11	Níveis de Acesso	Existe autenticação em dois fatores (2FA)			
12	Segurança da Informação	Existe política de segurança formal			
13	Segurança da Informação	Funcionários recebem treinamento			
14	Segurança da Informação	Há antivírus e firewall ativos			
15	Segurança da Informação	Sistemas são atualizados regularmente			
16	Segurança da Informação	Existe backup dos dados			
17	Segurança da Informação	Backup é testado periodicamente			
18	LGPD	A empresa sabe quais dados coleta			
19	LGPD	Existe base legal para tratamento de dados			
20	LGPD	Há política de privacidade documentada			
21	LGPD	Dados são armazenados com segurança			

Fonte: Grupo, 2026

Figura 6 - Modelo 2 de Checklist



Checklist LGPD — Analista de Recursos Humanos

Lei nº 13.709/2018 | Etec de Cubatão — Curso Técnico de Informática

Empresa / Setor:	**Data:**
Responsável:	**Cargo:**

Objetivo

Verificar se o setor de Recursos Humanos adota as práticas exigidas pela LGPD para a proteção de dados pessoais de colaboradores, candidatos e terceiros. Marque cada item conforme a situação identificada na empresa.

Como preencher

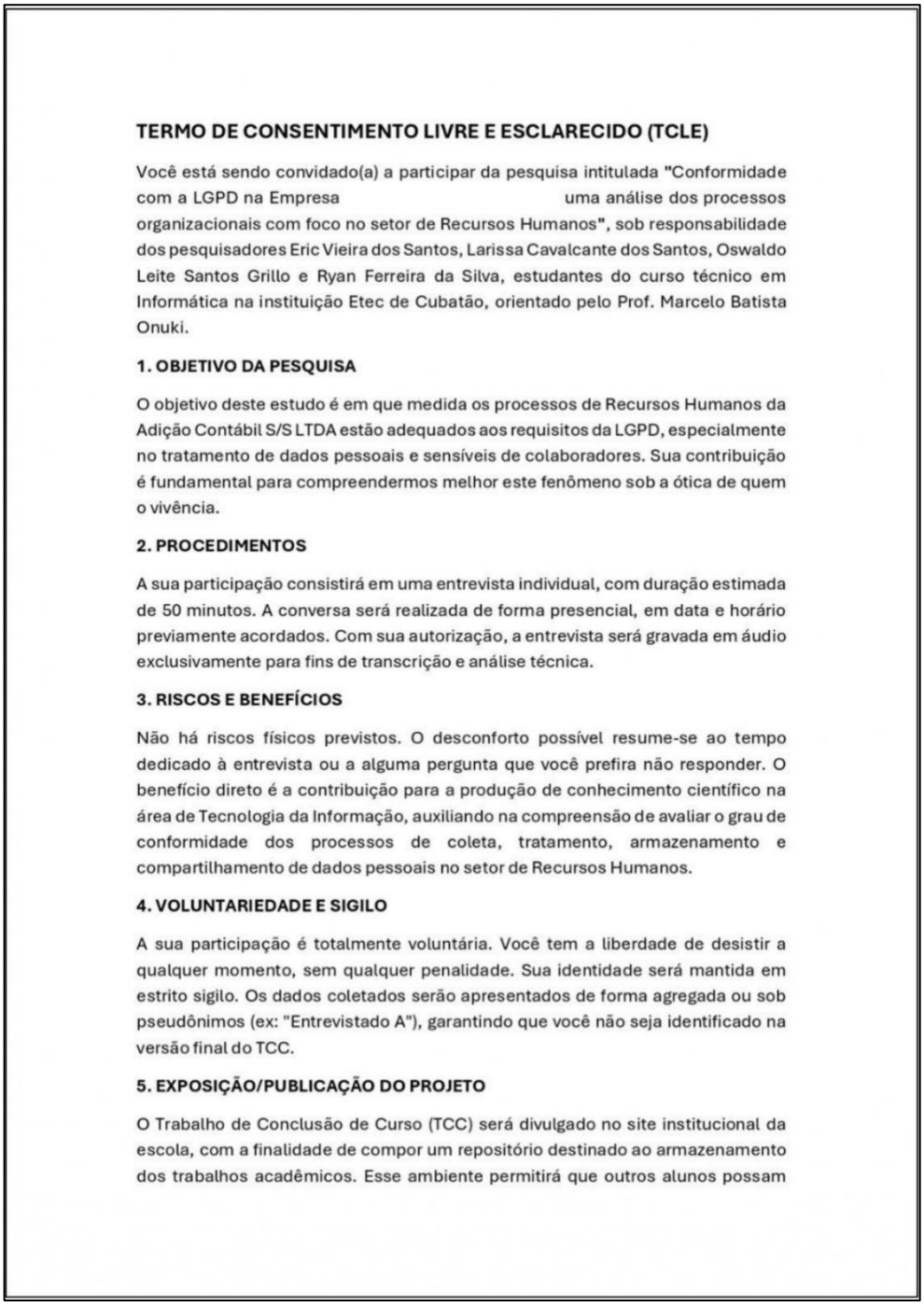
Como preencher	Descrição
Sim / Conforme	O critério é atendido pela empresa.
Não / Não Conforme	O critério NÃO é atendido — requer ação corretiva.
Parcial / Em Adequação	Atendido parcialmente — em processo de melhoria.
N/A	Não se aplica ao contexto da empresa.
EXTRA	Pergunta adicional recomendada para maior completude.

Perguntas — RH

Nº	OK?	Pergunta / Critério	Base Legal LGPD
Proteção de Dados Pessoais — Setor de RH (Perguntas originais)			
6		Os documentos físicos contendo dados pessoais ficam em local com acesso restrito (arquivo trancado, sala fechada)?	
7		Visitantes ou clientes têm acesso visual ou físico a documentos ou telas com dados de colaboradores?	
8		Existe registro de terceiros (técnicos de TI, manutenção, prestadores) que acessam áreas com informações sensíveis?	
9		Os colaboradores recebem orientação para bloquear a tela do computador ao se ausentarem?	
10		Há termo de confidencialidade assinado por prestadores de serviço que possam ter contato com dados pessoais?	
Perguntas Extras Originais (A e B)			
A		**Os dados pessoais de candidatos (currículos, testes) são descartados de forma segura após o processo seletivo? [EXTRA]**	Art. 16
B		**Existe uma política clara de retenção e descarte de documentos com dados de ex-colaboradores? [EXTRA]**	Art. 15 e 16
Novas Questões Recomendadas (11, 12 e 13)			
11		**O setor de RH possui base legal definida e documentada para cada tipo de tratamento de dados realizado (ex: consentimento para currículos, obrigação legal para dados de folha de pagamento)? [NOVO]**	Art. 7º

Fonte: Grupo, 2026

Figura 7 - Modelo de Termo de Consentimento



TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Você está sendo convidado(a) a participar da pesquisa intitulada "Conformidade com a LGPD na Empresa uma análise dos processos organizacionais com foco no setor de Recursos Humanos", sob responsabilidade dos pesquisadores Eric Vieira dos Santos, Larissa Cavalcante dos Santos, Oswaldo Leite Santos Grillo e Ryan Ferreira da Silva, estudantes do curso técnico em Informática na instituição Etec de Cubatão, orientado pelo Prof. Marcelo Batista Onuki.

1. OBJETIVO DA PESQUISA

O objetivo deste estudo é em que medida os processos de Recursos Humanos da Adição Contábil S/S LTDA estão adequados aos requisitos da LGPD, especialmente no tratamento de dados pessoais e sensíveis de colaboradores. Sua contribuição é fundamental para compreendermos melhor este fenômeno sob a ótica de quem o vivência.

2. PROCEDIMENTOS

A sua participação consistirá em uma entrevista individual, com duração estimada de 50 minutos. A conversa será realizada de forma presencial, em data e horário previamente acordados. Com sua autorização, a entrevista será gravada em áudio exclusivamente para fins de transcrição e análise técnica.

3. RISCOS E BENEFÍCIOS

Não há riscos físicos previstos. O desconforto possível resume-se ao tempo dedicado à entrevista ou a alguma pergunta que você prefira não responder. O benefício direto é a contribuição para a produção de conhecimento científico na área de Tecnologia da Informação, auxiliando na compreensão de avaliar o grau de conformidade dos processos de coleta, tratamento, armazenamento e compartilhamento de dados pessoais no setor de Recursos Humanos.

4. VOLUNTARIEDADE E SIGILO

A sua participação é totalmente voluntária. Você tem a liberdade de desistir a qualquer momento, sem qualquer penalidade. Sua identidade será mantida em estrito sigilo. Os dados coletados serão apresentados de forma agregada ou sob pseudônimos (ex: "Entrevistado A"), garantindo que você não seja identificado na versão final do TCC.

5. EXPOSIÇÃO/PUBLICAÇÃO DO PROJETO

O Trabalho de Conclusão de Curso (TCC) será divulgado no site institucional da escola, com a finalidade de compor um repositório destinado ao armazenamento dos trabalhos acadêmicos. Esse ambiente permitirá que outros alunos possam

Fonte: Grupo, 2026

3.1.1 Elaboração do E-mail para Solicitação de Visita Técnica

Para a realização das visitas técnicas na instituição, foi necessário elaborar um e-mail formal e, paralelamente, alinhar as datas de acordo com a disponibilidade dos participantes que seriam entrevistados. Durante a elaboração do e-mail, o Sócio solicitou que fossem descritas, de forma detalhada, as atividades que seriam

desenvolvidas na instituição, bem como os documentos que seriam utilizados para a coleta de dados.

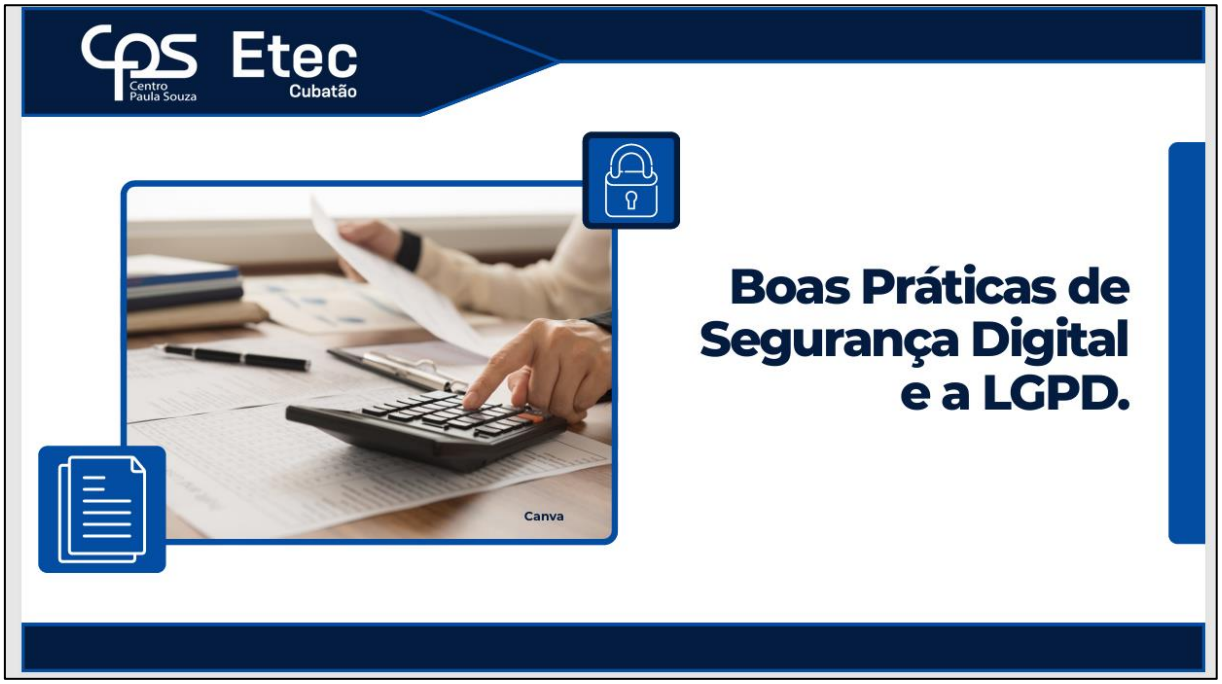
Além disso, tornou-se necessário o envio da comunicação por meio do orientador responsável, considerando sua posição hierárquica superior, o que confere maior formalidade ao processo e evidencia que a instituição de ensino estava ciente da visita.

Ademais, foi providenciada a autorização os integrantes do grupo que são alunos menores de idade, a ser assinada pelos responsáveis legais, permitindo a realização da atividade.

3.1.2 Elaboração da Apresentação de Segurança Digital e LGPD

Para a elaboração da apresentação voltada à capacitação e conscientização dos colaboradores sobre a LGPD e segurança digital, foi utilizado como referência o material desenvolvido na disciplina de Segurança Digital, ministrada pelo professor André Seoane. O conteúdo original, que abordava o funcionamento da segurança digital no contexto de um escritório contábil, serviu como base para a construção do material aplicado, sendo adaptado para uma linguagem mais acessível e alinhada à realidade da empresa. Os tópicos contemplados foram: boas práticas de segurança digital, identificação de golpes digitais, tríade CID, gestão documental e LGPD.

Figura 8 - Capa de Apresentação



Fonte: Grupo, 2026

3.1.3 Elaboração do Questionário Avaliativo

Para que a apresentação contasse com uma métrica de avaliação, foi decidido utilizar um questionário avaliativo com 12 perguntas elaboradas como instrumento de coleta de dados. A ferramenta escolhida foi o Kahoot, plataforma que possibilita a criação de questionários gamificados com perguntas elaboradas com base no conteúdo apresentado, tornando a avaliação mais dinâmica e engajadora para os participantes.

As questões foram desenvolvidas previamente pela equipe com base nos tópicos que seriam abordados na apresentação, buscando verificar, de forma objetiva, o nível de compreensão dos colaboradores sobre os temas de segurança digital e LGPD.

3.2 Entrevistas

A coleta de dados principal foi realizada por meio de entrevistas com representantes das três áreas que abrangem esse trabalho: O sócio representando a empresa, a responsável pelo setor de Recursos Humanos e o profissional de Tecnologia da Informação. O roteiro foi baseado nos eixos temáticos de Controle de Acesso, Segurança da Informação, LGPD, Gestão de Incidentes, Governança e

Direitos dos Titulares, com o objetivo de identificar o nível de conformidade da empresa com a LGPD.

3.2.1 Entrevista com o Sócio

No dia 19 de março de 2026, foi realizada uma entrevista com o Sócio da empresa, que acumula também a função de Encarregado de Dados (DPO) da organização. Essa entrevista correspondeu a uma das três áreas estratégicas definidas como eixo central deste trabalho, representando a perspectiva institucional da empresa como um todo. O objetivo foi coletar informações que permitissem avaliar o nível de conformidade da organização com os requisitos da Lei Geral de Proteção de Dados Pessoais. Para isso, foi utilizado um checklist elaborado com base nos principais temas da legislação, abrangendo os eixos de controle de acesso, segurança da informação, gestão documental e direitos dos titulares de dados.

3.2.2 Entrevista com o Setor de Recursos Humanos - RH

No dia 28 de abril de 2026, foi realizada uma entrevista com a responsável pelo setor de Recursos Humanos da empresa. Essa entrevista correspondeu à segunda área estratégica definida para este trabalho, com foco nos dados dos colaboradores. Como instrumento de coleta, foi utilizado o mesmo checklist baseado nos requisitos da LGPD, abrangendo os eixos de controle de acesso, gestão documental e tratamento de dados pessoais no contexto do RH.

3.2.3 Entrevista com o Setor de Tecnologia da Informação – TI

No dia 29 de abril de 2026, foi realizada uma entrevista com o profissional responsável pelo setor de Tecnologia da Informação da empresa. Essa entrevista correspondeu à terceira área estratégica definida para este trabalho, com foco na governança de dados e na infraestrutura tecnológica da organização. Assim como nas demais entrevistas, foi utilizado o checklist baseado nos requisitos da LGPD como instrumento de coleta.

3.3 Capacitação e Conscientização dos Colaboradores

No dia 28 de abril de 2026, como parte dos objetivos deste trabalho, foi realizada uma apresentação sobre segurança digital e LGPD nas dependências da empresa. O material, elaborado previamente pela equipe, foi adaptado para uma linguagem mais acessível e interativa, com exemplos práticos do cotidiano profissional, abordando temas como boas práticas de segurança digital, identificação de golpes digitais, tríade CID, gestão documental e LGPD.

Ao término da apresentação, foi aplicado um questionário gamificado por meio da plataforma Kahoot, desenvolvido previamente pela equipe com o objetivo de avaliar o nível de absorção do conteúdo pelos participantes de forma dinâmica, permitindo também, uma análise dos resultados da apresentação.

Figura 9 - Registro da Capacitação

Fonte: Grupo, 2026

3.4 Formulário aos Colaboradores

Com base em uma das hipóteses levantadas neste trabalho, identificou-se a necessidade de aplicar um formulário diretamente aos colaboradores da empresa, com o objetivo de coletar dados sobre o conhecimento e a percepção dos funcionários em relação às boas práticas de segurança digital e à LGPD. O instrumento foi

desenvolvido por meio do Google Forms e contemplou 11 perguntas distribuídas entre os tópicos de controle de acesso, boas práticas e conformidade com a LGPD.

A fim de garantir respostas mais honestas e espontâneas, o formulário foi disponibilizado de forma anônima, assegurando aos colaboradores liberdade para responder sem receio de identificação ou julgamento.

Figura 10 - Formulário Aplicado

Fonte: Grupo, 2026

3.5 Proposta de Intervenção

Com base nos resultados obtidos ao longo da pesquisa, foi elaborado um Plano de Intervenção com o objetivo de propor ações concretas para a adequação da empresa às exigências da LGPD. O plano foi estruturado a partir das principais não conformidades identificadas nas entrevistas, no formulário aplicado aos colaboradores e no questionário gamificado via Kahoot, e organizado em oito ações distribuídas em quatro fases ao longo de doze meses. O documento completo encontra-se disponível no Apêndice D deste trabalho.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A análise dos dados coletados por meio das entrevistas com os profissionais da empresa, do formulário aplicado aos colaboradores e do questionário gamificado realizado via Kahoot possibilitou compreender, com maior precisão, o nível de conformidade da organização em relação às diretrizes da Lei Geral de Proteção de Dados Pessoais e às boas práticas de segurança da informação. De modo geral, os resultados evidenciam a existência de práticas parcialmente alinhadas à legislação, revelando avanços significativos em alguns aspectos, mas também lacunas relevantes que demandam atenção por parte da gestão.

4.1 Resultado das Entrevistas

A coleta de dados por meio das entrevistas foi realizada com representantes das três áreas estratégicas definidas para este trabalho: a Empresa, representada pelo Sócio e Encarregado de Dados (DPO); o setor de Recursos Humanos, com foco no tratamento de dados dos colaboradores; e o setor de Tecnologia da Informação, com foco na governança e infraestrutura tecnológica. As entrevistas foram conduzidas com base em um checklist estruturado a partir dos requisitos da LGPD, permitindo identificar o nível de conformidade da organização em cada uma dessas frentes. Os resultados são apresentados e analisados a seguir.

4.1.1 Resultados da Entrevista do Sócio - DPO

A entrevista com o Sócio revelou um cenário de conformidade parcial com a LGPD. A organização demonstra consciência sobre a importância da proteção de dados e possui iniciativas estruturadas em algumas frentes, embora persistam lacunas relevantes.

Em relação ao controle de acesso, identificou-se que os computadores com sistema operacional Windows não possuem senha individual na maior parte das estações de trabalho, decisão tomada após episódios de bloqueio por esquecimento de credenciais. Para os sistemas específicos, cada colaborador recebe uma senha padrão no primeiro acesso, sem requisito mínimo de complexidade definido pela empresa. Essa ausência de credenciais individuais compromete a rastreabilidade de acessos, dificultando a identificação de responsáveis em caso de incidentes e

contrariando o princípio da responsabilização e prestação de contas previsto no artigo 6º, inciso X, da LGPD.

Quanto à segurança da informação, a empresa mantém antivírus, firewall ativo e backup quádruplo com cópias em nuvem e em locais físicos distintos, o que demonstra maturidade na continuidade de negócios. A criptografia, no entanto, é aplicada apenas a clientes prioritários, podendo ser inconsistente com o princípio da segurança do artigo 6º da LGPD, que exige proteção adequada independentemente do perfil do titular.

Os treinamentos de conscientização são realizados sem periodicidade regular, conforme relatado pelo entrevistado: *"Foi feito lá atrás, mas ele precisa ser refeito periodicamente e a gente ainda não fez esse ano por exemplo."* A ausência de um calendário definido fragiliza a cultura de proteção de dados na organização.

Por fim, identificou-se a ausência de cláusula contratual que obrigue colaboradores desligados a excluir dados corporativos de dispositivos pessoais: "*Não tem. Esse é um bom questionamento inclusive. Ele vai ficar querendo ou não com as informações na pasta de download dele.*" Essa lacuna representa um risco à confidencialidade das informações dos clientes após o encerramento do vínculo empregatício.

4.1.2 Resultados da Entrevista do Setor de Recursos Humanos

A entrevista com a responsável pelo RH revelou práticas positivas no tratamento de dados dos colaboradores, acompanhadas de pontos que merecem atenção sob a ótica da LGPD.

A entrevistada confirmou que documentos físicos com dados pessoais ficam armazenados em local com acesso restrito, inacessível a visitantes e clientes, e que os colaboradores possuem termo de confidencialidade previsto no contrato de trabalho. Esses aspectos demonstram alinhamento com o princípio da segurança da informação. No entanto, não foi possível confirmar se o mesmo termo foi exigido do prestador de serviços de TI, por tratar-se de contratação anterior à chegada da entrevistada à empresa. Essa lacuna é relevante, uma vez que o prestador possui acesso privilegiado a sistemas e dados da organização, devendo estar sujeito às mesmas obrigações de confidencialidade.

Sobre o processo de recrutamento e seleção, foi informado que currículos de candidatos não aprovados são mantidos em banco de talentos para oportunidades

futuras. Essa prática, embora comum no mercado, pode ser inconsistente com a LGPD, pois a retenção prolongada de dados pessoais de candidatos sem consentimento explícito para essa finalidade específica contraria o princípio da finalidade previsto no artigo 6º da lei, que exige que os dados sejam utilizados apenas para os propósitos que motivaram sua coleta.

A política de retenção de documentos de ex-colaboradores segue o prazo legal de cinco anos, demonstrando conformidade com as obrigações trabalhistas. O projeto de digitalização do acervo físico em andamento também representa um avanço relevante, contribuindo para maior controle, rastreabilidade e segurança no armazenamento das informações.

4.1.3 Resultados da Entrevista do Setor de Tecnologia da Informação

A entrevista com o profissional de TI permitiu avaliar a infraestrutura tecnológica da empresa sob a perspectiva da segurança da informação e da conformidade com a LGPD.

O entrevistado confirmou que os sistemas possuem credenciais individuais e perfis de permissão por função, e que o acesso físico ao servidor é controlado. Técnicos externos atuam sob supervisão ou com acesso temporário, o que demonstra cuidado no controle de acessos privilegiados. Esses aspectos estão alinhados às boas práticas recomendadas pela ISO/IEC 27001.

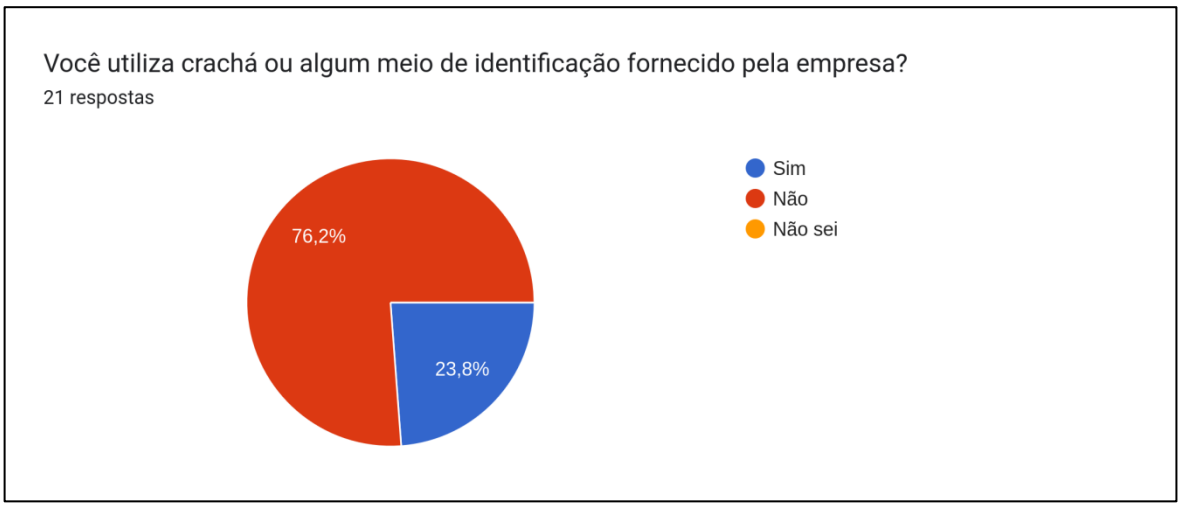
Em relação ao registro de logs, o profissional demonstrou incerteza sobre a existência desses registros fora do aplicativo comercial utilizado pela empresa: *"Eu acho que não. Só se for por dentro do aplicativo comercial mesmo, mas eu acho que não."* A ausência de logs de acesso representa uma lacuna significativa para fins de rastreabilidade e auditoria, dificultando a identificação de acessos indevidos e contrariando o princípio da responsabilização e prestação de contas previsto no artigo 6º, inciso X, da LGPD.

O próprio profissional reconheceu a necessidade de aprimorar o controle de acesso à rede corporativa. A segmentação por nicho de rede já foi iniciada para a diretoria e o Departamento Pessoal, mas os setores operacionais ainda operam com acesso amplo à estrutura de pastas da empresa. Essa configuração contraria o princípio do menor privilégio, amplamente recomendado pela ISO/IEC 27001, segundo o qual cada usuário deve ter acesso apenas às informações estritamente necessárias para o exercício de suas funções.

4.2 Análise do Formulário

O questionário foi respondido por 21 colaboradores da empresa e abrangeu onze questões relacionadas a controle de acesso, conhecimento sobre a LGPD e percepção sobre as práticas de segurança da informação adotadas pela organização. A seguir, são apresentados e analisados os resultados de cada questão.

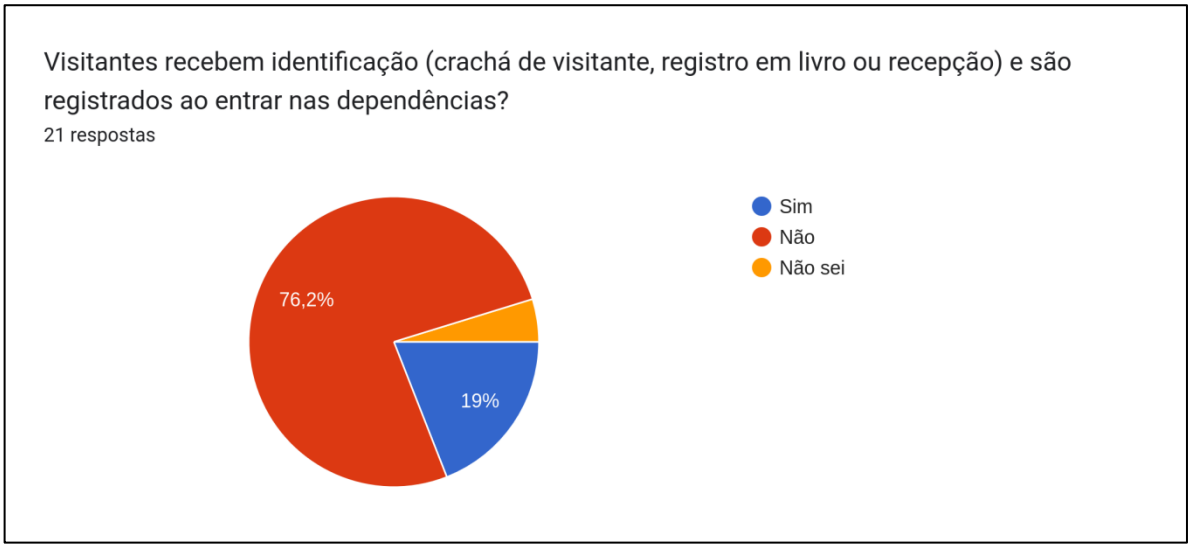
Gráfico 1– Você utiliza crachá ou algum meio de identificação fornecido pela empresa?



Fonte: Grupo, 2026

76,2% dos colaboradores (16 de 21) responderam que não utilizam crachá ou qualquer meio de identificação fornecido pela empresa. Apenas 23,8% (5 respondentes) afirmaram utilizar alguma forma de identificação. Esse resultado está alinhado com o que foi relatado pela gestão na entrevista: a empresa não adota crachás como padrão. Essa ausência representa uma lacuna no controle de acesso físico, especialmente em um ambiente tão sensível.

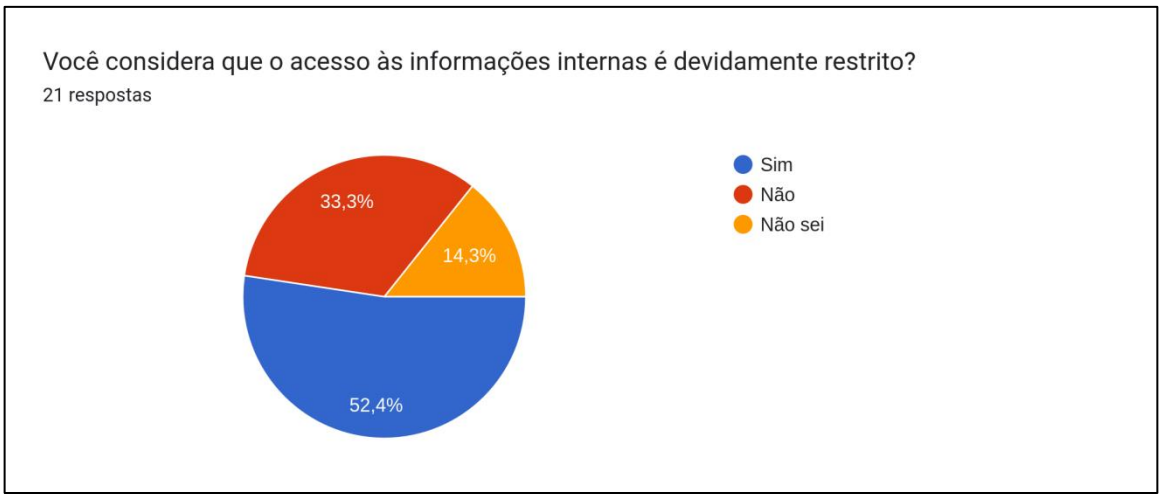
Gráfico 2 – Visitantes recebem identificação e são registrados ao entrar nas dependências?



Fonte: Grupo, 2026

76,2% dos colaboradores (16 de 21) responderam que visitantes não recebem identificação ao entrar na empresa. Apenas 4 respondentes (19%) afirmaram que sim, e 1 (4,8%) declarou não saber. Embora a gestão tenha mencionado a existência de um porteiro que registra entradas e autoriza visitantes, a percepção da maioria dos colaboradores indica que esse processo não é percebido como um controle formal de identificação, evidenciando uma desconexão entre a prática existente e o entendimento dos funcionários sobre ela.

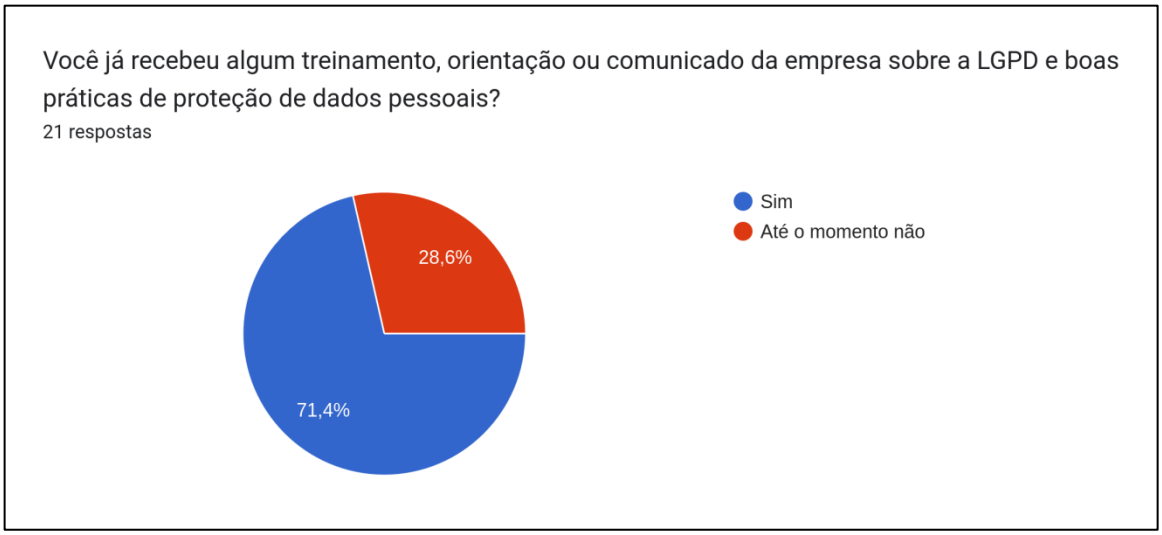
Gráfico 3 – Você considera que o acesso às informações internas é devidamente restrito?



Fonte: Grupo, 2026

As respostas a essa questão foram divididas: 52,4% (11 colaboradores) responderam que sim, 33,3% (7) responderam que não e 14,3% (3) declararam não saber. O resultado reflete o cenário parcial identificado nas entrevistas, onde a segmentação de acesso à rede ainda está em implantação e não abrange todos os setores. A divisão das respostas indica que a percepção varia possivelmente conforme o setor do colaborador, sendo mais positiva entre aqueles já inseridos em ambientes com acesso restrito.

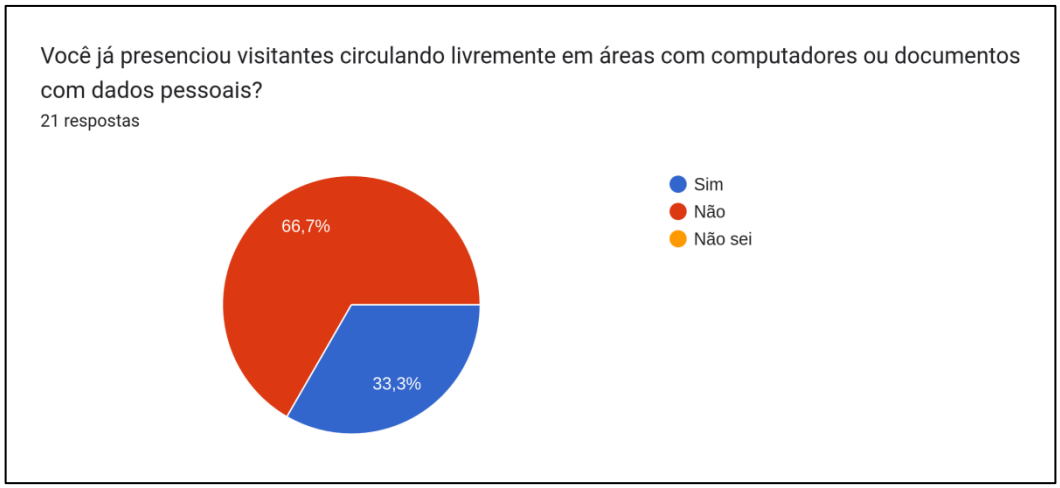
Gráfico 4 – Você já recebeu algum treinamento, orientação ou comunicado da empresa sobre a LGPD?



Fonte: Grupo, 2026

71,4% dos colaboradores (15 de 21) afirmaram já ter recebido algum treinamento, orientação ou comunicado sobre a LGPD e boas práticas de proteção de dados. Os demais 28,6% (6 respondentes) indicaram que até o momento não haviam recebido esse tipo de orientação. Esse índice, embora majoritariamente positivo, reforça a preocupação levantada na entrevista com a gestão sobre a ausência de periodicidade regular nos treinamentos, já que uma parcela significativa dos colaboradores ainda não foi alcançada.

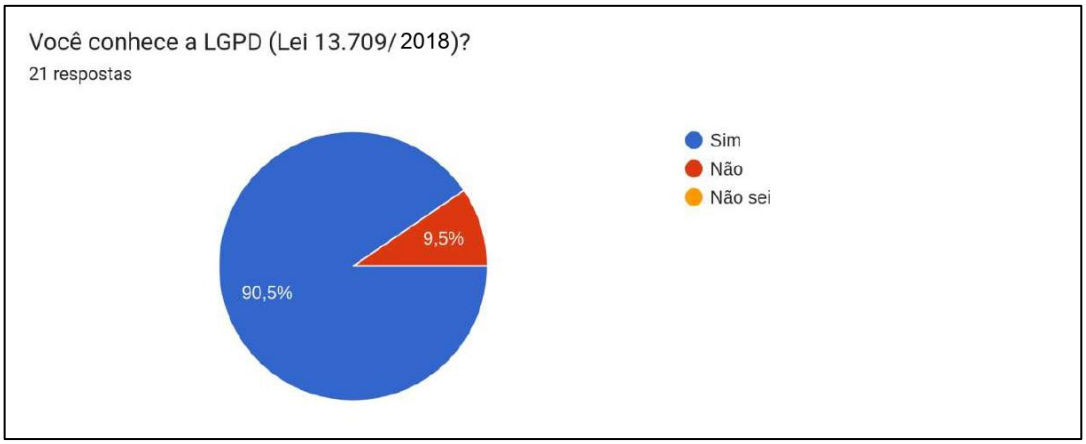
Gráfico 5 – Você já presenciou visitantes circulando livremente em áreas com computadores ou documentos com dados pessoais?



Fonte: Grupo, 2026

66,7% dos colaboradores (14 de 21) responderam que nunca presenciaram visitantes circulando livremente em áreas com computadores ou documentos com dados pessoais. No entanto, 33,3% (7 respondentes) afirmaram já ter presenciado essa situação. Esse percentual é relevante e aponta para brechas no controle de circulação de pessoas externas nas dependências da empresa, especialmente considerando que, segundo a gestão, visitantes devem sempre ser acompanhados por um responsável.

Gráfico 6 – Você conhece a LGPD (Lei 13.709/2018)?

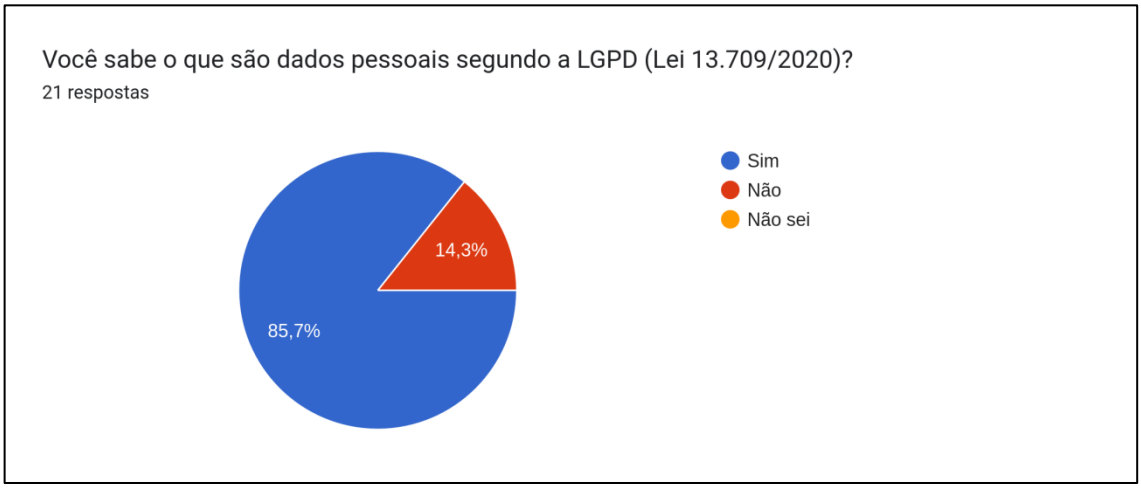


Fonte: Grupo, 2026

90,5% dos colaboradores (19 de 21) afirmaram conhecer a LGPD, enquanto apenas 2 respondentes (9,5%) declararam não conhecê-la. Esse resultado é positivo

e indica que as ações de conscientização realizadas pela empresa ao longo dos anos surtiram efeito no que diz respeito ao conhecimento geral da legislação. Ainda assim, a existência de colaboradores sem ciência da lei reforça a necessidade de treinamentos periódicos e abrangentes.

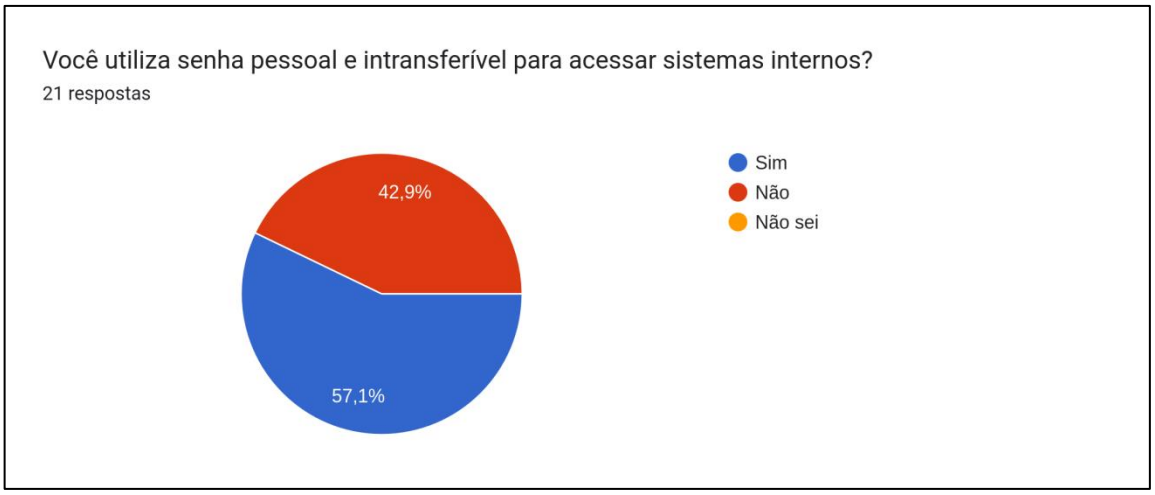
Gráfico 7 – Você sabe o que são dados pessoais segundo a LGPD?



Fonte: Grupo, 2026

85,7% dos colaboradores (18 de 21) afirmaram saber o que são dados pessoais conforme definido pela LGPD. Os 14,3% restantes (3 respondentes) responderam negativamente. O alto índice de conhecimento conceitual é um indicativo positivo, porém deve ser complementado pela aplicação prática desse entendimento no cotidiano do trabalho.

Gráfico 8 – Você utiliza senha pessoal e intransferível para acessar sistemas internos?



Fonte: Grupo, 2026

Apenas 57,1% dos colaboradores (12 de 21) afirmaram utilizar senha pessoal e intransferível para acessar os sistemas internos, enquanto 42,9% (9 respondentes) responderam negativamente. Esse resultado é preocupante e confirma o cenário identificado nas entrevistas: a ausência de senha individual nos computadores com sistema operacional Windows e a prática de senhas compartilhadas em alguns setores, como o Departamento Pessoal, impactam diretamente a segurança das informações e dificultam a rastreabilidade de acessos, deixando acessos genéricos nos logs.

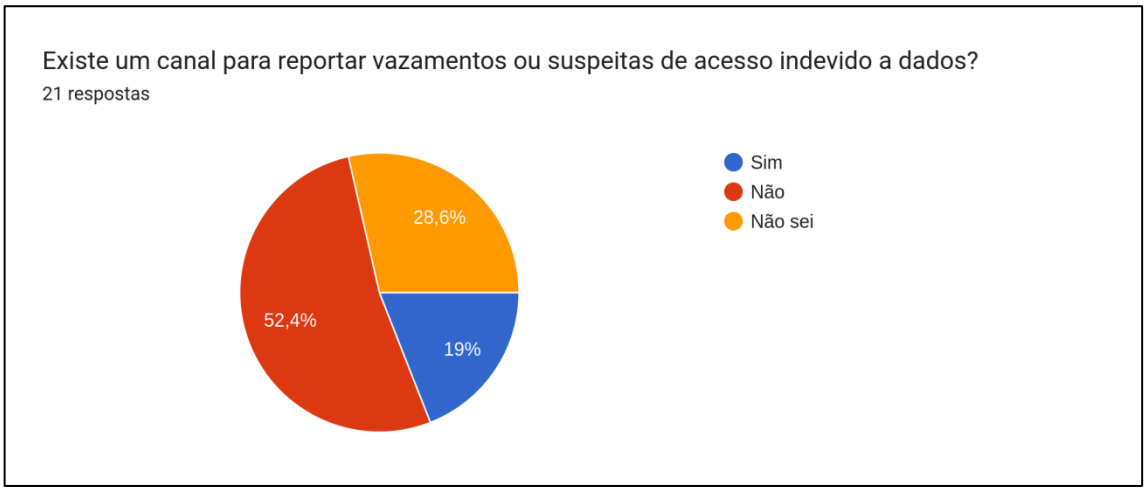
Gráfico 9 – Você tem acesso apenas às informações necessárias para o exercício da sua função?

Fonte: Grupo, 2026

85,7% dos colaboradores (18 de 21) responderam que têm acesso apenas às informações necessárias para o exercício de suas funções. Dois respondentes (9,5%)

declararam não saber e apenas 1 (4,8%) respondeu negativamente. Embora o índice positivo seja expressivo, é importante considerar que a percepção dos colaboradores pode diferir da realidade técnica do sistema: conforme identificado nas entrevistas, a segmentação de rede ainda está incompleta para os setores operacionais, e colaboradores podem não ter ciência do alcance real dos seus próprios acessos.

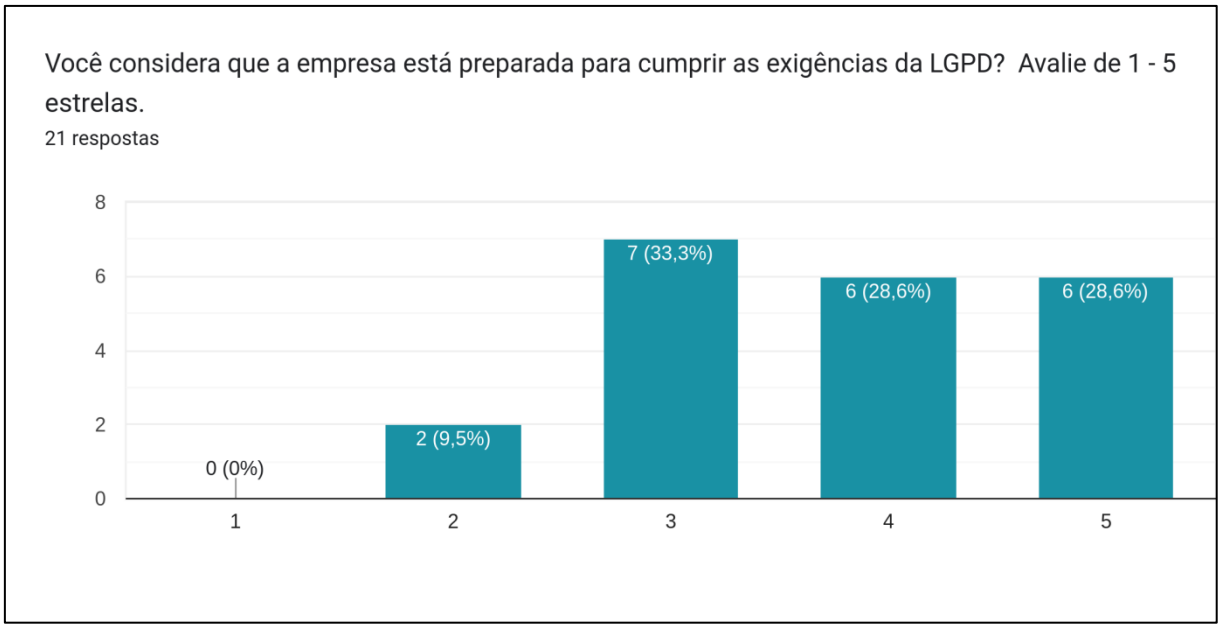
Gráfico 10 – Existe um canal para reportar vazamentos ou suspeitas de acesso indevido a dados?



Fonte: Grupo, 2026

Esta questão apresentou os resultados mais críticos do questionário: 52,4% dos colaboradores (11 de 21) responderam que não existe um canal para reportar vazamentos ou suspeitas de acesso indevido, 28,6% (6 respondentes) declararam não saber e apenas 19% (4 respondentes) afirmaram que tal canal existe. Esses dados revelam uma lacuna comunicacional relevante: mesmo que a empresa disponha de algum meio de reporte via e-mail ou WhatsApp, a grande maioria dos colaboradores desconhece essa possibilidade, o que compromete a efetividade do plano de resposta a incidentes.

Gráfico 11– Você considera que a empresa está preparada para cumprir as exigências da LGPD?

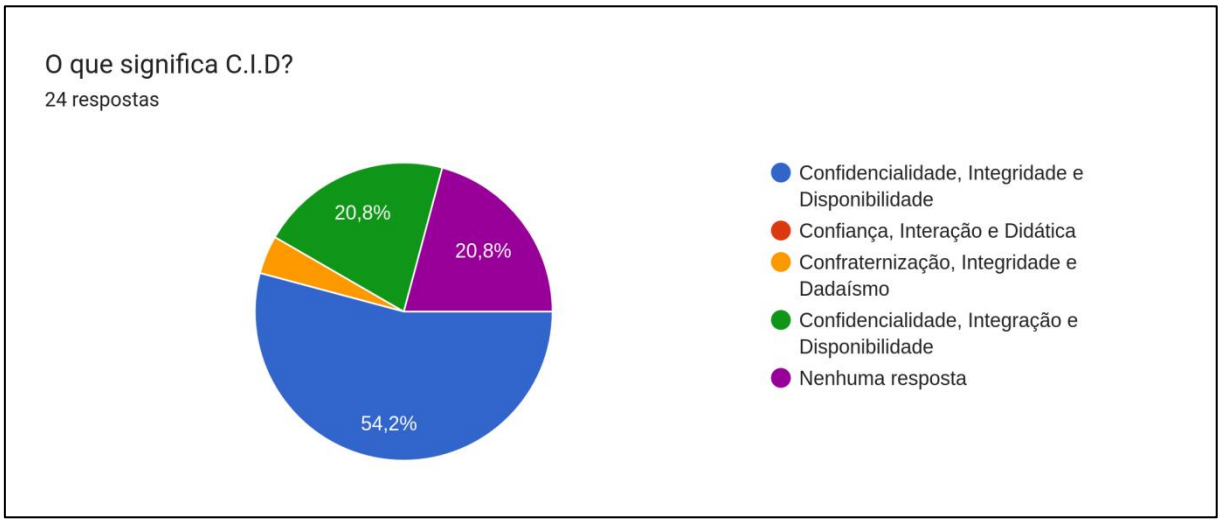


Fonte: Grupo, 2026

A avaliação média atribuída pelos colaboradores foi de 3,76 estrelas. A distribuição das notas foi a seguinte: 7 colaboradores (33,3%) atribuíram nota 3; 6 colaboradores (28,6%) atribuíram nota 4; 6 colaboradores (28,6%) atribuíram nota 5; e 2 colaboradores (9,5%) atribuíram nota 2. Nenhum colaborador atribuiu nota 1. A média levemente abaixo de 4 reflete uma percepção moderada sobre a maturidade da empresa em relação à conformidade com a LGPD, compatível com o cenário identificado nas entrevistas: existem boas práticas implementadas, mas ainda há lacunas relevantes a serem endereçadas.

4.3 Análise do Questionário Avaliativo

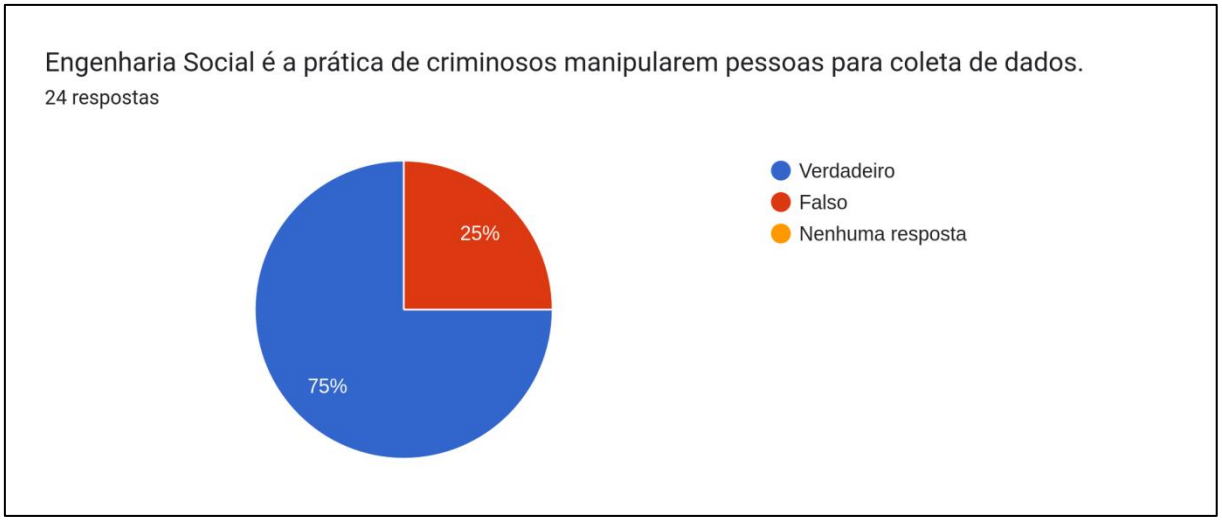
Gráfico 12 – O que significa C.I.D?



Fonte: Grupo, 2026

54,2% dos participantes (13 de 24) acertaram a questão, identificando corretamente que C.I.D representa Confidencialidade, Integridade e Disponibilidade. O erro mais frequente foi a confusão com a alternativa "Confidencialidade, Integração e Disponibilidade", escolhida por 5 participantes. Trata-se de um conceito fundamental da segurança da informação, e o índice de acertos abaixo de 60% indica que parte dos colaboradores ainda não assimilou plenamente a tríade CID, apesar de ela ter sido abordada na apresentação.

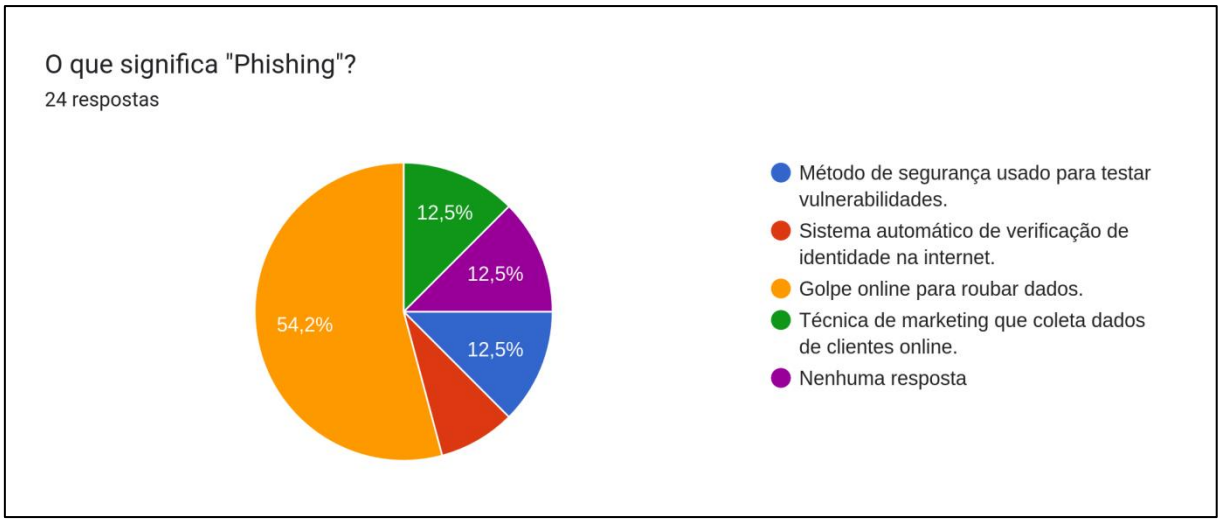
Gráfico 13 – Engenharia Social é a prática de criminosos manipularem pessoas para coleta de dados



Fonte: Grupo, 2026

75% dos participantes (18 de 24) responderam corretamente que a afirmativa é verdadeira. Os 6 participantes que erraram optaram por "Falso". O resultado indica um bom nível de compreensão sobre o conceito de Engenharia Social, especialmente relevante no contexto da empresa, que já relatou ter sofrido tentativas de golpes digitais que simulavam sites utilizados no cotidiano operacional.

Gráfico 14 – O que significa “Phishing”?

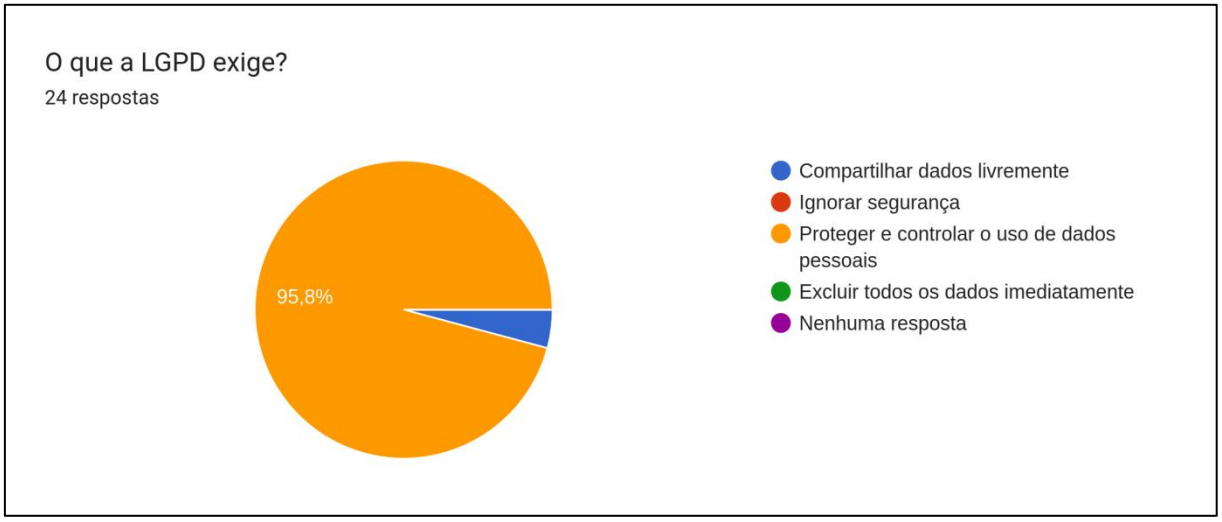


Fonte: Grupo, 2026

54,2% dos participantes (13 de 24) acertaram a questão, identificando Phishing como um golpe online para roubar dados. As alternativas incorretas dividiram os demais participantes entre "técnica de marketing" (3 respostas) e "método de

segurança para testar vulnerabilidades" (3 respostas). O índice de acertos idêntico ao da Questão 1 sugere que conceitos mais técnicos ainda demandam reforço, mesmo após a apresentação.

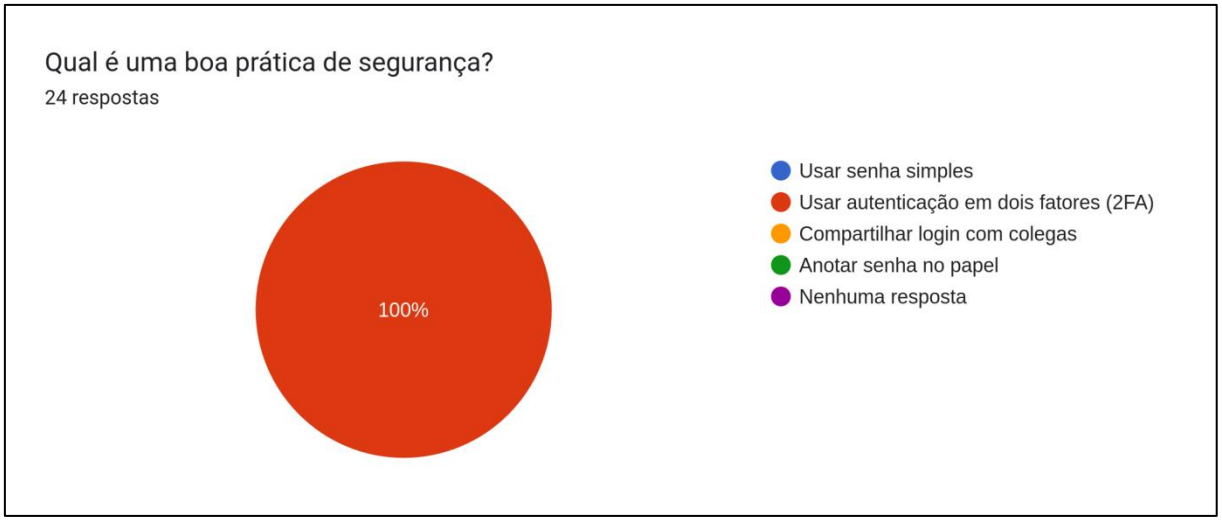
Gráfico 15 – O que a LGPD exige?



Fonte: Grupo, 2026

95,8% dos participantes (23 de 24) acertaram esta questão, reconhecendo que a LGPD exige proteger e controlar o uso de dados pessoais. Apenas 1 participante escolheu a alternativa incorreta "Compartilhar dados livremente". O altíssimo índice de acertos confirma que o objetivo central da lei é amplamente compreendido pelos colaboradores, o que é consistente com os resultados do questionário, onde 90,5% afirmaram conhecer a LGPD.

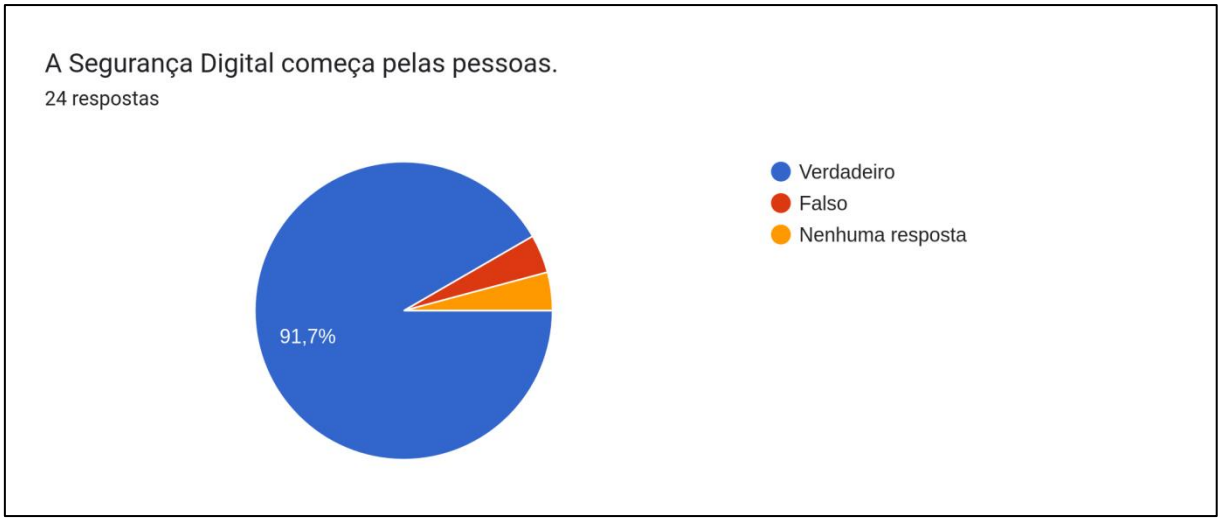
Gráfico 16 – Qual é uma boa prática de segurança?



Fonte: Grupo, 2026

Esta foi a única questão com 100% de acertos: todos os 24 participantes identificaram corretamente o uso de autenticação em dois fatores (2FA) como uma boa prática de segurança. O resultado é bastante positivo do ponto de vista da conscientização, embora contrastante com a realidade da empresa, onde a autenticação de dois fatores ainda não está implementada nos sistemas internos.

Gráfico 17 – A Segurança Digital começa pelas pessoas

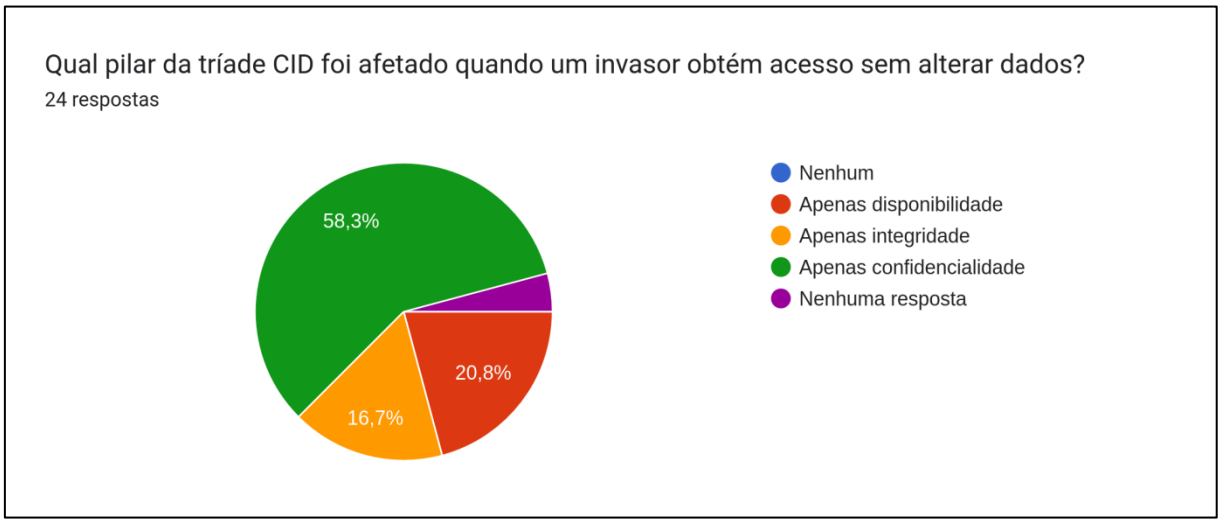


Fonte: Grupo, 2026

91,7% dos participantes (22 de 24) responderam corretamente que a afirmativa é verdadeira. Apenas 1 participante respondeu "Falso" e outro não respondeu. O resultado demonstra que os colaboradores compreendem que a segurança digital não

é responsabilidade exclusiva do setor de TI, mas de todos os envolvidos na organização.

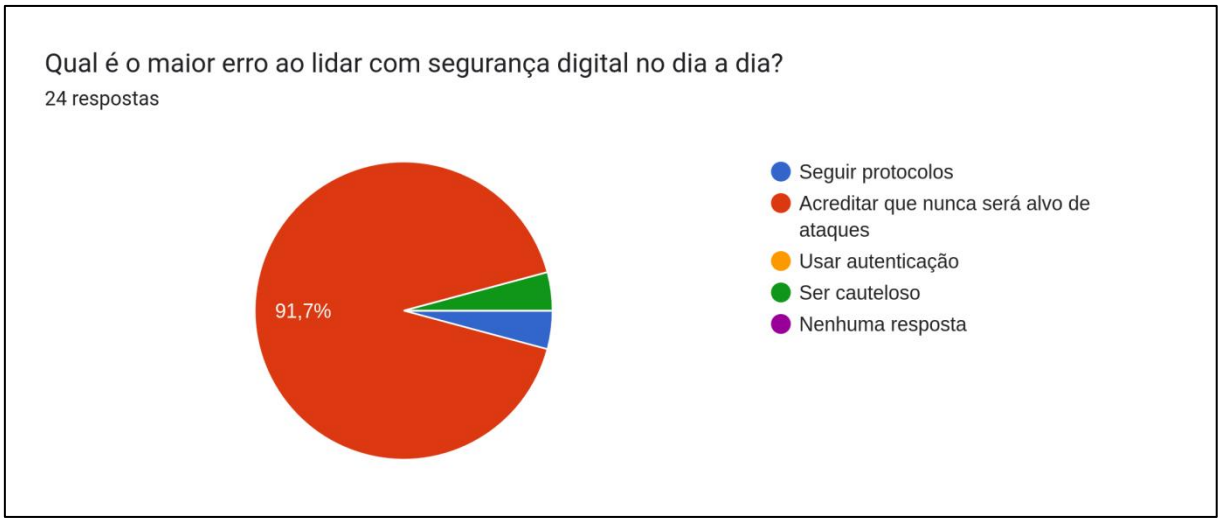
Gráfico 18 – Qual pilar da tríade CID foi afetado quando um invasor obtém acesso sem alterar dados?



Fonte: Grupo, 2026

58,3% dos participantes (14 de 24) acertaram a questão, identificando que apenas a Confidencialidade foi afetada. Os erros foram distribuídos entre "Apenas disponibilidade" (5 respostas) e "Apenas integridade" (4 respostas). A questão exigia uma compreensão mais aprofundada da tríade CID aplicada a cenários práticos, e o resultado evidencia que, embora o conceito seja conhecido, sua aplicação ainda gera dúvidas entre parte dos colaboradores.

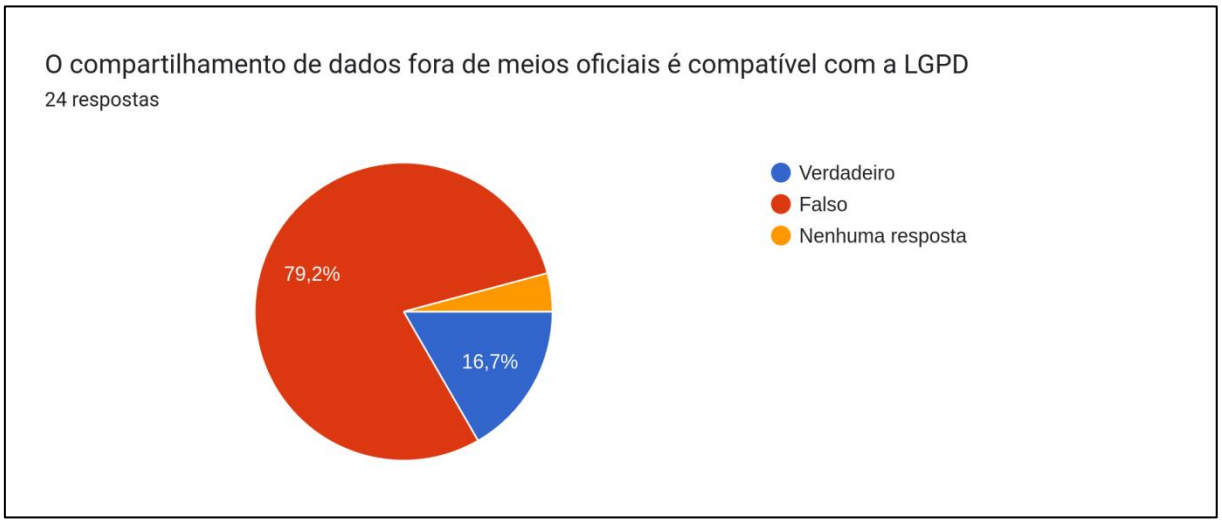
Gráfico 19 – Qual é o maior erro ao lidar com segurança digital no dia a dia?



Fonte: Grupo, 2026

91,7% dos participantes (22 de 24) identificaram corretamente que o maior erro é acreditar que nunca se será alvo de um ataque. Os dois participantes que erraram escolheram "Seguir protocolos" e "Ser cauteloso". O resultado é muito positivo e indica que os colaboradores têm consciência sobre a importância de não subestimar os riscos digitais, um comportamento crítico para a cultura de segurança da informação.

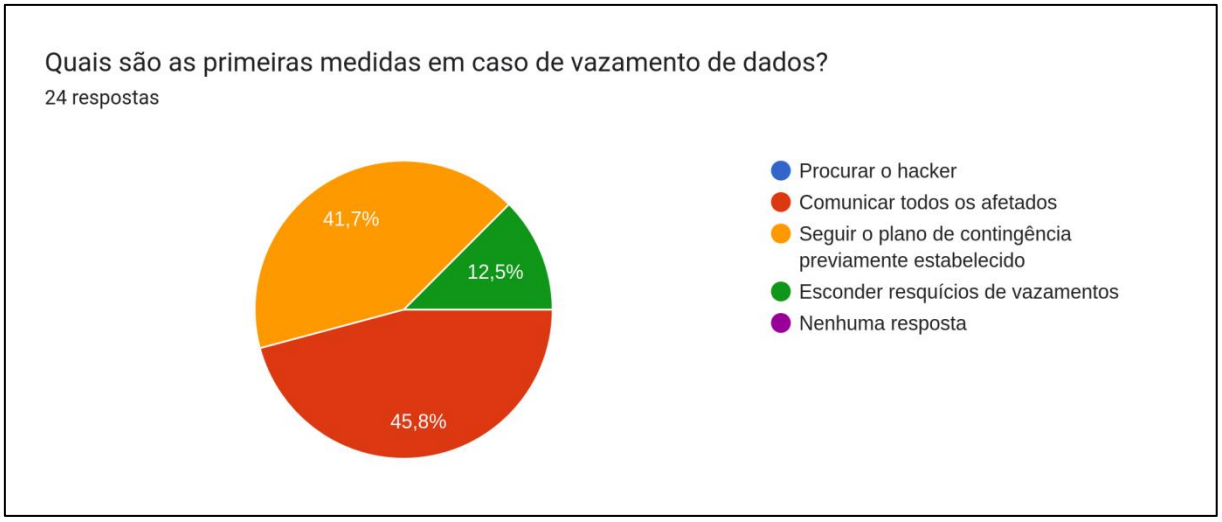
Gráfico 20 – O compartilhamento de dados de fora de meios oficiais é compatível com a LGPD



Fonte: Grupo, 2026

79,2% dos participantes (19 de 24) responderam corretamente que a afirmativa é falsa. Os 4 participantes que erraram responderam "Verdadeiro", indicando que ainda há uma parcela que acredita ser aceitável compartilhar dados fora dos canais oficiais. Esse ponto é especialmente relevante considerando que a empresa utiliza WhatsApp e e-mail como canais de comunicação com clientes, o que pode gerar ambiguidade sobre o que constitui um meio oficial ou não.

Gráfico 21 – Quais são as primeiras medidas em caso de vazamento de dados?



Fonte: Grupo, 2026

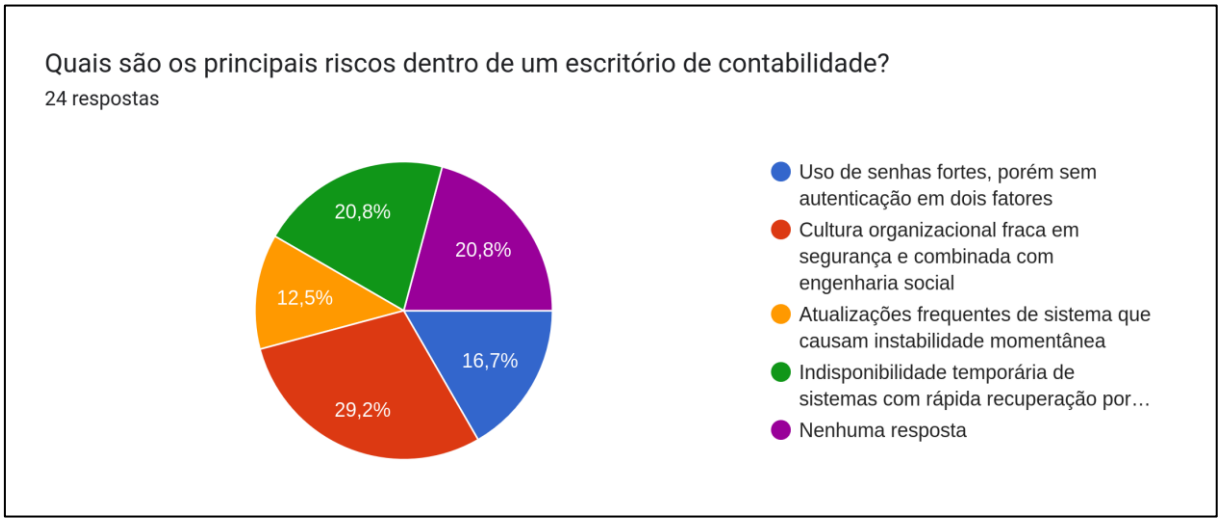
87,5% dos participantes (21 de 24) acertaram esta questão. As respostas corretas se dividiram entre "Comunicar todos os afetados" (11 respostas) e "Seguir o plano de contingência previamente estabelecido" (10 respostas), ambas consideradas corretas pelo contexto da questão. Os 3 participantes que erraram escolheram "Esconder resquícios de vazamentos". O alto índice de acertos demonstra que os colaboradores compreendem a importância da transparência e da adoção de protocolos formais diante de incidentes.

Gráfico 22 - – Quem é o responsável pela segurança no escritório?

Fonte: Grupo, 2026

83,3% dos participantes (20 de 24) responderam corretamente que todos os colaboradores são responsáveis pela segu rança no escritório. Três participantes escolheram "Apenas o TI" e 1 optou por "Apenas o dono". O resultado reforça a compreensão coletiva sobre a responsabilidade compartilhada pela segurança, consistente com o resultado da Questão 6.

Gráfico 23 – Quais são os principais riscos dentro de um escritório de contabilidade?



Fonte: Grupo, 2026

Esta foi a questão com menor índice de acertos do Kahoot: apenas 29,2% dos participantes (7 de 24) identificaram corretamente que o principal risco é a combinação de cultura organizacional fraca em segurança com engenharia social. As respostas foram bastante distribuídas entre as alternativas, com destaque para "Indisponibilidade temporária de sistemas com rápida recuperação por backup" (5 respostas) e "Uso de senhas fortes, porém sem autenticação em dois fatores" (4 respostas). O baixo índice de acertos indica que, embora os colaboradores conheçam boas práticas individuais, a compreensão sistêmica dos riscos organizacionais no contexto específico de um escritório contábil ainda é limitada e demanda aprofundamento.

4.4 Análise Geral dos Resultados

O questionário gamificado aplicado via Kahoot contou com a participação de 24 colaboradores e registrou uma média geral de 75% de respostas corretas, resultado considerado satisfatório para uma primeira aplicação. As questões com

melhor desempenho foram as de caráter mais direto, como a identificação de boas práticas de segurança (100% de acertos) e o conceito central da LGPD (95,8%). Em contrapartida, as questões que exigiam raciocínio aplicado obtiveram os menores índices: a identificação do pilar da tríade CID afetado em um cenário prático (58,3%) e, sobretudo, o reconhecimento dos principais riscos em um escritório contábil (29,2%), evidenciando que o conhecimento teórico ainda não se traduz plenamente em compreensão sistêmica.

A análise conjunta dos dados das entrevistas, formulário e do Kahoot permite traçar um panorama consistente sobre o nível de maturidade em segurança da informação e conformidade com a LGPD na empresa. De forma geral, os colaboradores demonstram bom conhecimento conceitual sobre a LGPD e seus objetivos, especialmente nos temas abordados diretamente nos treinamentos realizados. Por outro lado, questões que exigem aplicação prática apresentaram resultados mais baixos, sinalizando que esse conhecimento ainda não se traduziu completamente em comportamentos consistentes no dia a dia.

Os pontos de maior atenção identificados foram: o desconhecimento de um canal de reporte de incidentes por mais de 80% dos colaboradores; o uso de senhas não individuais por 42,9% dos respondentes; a circulação de visitantes sem controle percebida por 33,3% dos colaboradores; e o baixo índice de acertos na questão sobre riscos sistêmicos no Kahoot. Esses dados reforçam as lacunas identificadas nas entrevistas e apontam para a necessidade de ações concretas de melhoria, especialmente no que diz respeito à comunicação interna, políticas de acesso e periodicidade dos treinamentos.

4.5 Intervenção Proposta

O Plano de Intervenção foi elaborado com foco nas lacunas de maior criticidade identificadas ao longo da pesquisa, priorizando ações que impactam diretamente a conformidade com a LGPD e a segurança da informação. As ações propostas abrangem desde melhorias físicas no controle de acesso até a implementação de políticas formalizadas, a criação de canal de atendimento ao titular e a realização de simulações periódicas de incidentes.

A estrutura progressiva do plano, partindo de medidas de planejamento e documentação nas primeiras fases e avançando para controles técnicos, capacitação e monitoramento contínuo, está alinhada à lógica do ciclo PDCA recomendada pela

ISO/IEC 27001, que pressupõe planejamento, execução, verificação e ação corretiva como base para a maturidade em segurança da informação.

O plano foi apresentado à gestão ao término da pesquisa, que sinalizou que as propostas seriam discutidas internamente. Não houve, até o momento de conclusão deste trabalho, manifestação formal sobre quais ações seriam adotadas ou em qual prazo. Esse retorno, ainda que preliminar, demonstra abertura da organização ao tema e receptividade às propostas apresentadas.

5 CONSIDERAÇÕES FINAIS

O presente trabalho buscou compreender em que medida os processos e as práticas da empresa estudada estão alinhados aos requisitos da LGPD, com ênfase no setor de Recursos Humanos. O diagnóstico produzido permite concluir que a organização se encontra em estágio de conformidade parcial, no qual boas práticas já consolidadas coexistem com lacunas que ainda precisam ser endereçadas.

Os objetivos estabelecidos para esta pesquisa foram integralmente alcançados. O levantamento do nível de conhecimento dos colaboradores sobre a LGPD foi realizado por meio do formulário e do Kahoot; o treinamento em segurança digital e LGPD foi conduzido e permitiu identificar as principais lacunas de conhecimento; e a proposta de intervenção foi elaborada e entregue à gestão com base na síntese de todos os resultados obtidos.

Os achados confirmaram, em graus distintos, as três hipóteses formuladas. Ficou evidente que o conhecimento sobre a LGPD, por si só, não garante comportamentos seguros no dia a dia, o que reforça a necessidade de uma cultura de proteção de dados construída de forma contínua. As fragilidades nos controles de acesso e na formalização de políticas internas confirmam que vulnerabilidades estruturais aumentam os riscos de não conformidade. Ao mesmo tempo, os resultados positivos da capacitação realizada mostraram que, quando os treinamentos são bem conduzidos, produzem efeitos concretos e mensuráveis.

Em termos de contribuições práticas, o estudo resultou na realização de uma capacitação em segurança digital e LGPD com os colaboradores e na entrega de um Plano de Intervenção com oito ações estruturadas ao longo de doze meses, ambos fundamentados nos achados da pesquisa e nos princípios da LGPD e da norma ABNT NBR ISO/IEC 27001:2022, oferecendo à organização um caminho concreto de adequação.

Como limitação, o recorte a uma única empresa impede que os resultados sejam generalizados para o setor contábil como um todo. A ausência de retorno formal sobre a implementação do plano também limitou a avaliação dos seus efeitos práticos. Para estudos futuros, recomenda-se pesquisas comparativas entre organizações do mesmo segmento e o acompanhamento longitudinal da empresa, a fim de verificar os avanços obtidos após a implementação das ações propostas.

Por fim, a adequação à LGPD não se resume à adoção de ferramentas ou documentos. É um processo contínuo, que depende de comprometimento da gestão

e de uma cultura organizacional voltada à proteção de dados. A abertura demonstrada pela empresa ao longo desta pesquisa indica que esse caminho, embora ainda em construção, já teve seu primeiro passo dado.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022: segurança da informação, segurança cibernética e proteção à privacidade — sistemas de gestão da segurança da informação — requisitos. Versão corrigida. Rio de Janeiro: ABNT, 2023.

ALBERTIN, A. L. Valor Estratégico dos projetos de tecnologia de informação. RAE – Revista de Administração de Empresas. Jul/Set. 2001. São Paulo, v. 41, p. 42-50 [Entrada removida: referência duplicada à versão 2013, substituída pela entrada única da versão 2022 acima.]

BARCELOS, Enio Marcos Babireski; ROSA, Mariana Pegoraro; BRAGA, Rodrigo Julio. A relação das áreas de tecnologia da informação e recursos humanos nas organizações. Conhecimento Interativo, São José dos Pinhais, 2008.

Bergson Lopes Rego. Gestão e Governança de Dados: promovendo dados como ativo de valor nas empresas. Rio de Janeiro: Brasport, 2013.

BIOGRAFIA – Danilo Doneda. Disponível em: https://doneda.net/biografia. Acesso em: 7 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

CARVALHO, Alexandre. O novo (e atraente) departamento pessoal. Você RH, fev./mar. 2026.

CHIAVENATO, Idalberto. Gestão de pessoas: o novo papel da gestão do talento humano. 5. ed. São Paulo: GEN Atlas, 2022.

CHIAVENATO, Idalberto. Gestão de pessoas: o novo papel dos recursos humanos nas organizações. 4. ed. Barueri: Manole, 2014.

COSTA, Tatiana Ribeiro da. E-RH: o impacto da tecnologia para a gestão competitiva de recursos humanos. São Paulo: Universidade de São Paulo, 2005.

DAMA International. DAMA-DMBOK: Guia para o corpo de conhecimento de gestão de dados. 2. ed. [S. l.]: Technics Publications, 2017

DONDA, Daniel. Guia prático de implementação da LGPD. São Paulo: Labrador, 2020

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020.

GESTÃO DE PESSOAS. Os subsistemas do RH. Blog Gestão de Pessoas, 13 maio 2014. Disponível em: https://gestaodepessoasbmln.blogspot.com/2014/05/os-subsistema-do-rh.html. Acesso em: 10 mar. 2026.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

HOLMES, Hélio. Departamento pessoal: da rotina à gestão estratégica. Maringá: Viseu, 2019.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: Editora UFPB, 2019.

MENDES, R. R. et al. Uma metodologia para implantação de um Sistema de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002. Revista Principia, João Pessoa, n. 22, p. 69-80, 2013.

NUNAN, Angelo Eduardo; COSTA FILHO, Mário José de Moraes; LIMA, Adriana Almeida. Implantação da segurança na gestão da informação na administração pública: um estudo de caso no Tribunal de Contas do Estado do Amazonas. Revista do Serviço Público, Brasília, v. 67, n. 1, p. 109-130, jan./mar. 2016.

ONE moment, please... Disponível em: https://digitaldefynd.com/IQ/inspirational-cybersecurity-quotes/. Acesso em: 8 jun. 2026.

O QUE muda com a LGPD — LGPD - Lei Geral de Proteção de Dados Pessoais | Serpro. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 9 abr. 2026.

PROTEÇÃO de dados é um direito fundamental que baliza a democracia - Jurista Laura Schertel Mendes. 14 maio 2020. 1 vídeo (23 min 51 s). Publicado pelo canal Escola Superior do MPU. Disponível em: https://www.youtube.com/watch?v=QuvhHxL6hNA. Acesso em: 09 abr. 2026.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

APÊNDICES

APÊNDICE A – Questionário Aplicado aos Colaboradores

O questionário a seguir foi aplicado aos colaboradores da empresa com o objetivo de coletar dados sobre a percepção dos funcionários em relação às práticas de segurança da informação e conformidade com a LGPD adotadas pela organização.

1) **Você utiliza crachá ou algum meio de identificação fornecido pela empresa?**
2) **Visitantes recebem identificação (crachá de visitante, registro em livro ou recepção) e são registrados ao entrar nas dependências?**
3) **Você considera que o acesso às informações internas é devidamente restrito?**
4) **Você já recebeu algum treinamento, orientação ou comunicado da empresa sobre a LGPD e boas práticas de proteção de dados pessoais?**
5) **Você já presenciou visitantes circulando livremente em áreas com computadores ou documentos com dados pessoais?**
6) **Você conhece a LGPD (Lei nº 13.709/2018)?**
7) **Você sabe o que são dados pessoais segundo a LGPD (Lei nº 13.709/2018)?**
8) **Você utiliza senha pessoal e intransferível para acessar sistemas internos?**
9) **Você tem acesso apenas às informações necessárias para o exercício da sua função?**
10) **Existe um canal para reportar vazamentos ou suspeitas de acesso indevido a dados?**
11) **Você considera que a empresa está preparada para cumprir as exigências da LGPD? Avalie de 1 a 5 estrelas.**

APÊNDICE B – Questões Aplicadas no Kahoot

As questões a seguir foram elaboradas pela equipe e aplicadas por meio da plataforma Kahoot ao término da apresentação sobre segurança digital e LGPD, realizada no dia 28 de abril de 2026. O questionário contou com a participação de 24 colaboradores e obteve 75% de acertos no geral.

1. **O que significa C.I.D?**
   a) Confidencialidade, Integridade e Disponibilidade
   b) Confiança, Interação e Didática
   c) Confraternização, Integridade e Dadaísmo
   d) Confidencialidade, Integração e Disponibilidade

2. **Engenharia Social é a prática de criminosos manipularem pessoas para a coleta de dados e informações pessoais.**
   a) Verdadeiro
   b) Falso

3. **O que significa "Phishing"?**
   a) Golpe online para roubar dados
   b) Técnica de marketing que coleta dados de clientes online
   c) Método de segurança usado para testar vulnerabilidades
   d) Sistema automático de verificação de identidade na internet

4. **O que a LGPD exige?**
   a) Proteger e controlar o uso de dados pessoais
   b) Compartilhar dados livremente
   c) Armazenar todos os dados dos clientes indefinidamente
   d) Divulgar informações pessoais apenas por e-mail

5. **Qual é uma boa prática de segurança?**
   a) Usar autenticação em dois fatores (2FA)

b) Compartilhar senhas com colegas de confiança
c) Usar a mesma senha para todos os sistemas
d) Desativar o antivírus para maior velocidade

6. **A Segurança Digital começa pelas pessoas.**
   a) Verdadeiro
   b) Falso

7. **Um invasor obtém acesso, mas não altera nem vaza dados. Qual pilar da tríade foi afetado?**
   a) Apenas confidencialidade
   b) Apenas integridade
   c) Apenas disponibilidade
   d) Todos os pilares

8. **Qual é o maior erro ao lidar com segurança digital no dia a dia?**
   a) Acreditar que nunca será alvo de ataque
   b) Ser cauteloso
   c) Seguir protocolos
   d) Usar senhas fortes

9. **O compartilhamento de dados fora de meios oficiais é compatível com a LGPD e facilita o trabalho.**
   a) Verdadeiro
   b) Falso

10. **Quais são as primeiras medidas que se deve tomar em caso de vazamento de dados?**
    a) Seguir o plano de contingência previamente estabelecido
    b) Comunicar todos os afetados
    c) Esconder resquícios de vazamentos
    d) Ignorar e aguardar resolução espontânea

11. Quem é responsável pela segurança no escritório?

a) Todos os colaboradores
b) Apenas o TI
c) Apenas o dono
d) Apenas o gestor de RH

12. Quais são os principais riscos dentro de um escritório de contabilidade?

a) Cultura organizacional fraca em segurança combinada com engenharia social
b) Uso de senhas fortes, porém sem autenticação em dois fatores
c) Indisponibilidade temporária de sistemas com rápida recuperação por backup
d) Atualizações frequentes de sistema que causam instabilidade momentânea

APÊNDICE C – Checklists Aplicados

Tabela X – Checklist de Conformidade com LGPD e ISO 27001 em Empresa de Contabilidade

Nº	Categoria	Item de Verificação	Status	Evidência	Responsável
1	Controle de Acesso	Funcionários utilizam crachá de identificação			
2	Controle de Acesso	Existe controle de entrada/saída de pessoas			
3	Controle de Acesso	Computadores possuem login individual			
4	Controle de Acesso	Há política de senhas definida			
5	Controle de Acesso	Acessos são removidos após desligamento			
6	Níveis de Acesso	Sistemas possuem acesso por perfil (RBAC)			
7	Níveis de Acesso	Usuários acessam apenas o necessário (menor privilégio)			
8	Níveis de Acesso	Existe segregação de funções			
9	Níveis de Acesso	Há registro de logs de acesso			
10	Níveis de Acesso	Acessos são revisados periodicamente			
11	Níveis de Acesso	Existe autenticação em dois fatores (2FA)			
12	Segurança da Informação	Existe política de segurança formal			
13	Segurança da Informação	Funcionários recebem treinamento			
14	Segurança da Informação	Há antivírus e firewall ativos			
15	Segurança da Informação	Sistemas são atualizados regularmente			
16	Segurança da Informação	Existe backup dos dados			
17	Segurança da Informação	Backup é testado periodicamente			
18	LGPD	A empresa sabe quais dados coleta			
19	LGPD	Existe base legal para tratamento de dados			
20	LGPD	Há política de privacidade documentada			
21	LGPD	Dados são armazenados com segurança			

Checklist LGPD — Analista de Recursos Humanos

Lei nº 13.709/2018 | Etec de Cubatão — Curso Técnico de Informática

Empresa / Setor:	Data:
Responsável:	Cargo:

Objetivo

Verificar se o setor de Recursos Humanos adota as práticas exigidas pela LGPD para a proteção de dados pessoais de colaboradores, candidatos e terceiros. Marque cada item conforme a situação identificada na empresa.

Como preencher

Como preencher	Descrição
Sim / Conforme	O critério é atendido pela empresa.
Não / Não Conforme	O critério NÃO é atendido — requer ação corretiva.
Parcial / Em Adequação	Atendido parcialmente — em processo de melhoria.
N/A	Não se aplica ao contexto da empresa.
EXTRA	Pergunta adicional recomendada para maior completude.

Perguntas — RH

Nº	OK?	Pergunta / Critério	Base Legal LGPD
Proteção de Dados Pessoais — Setor de RH (Perguntas originais)			
6		Os documentos físicos contendo dados pessoais ficam em local com acesso restrito (arquivo trancado, sala fechada)?	
7		Visitantes ou clientes têm acesso visual ou físico a documentos ou telas com dados de colaboradores?	
8		Existe registro de terceiros (técnicos de TI, manutenção, prestadores) que acessam áreas com informações sensíveis?	
9		Os colaboradores recebem orientação para bloquear a tela do computador ao se ausentarem?	
10		Há termo de confidencialidade assinado por prestadores de serviço que possam ter contato com dados pessoais?	
Perguntas Extras Originais (A e B)			
A		**Os dados pessoais de candidatos (currículos, testes) são descartados de forma segura após o processo seletivo? [EXTRA]**	Art. 16
B		**Existe uma política clara de retenção e descarte de documentos com dados de ex-colaboradores? [EXTRA]**	Art. 15 e 16
Novas Questões Recomendadas (11, 12 e 13)			
11		**O setor de RH possui base legal definida e documentada para cada tipo de tratamento de dados realizado (ex: consentimento para currículos, obrigação legal para dados de folha de pagamento)? [NOVO]**	Art. 7º

Checklist LGPD

Setor de TI — Segurança da Informação e Acesso — Lei nº 13.709/2018

Empresa / Setor:		**Data:**	
Responsável:		**Cargo:**	

Objetivo

Verificar se o setor de Tecnologia da Informação adota as práticas exigidas pela LGPD para controle de acesso, segurança dos sistemas e proteção dos dados pessoais armazenados e processados pela empresa. Marque cada item conforme a situação identificada.

Como preencher

Sim / Conforme	O critério é atendido pela empresa.
Não / Não Conforme	O critério NÃO é atendido — requer ação corretiva.
Parcial / Em Adequação	Atendido parcialmente — em processo de melhoria.
N/A	Não se aplica ao contexto da empresa.
EXTRA	Pergunta adicional recomendada para maior completude.

Segurança da Informação e Controle de Acesso — Setor de TI

Perguntas 11 a 15 (obrigatórias) + Perguntas C e D (extras recomendadas)

Nº	OK?	Pergunta / Critério
11		Existe controle de acesso individual aos sistemas (login e senha pessoal e intransferível)?
12		Há níveis de permissão restritos conforme a função do colaborador?
13		O ambiente onde ficam servidores ou equipamentos de rede possui acesso físico controlado?
14		É realizado registro (log) de acessos aos sistemas que armazenam dados sensíveis?
15		Técnicos externos que realizam manutenção possuem supervisão ou acesso temporário controlado aos sistemas?
C		Os sistemas e dispositivos possuem antivírus, firewall e atualizações de segurança em dia? **EXTRA**
D		Existe um processo definido para revogar acessos imediatamente quando um colaborador é desligado? **EXTRA**

APÊNDICE D – Proposta de Intervenção

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA

ESCOLA TÉCNICA DE CUBATÃO

Curso Técnico em Informática

Eric Vieira dos Santos

Larissa Cavalcante dos Santos

Oswaldo Leite Santos Grillo

Ryan Ferreira da Silva

PLANO DE INTERVENÇÃO PARA ADEQUAÇÃO À LGPD EM EMPRESA COM SEGMENTO NA ÁREA CONTÁBIL, LOCALIZADA EM SANTOS

Cubatão

2026

Eric Vieira dos Santos

Larissa Cavalcante dos Santos

Oswaldo Leite Santos Grillo

Ryan Ferreira da Silva

PLANO DE INTERVENÇÃO PARA ADEQUAÇÃO À LGPD EM EMPRESA COM SEGMENTO NA ÁREA CONTÁBIL, LOCALIZADA EM SANTOS

Plano de Intervenção elaborado como parte integrante do Trabalho de Conclusão de Curso do Curso Técnico em Informática da Etec de Cubatão, orientado pelo Prof. Marcelo Batista Onuki, como requisito parcial para obtenção do título de Técnico em Informática.

Cubatão

2026

1. APRESENTAÇÃO

O presente Plano de Intervenção integra o Trabalho de Conclusão de Curso realizado pelo grupo em empresa com segmento na área contábil, localizada em Santos/SP. O objetivo é propor ações concretas e aplicáveis para a adequação da organização às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD — Lei n.º 13.709/2018), com base nas não conformidades identificadas ao longo do processo de pesquisa.

A pesquisa contemplou entrevistas semiestruturadas com o sócio-administrador e com os responsáveis pelos setores de Recursos Humanos e Tecnologia da Informação, além da aplicação de formulário aos colaboradores e de questionário avaliativo gamificado via plataforma Kahoot. Os instrumentos foram elaborados com base nos princípios da LGPD e nos requisitos da norma ABNT NBR ISO/IEC 27001:2022 (ABNT, 2022).

As intervenções propostas neste documento estão alinhadas ao diagnóstico produzido e têm como foco as áreas de maior vulnerabilidade identificadas na empresa: controle de acesso físico, gestão de credenciais, comunicação interna sobre privacidade, capacitação dos colaboradores e resposta a incidentes.

2. DIAGNÓSTICO

Os resultados obtidos por meio dos instrumentos de pesquisa aplicados na empresa revelaram um cenário de conformidade parcial com a LGPD. Embora a organização apresente boas práticas em algumas áreas, como o reconhecimento da importância da segurança digital pelos colaboradores (91,7% entendem que a segurança começa pelas pessoas) e o alto índice de acertos sobre o objetivo central da LGPD (95,8%), foram identificadas lacunas relevantes que exigem atenção.

As principais não conformidades detectadas foram:

- Ausência de identificação formal dos colaboradores por meio de crachás: 76,2% dos respondentes confirmaram não utilizar nenhum meio de identificação fornecido pela empresa.
- Controle insuficiente de visitantes: 76,2% indicaram que visitantes não recebem identificação formal ao ingressar nas dependências, e 33,3% relataram já ter presenciado visitantes circulando livremente em áreas com dados pessoais.

- Uso de senhas compartilhadas: 42,9% dos colaboradores afirmaram não utilizar senha pessoal e intransferível para acesso aos sistemas internos.
- Desconhecimento do canal de reporte de incidentes: 52,4% dos colaboradores declararam não existir canal para reportar suspeitas de vazamento, e 28,6% afirmaram desconhecer sua existência.
- Ausência de autenticação de dois fatores nos sistemas internos, mesmo com 100% dos colaboradores reconhecendo o 2FA como boa prática.
- Baixo índice de acertos (29,2%) na questão sobre riscos sistêmicos específicos de escritórios contábeis, indicando que o conhecimento teórico ainda não se traduziu em compreensão prática do ambiente.
- Ausência de políticas formalizadas de senhas, segurança da informação e privacidade.
- Inexistência de simulações de incidentes de segurança e de testes periódicos de phishing e engenharia social.

Esses dados fundamentam diretamente as ações propostas nas seções seguintes.

3. OBJETIVOS DA INTERVENÇÃO

O presente plano tem como objetivo geral contribuir para a adequação da empresa às exigências da LGPD, reduzindo as vulnerabilidades identificadas no diagnóstico e fortalecendo a cultura de proteção de dados na organização.

São objetivos específicos:

- Propor melhorias nos controles físicos de acesso às dependências da empresa.
- Estabelecer cláusula contratual que impeça a retenção de dados organizacionais em dispositivos pessoais após desligamento.
- Formalizar canal de atendimento às solicitações dos titulares de dados pessoais.
- Implantar sistema rigoroso de registro de entrada e saída de colaboradores e visitantes.
- Publicar e implementar política formalizada de senhas.
- Elaborar e divulgar política de segurança da informação.

- Realizar simulações periódicas de incidentes de vazamento de dados.
- Implementar programa de testes regulares de phishing e engenharia social.

4. AÇÕES DE INTERVENÇÃO

As ações descritas a seguir foram organizadas por área temática, com indicação das medidas propostas, fundamentos legais aplicáveis e responsáveis sugeridos para a implementação.

4.1. Melhorias nas Estruturas Físicas

Fundamento legal: Art. 46 da LGPD, que determina a adoção de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados.

O diagnóstico revelou que visitantes circulam sem identificação formal e que parte dos colaboradores não porta meio de identificação. O controle físico do ambiente é o primeiro perímetro de proteção de dados pessoais.

Medidas propostas:

- Implantação de crachás de identificação obrigatória para todos os colaboradores, com diferenciação visual por setor.
- Adoção de crachás de visitante com número de série, preenchidos na recepção e devolvidos na saída.
- Instalação de travas de acesso com controle por crachá ou biometria em salas com dados sensíveis.
- Reforço do acompanhamento obrigatório de visitantes por colaborador responsável em todas as dependências.
- Aplicação de política de mesa limpa e tela limpa, proibindo a exposição de dados pessoais em ambientes visíveis a terceiros não autorizados.
- Posicionamento de monitores de forma a impedir a visualização por visitantes.

Responsável sugerido: Sócio-administrador e gestão operacional.

4.2. Aditivo Contratual sobre Dispositivos Pessoais após Desligamento

Fundamento legal: Art. 46 e Art. 48 da LGPD, além das disposições gerais sobre responsabilidade dos agentes de tratamento.

A inexistência de cláusula contratual específica sobre a proibição de retenção de dados organizacionais em dispositivos pessoais cria vulnerabilidade jurídica e operacional após o encerramento dos vínculos empregatícios.

Medidas propostas:

- Elaboração de aditivo contratual, com assessoria jurídica, vedando expressamente a retenção, cópia ou transferência de dados pessoais de clientes, colaboradores e da organização para dispositivos pessoais.
- Instituição de procedimento formal de verificação e comprovação de exclusão de dados no ato do desligamento, com assinatura de termo pelo colaborador.
- Inclusão de cláusula de confidencialidade com vigência após o término do vínculo.
- Assinatura de termo de ciência e responsabilidade no momento da admissão.

Responsável sugerido: Assessoria jurídica contratada e setor de Recursos Humanos.

4.3. Canal de Ouvidoria e Atendimento ao Titular

Fundamento legal: Art. 18 da LGPD, que assegura ao titular de dados os direitos de acesso, correção, eliminação, portabilidade e revogação do consentimento, entre outros. Art. 41, que prevê a designação de Encarregado de Proteção de Dados.

O diagnóstico evidenciou que mais de 80% dos colaboradores desconhecem a existência de canal para reporte de incidentes. A ausência de canal formal de ouvidoria compromete tanto o atendimento aos titulares quanto a capacidade de resposta a incidentes.

Medidas propostas:

- Criação de endereço de e-mail institucional dedicado ao atendimento de solicitações de titulares de dados, com divulgação interna e no site da empresa.

- Designação de Encarregado de Proteção de Dados (DPO), conforme Art. 41 da LGPD, podendo ser um colaborador interno capacitado ou profissional externo.
- Elaboração de procedimento interno de atendimento com prazo de resposta de até 15 dias, em consonância com as orientações da ANPD.
- Comunicação formal do canal a todos os colaboradores e clientes.

Responsável sugerido: DPO designado e gestão administrativa.

4.4. Controle de Registro de Entrada e Saída

Fundamento legal: Art. 46 da LGPD. Princípio da segurança (Art. 6º, VII) e responsabilização (Art. 6º, X).

O registro precário de entrada e saída, aliado à circulação descontrolada de visitantes identificada no diagnóstico, aumenta o risco de acesso não autorizado a dados pessoais nas dependências da empresa.

Medidas propostas:

- Implantação de sistema eletrônico de controle de ponto para colaboradores, por meio de biometria ou cartão de acesso.
- Adoção de livro de registro digitalizado ou sistema para controle de visitantes e prestadores de serviço, com registro de nome, documento, data, horário e motivo da visita.
- Reforço da política de acompanhamento obrigatório de visitantes por colaborador responsável durante toda a permanência.
- Restrição formal de acesso de terceiros a áreas com equipamentos ou documentos contendo dados pessoais.

Responsável sugerido: Recepção e sócio-administrador.

4.5. Política de Senhas

Fundamento legal: Art. 46 da LGPD. Controles 5.15 (Controle de acesso), 5.16 (Gestão de identidade) e 8.2 (Direitos de acessos privilegiados) da ABNT NBR ISO/IEC 27001:2022 (ABNT, 2022).

O diagnóstico apontou que 42,9% dos colaboradores não utilizam senha pessoal e intransferível. Embora 100% reconheçam a autenticação de dois fatores

como boa prática, ela não está implementada nos sistemas internos. A gestão de credenciais inadequada é uma das principais causas de incidentes de segurança.

Medidas propostas:

- Publicação formal de Política de Senhas estabelecendo: mínimo de 12 caracteres, combinação de letras maiúsculas, minúsculas, números e caracteres especiais.
- Obrigatoriedade de troca de senhas a cada 90 dias, com proibição de reutilização das cinco últimas.
- Implementação de autenticação de dois fatores (2FA) para acesso a sistemas críticos e e-mails corporativos.
- Vedação expressa ao compartilhamento de credenciais entre colaboradores.
- Adoção de gerenciador de senhas corporativo.
- Treinamento obrigatório sobre a política na admissão e a cada 12 meses.

Responsável sugerido: Setor de TI e sócio-administrador.

4.6. Política de Segurança da Informação

Fundamento legal: Art. 46 e Art. 48 da LGPD. Controles 5.24 (Planejamento de gestão de incidentes), 5.25 (Avaliação de eventos), 5.26 (Resposta a incidentes) e 5.27 (Aprendizado com incidentes) da ABNT NBR ISO/IEC 27001:2022 (ABNT, 2022).

A ausência de política formalizada de segurança da informação foi identificada tanto nas entrevistas quanto nos resultados do formulário. A formalização desse instrumento é condição essencial para a consolidação de uma cultura de proteção de dados.

Medidas propostas:

- Elaboração de Política de Segurança da Informação (PSI) abrangendo: classificação da informação, controle de acesso lógico e físico, uso aceitável de recursos tecnológicos, gestão de ativos, backup e recuperação, e política de dispositivos móveis.
- Elaboração de Política de Privacidade alinhada à LGPD, a ser disponibilizada no site institucional.

- Mapeamento dos fluxos de tratamento de dados pessoais da organização (ROPA — Record of Processing Activities).
- Treinamento obrigatório sobre a PSI para todos os colaboradores, com atualização anual.
- Aprovação e assinatura formal pela alta direção, conferindo caráter normativo aos documentos.

Responsável sugerido: DPO, setor de TI e sócio-administrador.

4.7. Simulações de Vazamento de Dados

Fundamento legal: Art. 46 e Art. 48 da LGPD. ABNT NBR ISO/IEC 27035 — Gestão de incidentes de segurança da informação.

Nenhuma simulação de incidente havia sido realizada até o momento do diagnóstico. A ausência de exercícios práticos compromete a capacidade de resposta da organização diante de situações reais.

Medidas propostas:

- Elaboração de Plano de Resposta a Incidentes (PRI) com definição de papéis, responsabilidades e procedimentos.
- Realização de simulações semestrais de incidentes de vazamento de dados, com cenários distintos a cada edição.
- Documentação de cada simulação com registro de data, cenário, participantes, falhas identificadas e ações corretivas tomadas.
- Comunicação dos resultados à equipe para promover aprendizagem organizacional contínua.

Responsável sugerido: DPO e setor de TI.

4.8. Testes de Phishing e Engenharia Social

Fundamento legal: Art. 46 da LGPD. Princípios da prevenção e da segurança (Art. 6º, VII e VIII).

O diagnóstico revelou que, embora 75% dos colaboradores tenham reconhecido a engenharia social como ameaça e 54,2% identifiquem corretamente o conceito de phishing, a empresa nunca realizou testes práticos de resistência a essas

ameaças. A empresa já relatou ter sofrido tentativas de golpes que simulavam sites utilizados no cotidiano operacional, o que torna essa intervenção prioritária.

Medidas propostas:

- Implementação de programa de testes semanais de phishing simulado, com uso de plataforma especializada, avaliando a capacidade dos colaboradores de identificar e reportar tentativas.
- Realização periódica de simulações de engenharia social presencial e telefônica (vishing).
- Registro e análise dos resultados de cada teste, identificando setores e perfis de maior vulnerabilidade.
- Treinamento específico e imediato para colaboradores que interagirem com os cenários simulados.
- Produção de relatório mensal consolidando os resultados, com indicadores de evolução, encaminhado à liderança.

Responsável sugerido: Setor de TI e DPO.

5. CRONOGRAMA DE IMPLEMENTAÇÃO

O cronograma a seguir organiza as ações em quatro fases ao longo de 12 meses, priorizando as medidas de maior impacto imediato.

FASE 1 (Meses 1 e 2) — Planejamento e Fundamentos

Elaboração e aprovação da PSI e da Política de Senhas. Designação do DPO. Criação do canal de ouvidoria. Elaboração do aditivo contratual.

FASE 2 (Meses 3 e 4) — Controles e Estrutura

Implementação das melhorias físicas. Implantação do sistema de controle de entrada e saída. Implementação da política de senhas e do 2FA.

FASE 3 (Meses 5 e 6) — Capacitação e Testes Iniciais

Treinamento de todos os colaboradores sobre PSI e LGPD. Primeira simulação de vazamento de dados. Início dos testes semanais de phishing.

FASE 4 (Meses 7 a 12) — Maturação e Monitoramento

Continuidade e análise dos testes de phishing e engenharia social. Segunda simulação de vazamento (mês 12). Revisão de todos os documentos normativos. Avaliação consolidada da conformidade com a LGPD.

6. CONSIDERAÇÕES FINAIS

Este Plano de Intervenção foi elaborado com base em evidências coletadas diretamente na empresa por meio de entrevistas, formulários e avaliações aplicadas junto aos colaboradores. Os dados obtidos confirmaram duas das três hipóteses levantadas no TCC: o nível de conhecimento dos colaboradores influencia as práticas de proteção de dados e as fragilidades nos controles de acesso aumentam os riscos de não conformidade com a LGPD.

Os resultados demonstram que a empresa possui uma base favorável de conscientização, com colaboradores que reconhecem a importância da segurança da informação. No entanto, esse conhecimento ainda não se traduziu em políticas formalizadas, procedimentos documentados ou mecanismos de controle consolidados.

A adequação à LGPD não é um projeto com prazo definitivo, mas um processo contínuo de melhoria. Recomenda-se que a empresa adote este plano como ponto de partida, com revisões anuais dos documentos normativos, auditorias internas periódicas e manutenção de um programa permanente de capacitação em proteção de dados.

O grupo coloca-se à disposição para esclarecimentos adicionais e agradece a abertura da empresa para a realização desta pesquisa.

7. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022: segurança da informação, segurança cibernética e proteção à privacidade — sistemas de gestão da segurança da informação — requisitos. Versão corrigida. Rio de Janeiro: ABNT, 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd. Acesso em: [data de acesso].

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

DONDA, Daniel. Guia prático de implementação da LGPD. São Paulo: Labrador, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020.

HINTZBERGEN, Jule et al. Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.