Anais do Congresso Brasileiro de Iniciação Científica

(https://periodicos.unisanta.br/COB)

ISSN 2317-1316

CONFORMIDADE À LGPD EM ESCRITÓRIO CONTÁBIL: DIAGNÓSTICO DE SEGURANÇA DA INFORMAÇÃO E PROPOSTA DE INTERVENÇÃO

LGPD COMPLIANCE IN AN ACCOUNTING FIRM: INFORMATION SECURITY ASSESSMENT AND INTERVENTION PROPOSAL

Oswaldo Leite Santos Grillo, Marcelo Batista Onuki

Centro Estadual de Educação Tecnológica Paula Souza – Escola Técnica de Cubatão (ETEC de Cubatão), Curso Técnico em Informática, Cubatão, SP, Brasil.
E-mail de contato: marcelo.onuki@cps.sp.gov.br

RESUMO – Este estudo analisou práticas de proteção de dados em uma empresa contábil de Santos (SP), com ênfase em Recursos Humanos e segurança da informação. Adotou-se estudo de caso exploratório, com entrevistas a gestores de três áreas, formulário anônimo respondido por 21 colaboradores e avaliação gamificada com 24 participantes. Verificou-se que 42,9% não utilizavam senha individual e 81% não identificavam canal de reporte de incidentes. A avaliação apresentou 75% de acertos médios. Como resposta, propôs-se plano de oito ações em quatro fases, durante doze meses. Conclui-se que a organização exibe práticas positivas, mas necessita formalizar controles, comunicação e treinamento contínuo.

Palavras-chave: Lei Geral de Proteção de Dados; Segurança da informação; Recursos Humanos; Controle de acesso; Governança de dados.

ABSTRACT – This study examined data protection practices in an accounting firm in Santos, Brazil, focusing on Human Resources and information security. An exploratory case study included interviews with representatives of three management areas, an anonymous survey of 21 employees, and a gamified assessment involving 24 participants. Findings showed that 42.9% did not use individual passwords and 81% could not identify an incident reporting channel. The assessment yielded a 75% mean correct-answer rate. An eight-action intervention plan was proposed across four phases over twelve months. The company showed positive practices but requires stronger formal controls, communication, and continuous training.

Keywords: General Data Protection Law; Information security; Human resources; Access control; Data governance.

ISSN 2317-1316

1. INTRODUÇÃO

A ampliação do tratamento digital de informações modificou a rotina de organizações que administram dados de clientes, fornecedores e trabalhadores. Em escritórios de contabilidade, registros de remuneração, documentos de admissão, dados bancários, contratos e informações utilizadas em obrigações administrativas tornam a segurança da informação uma questão diretamente relacionada ao exercício das atividades profissionais. Esse cenário envolve tanto ferramentas computacionais quanto procedimentos cotidianos e decisões de gestão. A existência de sistemas digitais, isoladamente, não assegura que o acesso às informações seja limitado às pessoas autorizadas.

No Brasil, a Lei nº 13.709, de 14 de agosto de 2018, estabelece regras para o tratamento de dados pessoais, incluindo princípios como finalidade, necessidade, segurança, prevenção e responsabilização (BRASIL, 2018). A proteção de dados não se restringe à confidencialidade dos registros: relaciona-se ao controle sobre o uso de informações capazes de identificar pessoas e à própria tutela da personalidade (DONEDA, 2020). Para organizações privadas, a adequação exige articulação entre processos administrativos, responsabilidades institucionais, práticas de governança e medidas de segurança (DONDA, 2020).

O setor de Recursos Humanos (RH) ocupa posição relevante nesse processo, pois administra informações de candidatos, funcionários e ex-colaboradores em fases distintas do vínculo profissional. Suas atividades se conectam aos setores de Tecnologia da Informação (TI), Departamento Pessoal e direção, demandando regras consistentes para acesso, armazenamento, compartilhamento e descarte. A literatura de gestão de pessoas ressalta o caráter integrado das atividades de RH e sua dependência de informações organizacionais confiáveis (CHIAVENATO, 2022). Nesse contexto, controles insuficientes ou mal comunicados podem comprometer a capacidade da empresa de acompanhar quem consulta ou manipula determinados dados.

Em complemento ao marco legal, a ABNT NBR ISO/IEC 27001:2013, utilizada como referência no trabalho de origem, apresenta requisitos para sistemas de gestão de segurança da informação. A orientação por processos, identificação de riscos, documentação, acompanhamento e melhoria contínua oferece parâmetros para avaliar práticas corporativas, embora a adoção de um padrão de gestão não equivalha, por si só, à comprovação de conformidade jurídica à LGPD (ABNT, 2013; HINTZBERGEN et al., 2018). A governança de

ISSN 2317-1316

dados, por sua vez, relaciona definições de responsabilidade, qualidade e uso dos dados às necessidades organizacionais (DAMA INTERNATIONAL, 2017).

A problemática investigada foi: em que medida os processos de um escritório contábil situado em Santos (SP), com especial atenção ao RH, apresentam práticas compatíveis com os requisitos da LGPD e com princípios de segurança da informação? Partiu-se da hipótese de que fragilidades na gestão de acessos, comunicação sobre incidentes e capacitação dos colaboradores se relacionam à persistência de riscos operacionais. O objetivo geral consistiu em diagnosticar práticas existentes e lacunas observáveis e, a partir dos resultados, propor medidas de aprimoramento. Como objetivos específicos, buscaram-se identificar percepções dos trabalhadores, investigar procedimentos adotados por representantes da gestão, realizar capacitação sobre segurança digital e elaborar uma proposta de intervenção para a empresa.

2. MATERIAIS E MÉTODOS

A pesquisa foi conduzida como estudo de caso exploratório, com abordagem qualitativa e quantitativa, em uma empresa do segmento contábil localizada no município de Santos, estado de São Paulo. O estudo concentrou-se no tratamento de dados pessoais e sensíveis e nos processos de RH, considerando também decisões de direção e práticas de TI. O levantamento de campo integrou o TCC originalmente desenvolvido em grupo no Curso Técnico em Informática da Etec de Cubatão. A identidade da organização não é informada nesta síntese, e os resultados apresentados são agregados. Os instrumentos utilizados no TCC de origem foram entrevistas semiestruturadas, checklists temáticos, formulário anônimo, ação de capacitação, questionário avaliativo e síntese diagnóstica aplicada à elaboração de um plano de intervenção.

As entrevistas foram realizadas em três momentos: em 19 de março de 2026, com o sócio-administrador, que também acumulava a atribuição de encarregado de dados; em 28 de abril de 2026, com a responsável por Recursos Humanos; e em 29 de abril de 2026, com o profissional de Tecnologia da Informação. Os roteiros abordaram controle de acesso, segurança da informação, tratamento documental, direitos dos titulares, gestão de incidentes e governança. As respostas foram examinadas em conjunto, buscando convergências e diferenças entre o relato dos responsáveis e as práticas descritas pelos colaboradores.

ISSN 2317-1316

Para o levantamento quantitativo, utilizou-se formulário digital construído no Google Forms, composto por 11 perguntas sobre identificação de pessoas, restrição de acesso, conhecimento da LGPD, senhas, comunicação e percepção de conformidade. O formulário obteve 21 respostas de colaboradores e foi disponibilizado de forma anônima, conforme descrito no TCC. Os percentuais foram obtidos a partir das frequências de resposta a cada item. Como se trata de um único ambiente empresarial, os resultados representam os participantes do levantamento, não uma amostra probabilística do setor contábil.

Em 28 de abril de 2026, também foi ministrada apresentação de conscientização nas dependências da empresa. Os conteúdos incluíram boas práticas de segurança digital, golpes eletrônicos, engenharia social, confidencialidade, integridade, disponibilidade, gestão documental e LGPD. Ao final, aplicou-se um questionário gamificado de 12 questões, por meio da plataforma Kahoot, com 24 participantes. O resultado médio de acertos e os desempenhos por questão foram utilizados como indicadores descritivos da compreensão dos temas abordados naquele momento. O estudo não documenta uma avaliação equivalente anterior à capacitação; portanto, a pontuação posterior não foi tratada como prova de efeito causal do treinamento.

A interpretação qualitativa partiu da comparação entre depoimentos das três áreas e respostas agregadas dos trabalhadores. Posteriormente, os pontos de atenção foram organizados por criticidade operacional para subsidiar um plano de oito ações e execução sugerida em quatro fases ao longo de doze meses. Não foram executados testes independentes de invasão, auditorias certificadoras ou validações técnicas exaustivas de todos os sistemas. Assim, a pesquisa deve ser compreendida como diagnóstico exploratório de práticas e percepções, com proposição de melhorias, e não como certificação formal de conformidade legal ou técnica.

3. RESULTADOS E DISCUSSÃO

O levantamento evidenciou coexistência de procedimentos favoráveis à proteção de dados e de fragilidades administrativas e tecnológicas. Segundo o sócio-administrador, a empresa mantinha ferramentas de proteção, como antivírus e firewall, e mecanismos de cópias de segurança armazenadas em diferentes locais, o que indica atenção à continuidade operacional. Entretanto, as estações Windows não utilizavam credenciais individuais em parte

ISSN 2317-1316

significativa do ambiente, e faltavam exigências internas padronizadas para a criação de senhas. A direção relatou treinamentos anteriores, mas sem calendário regular. Essas observações são relevantes porque medidas de recuperação e defesa de perímetro não substituem identificação individual, registro de acessos e orientação permanente.

No RH, foram identificados documentos físicos mantidos em local de acesso restrito e cláusulas de confidencialidade atribuídas aos funcionários. Também foi mencionado o projeto de digitalização do acervo. Persistem, porém, questões a esclarecer sobre obrigações de confidencialidade aplicáveis a prestadores de TI e sobre critérios documentados de retenção e destinação de currículos preservados em banco de talentos. O achado não permite concluir, isoladamente, que determinada base legal esteja ausente ou que haja infração consumada: demonstra a importância de verificar finalidade, fundamento do tratamento, prazo de conservação e comunicação aos titulares, conforme os princípios da LGPD (BRASIL, 2018).

O profissional de TI relatou o uso de perfis de permissão em sistemas de negócio, proteção do acesso físico ao servidor e supervisão de profissionais externos. Contudo, manifestou incerteza sobre a abrangência dos registros de acesso, e reconheceu que a segregação das pastas corporativas ainda estava em implantação. O controle já havia sido reforçado em áreas como direção e Departamento Pessoal, enquanto setores operacionais continuavam com acesso mais amplo. A diferença entre a existência de credenciais nos aplicativos e a ausência de autenticação individual em algumas estações evidencia que a política de controle precisa abranger diferentes camadas tecnológicas. A documentação de perfis, eventos e responsabilidades é essencial para rastreabilidade e prevenção, objetivos discutidos na literatura de segurança da informação (ABNT, 2013; SÊMOLA, 2014).

O formulário dos 21 colaboradores permitiu quantificar percepções relacionadas às entrevistas. Enquanto 90,5% (19/21) afirmaram conhecer a LGPD e 85,7% (18/21) disseram saber o que são dados pessoais, 42,9% (9/21) informaram não utilizar senha pessoal e intransferível para acessar os sistemas internos. A combinação sugere que o conhecimento declarado sobre a legislação convivia com fragilidades em procedimentos concretos. Os resultados selecionados são sintetizados na Tabela 1.

ISSN 2317-1316

Tabela 1: Indicadores selecionados do diagnóstico de proteção de dados.

Indicador observado	**Frequência**	**Percentual**
Não utilizam identificação institucional	16 de 21	76,2%
Relatam ausência de identificação formal de visitantes	16 de 21	76,2%
Presenciaram visitantes em áreas com dados pessoais	7 de 21	33,3%
Não utilizam senha pessoal e intransferível	9 de 21	42,9%
Não identificam canal de reporte ou desconhecem sua existência	17 de 21	81,0%
Afirmam conhecer a LGPD	19 de 21	90,5%
Acertos médios no questionário Kahoot	24 participantes	75,0%
Acertos na questão sobre riscos sistêmicos do escritório	7 de 24	29,2%

Fonte: elaboração a partir dos resultados do TCC de origem (2026). Percentuais arredondados; para o Kahoot, a base é de 24 participantes, distinta do formulário com 21 respondentes.

As respostas sobre controles físicos reforçaram esse quadro. Dos 21 participantes, 76,2% relataram não utilizar crachá ou outro meio de identificação fornecido pela empresa, e a mesma proporção informou que visitantes não recebiam identificação formal. Além disso, 33,3% disseram já ter observado pessoas externas circulando livremente em ambientes com computadores ou documentos contendo dados pessoais. Nas entrevistas, a gestão relatou procedimentos de recepção e acompanhamento; a discrepância entre o procedimento descrito e a percepção dos respondentes aponta necessidade de padronização e comunicação das regras, sem permitir afirmar, por si só, que não existia qualquer controle de entrada.

O problema de comunicação interna foi especialmente perceptível na pergunta sobre canal para reporte de incidentes. Apenas 19,0% (4/21) afirmaram existir um canal; 52,4% (11/21) responderam que ele não existia e 28,6% (6/21) disseram não saber. Assim, 81,0% não conseguiram identificar positivamente sua existência. O dado não comprova que a organização carecia de qualquer forma de contato, pois foram mencionados meios como e-mail e aplicativos de mensagens, mas demonstra ausência de conhecimento compartilhado sobre o fluxo esperado

ISSN 2317-1316

de reporte. Para fins de gestão, a disponibilidade informal de um meio de contato é insuficiente se os trabalhadores não sabem quando e como utilizá-lo.

Outro resultado que exige interpretação contextual é o fato de 85,7% dos respondentes afirmarem ter acesso somente aos dados necessários ao trabalho. Essa percepção favorável contrasta com a informação fornecida pela TI de que a segmentação da rede não abrangia todas as equipes. Não se trata necessariamente de contradição nas respostas, uma vez que o trabalhador pode não conhecer o conjunto completo de permissões disponível em suas credenciais. Por essa razão, a percepção dos usuários constitui evidência complementar, mas não substitui levantamento técnico dos perfis de acesso.

Na ação educativa, a avaliação gamificada de 12 questões registrou média geral de 75% de respostas corretas entre 24 participantes. O desempenho variou significativamente conforme o tema: questões sobre boas práticas de proteção tiveram índices elevados, enquanto a aplicação da tríade confidencialidade, integridade e disponibilidade em situação concreta alcançou 58,3% e a identificação de riscos sistêmicos de um escritório contábil, 29,2%. Os resultados indicam que parte dos conceitos era reconhecida, mas a interpretação de situações operacionais complexas apresentava dificuldades. Como não houve teste equivalente anterior, não é metodologicamente possível atribuir os acertos observados exclusivamente à capacitação realizada.

A análise conjunta sugere uma diferença entre conhecimento declaratório e institucionalização das práticas. Conhecer a legislação ou reconhecer a importância de senhas fortes não implica que cada estação seja configurada com uma conta individual, que o acesso a pastas seja revisado periodicamente ou que haja fluxo documentado de comunicação de incidentes. A literatura utilizada no TCC associa segurança da informação a controles técnicos, processos organizacionais e responsabilidades humanas (HINTZBERGEN et al., 2018; MASCARENHAS NETO; ARAÚJO, 2019). O caso observado reproduz essa natureza multidimensional: onde havia iniciativas pontuais, faltava uniformidade normativa e evidência de monitoramento sistemático.

Com base no diagnóstico, foi entregue à gestão um Plano de Intervenção contendo oito frentes de ação: aprimoramento do controle físico e da identificação de colaboradores e visitantes; definição contratual sobre retenção de dados em dispositivos pessoais após o desligamento; estabelecimento de canal de atendimento ao titular e reporte; formalização do

ISSN 2317-1316

registro de entradas e saídas; política de senhas; política de segurança da informação e privacidade; simulações de incidentes; e testes de engenharia social e mensagens fraudulentas (phishing). Essas ações foram propostas para abordar os riscos identificados, e não como medidas já implementadas ou comprovadamente eficazes.

O cronograma sugerido compreendeu quatro fases. Nos meses 1 e 2, priorizaram-se documentos normativos, atribuições, canais de comunicação e revisão contratual. Nos meses 3 e 4, propuseram-se controles físicos, registro de circulação e fortalecimento da autenticação. Nos meses 5 e 6, previram-se treinamentos ampliados, primeira simulação de incidente e início de testes educativos. Entre os meses 7 e 12, a proposta recomendou acompanhamento dos indicadores, continuidade dos exercícios, revisão das normas e avaliação consolidada. A lógica de planejamento, execução, verificação e aperfeiçoamento aproxima-se do ciclo de melhoria contínua empregado em sistemas de gestão de segurança da informação (ABNT, 2013).

Na data de conclusão do TCC, a gestão havia recebido a proposta e informado que as ações seriam discutidas internamente, sem resposta formal sobre medidas efetivamente adotadas. Portanto, o principal produto aplicado da pesquisa foi o diagnóstico acompanhado de uma proposta estruturada, não uma comprovação de transformação organizacional. Essa distinção é central para avaliar o alcance científico do estudo e orientar acompanhamentos futuros. As limitações incluem a observação de apenas uma empresa, o caráter autodeclarado das respostas, a ausência de auditoria técnica integral e a falta de medição longitudinal antes e depois das ações. Ainda assim, a triangulação entre depoimentos de três áreas, percepção de colaboradores e desempenho em questionário contribuiu para identificar prioridades de gestão.

4. CONCLUSÃO

O estudo permitiu caracterizar um cenário de conformidade parcial com a LGPD no escritório contábil investigado, no qual procedimentos favoráveis à continuidade operacional e à proteção documental conviviam com fragilidades de autenticação, segmentação de acesso, identificação de visitantes e comunicação sobre incidentes. Entre os 21 respondentes, 42,9% não utilizavam credenciais pessoais e intransferíveis, e 81,0% não identificavam positivamente um canal de reporte; na avaliação com 24 participantes, a média de 75% de acertos ocultava dificuldades em questões aplicadas. Como resposta, a pesquisa produziu capacitação e proposta

ISSN 2317-1316

de oito ações escalonadas em doze meses, entregue à gestão, mas ainda sem implementação comprovada ao término da investigação. Conclui-se que o aperfeiçoamento da proteção de dados demanda integrar tecnologia, práticas administrativas e formação contínua. Recomenda-se acompanhar a aplicação das ações e repetir indicadores em momentos posteriores, além de comparar os resultados com outros escritórios contábeis. Agradece-se à empresa pesquisada e à orientação acadêmica pelo apoio à realização do estudo.

5. DECLARAÇÃO DE USO DE IA

Durante a elaboração do TCC, foram utilizadas, em diferentes momentos do início de 2026, as versões convencionais Claude Sonnet 4.5 e Claude Sonnet 4.6, Chat GPT GPT-5.2 Instant e GPT-5.3 Instant e Gemini 3 Flash, como apoio à elaboração e revisão da estrutura do trabalho. Na adaptação do TCC para este artigo, em outubro de 2026, utilizou-se exclusivamente o Chat GPT (GPT-6) para estruturar as informações da presente pesquisa.

6. REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 27001:2013: tecnologia da informação — técnicas de segurança — sistemas de gestão da segurança da informação — requisitos. Rio de Janeiro: ABNT, 2013.

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.

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

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.

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.

ISSN 2317-1316

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

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