

A SEGURANÇA DA INFORMAÇÃO EMPRESARIAL: UMA NECESSIDADE MULTISSETORIAL

BUSINESS INFORMATION SECURITY: A MULTI-SECTORAL NECESSITY

Ciências Sociais Aplicadas • 03/01/2026

REGISTRO DOI: [10.5281/zenodo.18142605](https://doi.org/10.5281/zenodo.18142605)

Ana Paula Von Zuben Hass¹

RESUMO

A segurança da informação é um elemento estratégico indispensável para organizações contemporâneas, impactando diretamente na continuidade operacional, na governança corporativa e na competitividade empresarial. O crescente uso de sistemas digitais e a intensificação de ataques cibernéticos exigem que as empresas desenvolvam processos estruturados para proteger seus ativos de informação. Esses processos devem ser aplicados a partir da observação das vulnerabilidades físicas e digitais existentes, realizando auditorias como forma de análise da atividade operacional. Dessa forma, o artigo aborda, através da pesquisa bibliográfica, a importância da implementação de políticas e práticas de segurança da informação no ambiente corporativo, detalhando tipos de ameaças, ferramentas tecnológicas, gestão de riscos, políticas internas, cultura organizacional e diferencial competitivo. Além disso, observa a gestação da segurança de forma setorial, a partir da área da atuação da empresa e da sua classificação lucrativa, o que ditará as soluções passíveis de aplicação diante da qualidade e quantidade de dados efetivamente tratados.

Palavras-chave: Segurança da Informação. Governança Corporativa. Ativos de Informação. Vulnerabilidades. Cultura Organizacional.

ABSTRACT

Information security is an indispensable strategic element for contemporary organizations, directly impacting operational continuity, corporate governance, and business competitiveness. The increasing use of digital systems and the intensification of cyberattacks require companies to develop structured processes to protect their information assets. These processes should be applied based on the observation of existing physical and digital vulnerabilities, conducting audits as a way to analyze operational

activity. Therefore, this article addresses, through bibliographic research, the importance of implementing information security policies and practices in the corporate environment, detailing types of threats, technological tools, risk management, internal policies, organizational culture, and competitive advantage. Furthermore, it examines the development of security sectorally, based on the company's area of operation and its profitability classification, which will dictate the solutions applicable to the quality and quantity of data actually processed.

Keywords: Information Security. Corporate Governance. Information Assets. Vulnerabilities. Organizational Culture.

INTRODUÇÃO

A sociedade atual é caracterizada pela digitalização intensa, na qual informações corporativas são armazenadas, processadas e compartilhadas por sistemas de tecnologia da informação (TI). O cenário atual gera vantagens como a maior produtividade, integração e possibilidade de tomada de decisões estratégicas.

Apesar de todas as benesses, a digitalização das empresas ocasiona um aumento de riscos diante da quantidade de informações disponíveis no ambiente digital. O acervo de cada empresa pode restar exposto quando não houver um planejamento para segurança da informação. Assim, vulnerabilidades podem ocasionar riscos significativos, como ataques cibernéticos, fraudes internas e vazamentos de dados confidenciais, que exigem a aplicação de contramedidas de segurança. (CORTEZ; KUBOTA, 2013).

Sabe-se que há algum tempo, a preocupação com a proteção da informação estava muito restrita a computadores ou redes.

Atualmente, a visão tem sido modificada diante da conscientização do todo, trazendo a necessidade de uma política de proteção de dados e da segurança da informação. Nessa toada, tornou-se um tema estratégico que integra tecnologia, processos e pessoas, impactando diretamente no desempenho organizacional e na competitividade.

Portanto, desenvolver processos de segurança da informação é essencial para proteger ativos críticos, assegurar a continuidade do negócio e sustentar a confiança de clientes e parceiros. Este artigo busca demonstrar, através da pesquisa bibliográfica, a relevância da segurança da informação no ambiente empresarial, detalhando os tipos de ameaças, tecnologias aplicáveis, políticas internas, gestão de riscos e impacto estratégico.

1. CONCEITOS FUNDAMENTAIS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é definida como um conjunto de políticas, processos e ferramentas que garantem a confidencialidade, integridade e disponibilidade dos dados corporativos. Diante desses princípios, são aplicadas ferramentas de tecnologia específicas, com protocolos de utilização dentro de um processo. (NAKAMURA; GEUS, 2007)

Assim, cada princípio possui relevância estratégica. Enquanto a confidencialidade assegura o acesso restrito a determinados dados, a integridade garante que eles permaneçam estáveis, corretos e confiáveis. Por sua vez, a disponibilidade garante acesso a eles quando o usuário assim desejar.

Cabe ainda a menção da confiabilidade como um requisito interno da integridade, já que avalia a qualidade dos dados e garante a fonte

do conteúdo. Apesar de não haver uma presunção absoluta de veracidade da informação, ela garante a confiabilidade da fonte, o que gera maior autoridade na questão tratada. (SORDI; MIRELES E GRIJO, 2008)

Nota-se assim que existe um encadeamento de garantias, de forma a se presumir que a informação, verídica e completa, possa ser acessada quando necessário por um usuário devidamente qualificado para tanto.

Além desses princípios, a segurança da informação deve ser encarada como um ativo organizacional, capaz de influenciar decisões estratégicas, promover inovação segura e proteger a reputação da empresa. A combinação de tecnologia, processos internos e treinamento de colaboradores é essencial para que a segurança da informação seja eficaz e sustentável.

2. TIPOS DE AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

Tendo em vista que a inserção digital dá azo para infiltrações indesejadas, é necessário que se analise possíveis ameaças a esses sistemas. As ameaças físicas até então vistas como as principais, vêm sendo acompanhadas pelas ameaças digitais, a partir da digitalização de um acervo empresarial.

Assim, as ameaças à segurança da informação podem ser classificadas em cinco categorias principais: *Malware e Ransomware*: programas maliciosos que corrompem dados e exigem resgate financeiro; *Phishing* e engenharia social: técnicas que enganam colaboradores para obter informações confidenciais; Acessos internos indevidos: colaboradores que, intencionalmente ou por descuido, comprometem dados corporativos; Vazamentos

acidentais: compartilhamento involuntário de informações sensíveis; e Falhas técnicas: problemas em sistemas e servidores que afetam a disponibilidade e integridade dos dados.

A título de exemplo, são frequentes as comunicações feitas por grandes empresas sobre vazamento de dados pessoais, como e-mail, CPF, endereços, dentre outros. Nesse sentido, para cada categoria apresentada haverá uma contramedida necessária para evitar ou reduzir prejuízos.

Diante de *Malware* e do *Ransomware*, que podem causar interrupção de processos críticos, existem os antivírus, o firewall, e o próprio backup regular como medidas preventivas. Já o *Phishing*, que pode gerar vazamento de dados confidenciais, pode-se realizar o treinamento de colaboradores, em especial aqueles que lidam diariamente com o ambiente digital.

O acesso interno aos dados também é uma causa que pode comprometer a segurança da informação, importando na manipulação indevida ou na destruição de dados essenciais. Para tanto, a estipulação de níveis de acessos distintos entre os colaboradores, bem como seu controle através de auditorias, poderá mitigar dita vulnerabilidade.

Existe ainda o vazamento acidental, quando ausente o dolo, verifica-se a perda de informações estratégicas, ou ainda a divulgação daquilo que deveria permanecer em sigilo. Visando uma melhoria nesse aspecto, treinamentos internos, e a aplicação de políticas dentro do ambiente empresarial são ferramentas de melhoria para o caso.

Cabe ainda evidenciar que a falha, enquanto vazamento acidental, pode ser classificada também como uma falha técnica, e não humana. Nesse caso, caberá o monitoramento contínuo do sistema para verificar eventuais padrões de vulnerabilidades que possam causar a interrupção e a divulgação indevida de informações. A contratação de profissionais especializados em tecnologia da informação também é um meio eficiente para o combate à ocorrência indesejada.

Resta claro que a segurança da informação é uma necessidade estratégica, impactando diretamente na sustentabilidade e competitividade das empresas. Assim, muito mais que combater, a prevenção é a adequada política a ser aplicada para o maior êxito organizacional.

3. FERRAMENTAS E TECNOLOGIAS DE SEGURANÇA

A segurança da informação, vista agora como uma necessidade física e digital, pode (e deve) se apoiar na tecnologia, como forma de criar processos estratégicos de atuação. É nesse cenário tecnológico que surgem ferramentas essenciais: *firewalls* e antivírus, já que bloqueiam softwares maliciosos e filtram tráfego suspeito; a criptografia, que protege dados em trânsito e em armazenamento; os sistemas de detecção de intrusão (IDS/IPS), uma vez que monitoram acessos suspeitos; o backup e a redundância, os quais garantem a recuperação de informações em caso de falhas; e autenticação multifator, já que ela adiciona camada extra de proteção em acessos críticos.

O uso dessas ferramentas, aliado a processos internos claros, cria uma barreira robusta contra os ataques, reforçando a confiança de

clientes e parceiros e garantindo a continuidade operacional.

4. POLÍTICAS INTERNAS E CULTURA ORGANIZACIONAL

Apesar de muito benéfica, a tecnologia, isoladamente, não garante a segurança integral da empresa. É importante criar uma cultura organizacional, voltada à segurança, incluindo treinamentos periódicos, com capacitação dos colaboradores, de forma a propagar a conscientização sobre os riscos no tratamento de dados e as boas práticas organizacionais.

Além disso, ter um código de conduta e políticas internas, definindo regras claras de acesso, a forma de armazenar as informações e quais são as possibilidades de compartilhamentos, quando se coadunam a uma Gestão de Permissões da empresa, garantem o acesso controlado e efetivo diante de determinadas necessidades.

É evidente que a implementação de políticas e a conscientização dos colaboradores reduzem significativamente incidentes, promovendo um ambiente de responsabilidade coletiva. No mais, as medidas aplicadas devem ser acompanhadas de auditorias e monitoramentos contínuos, como forma de identificar de forma antecipada as vulnerabilidades de um sistema interno, físico ou digital, reduzindo os prejuízos de uma interferência indesejada.

5. GESTÃO DE RISCOS E CONTINUIDADE DE NEGÓCIOS

A gestão de riscos é uma etapa crítica na segurança da informação. Para tanto, é recomendado identificar vulnerabilidades, avaliar impactos e implementar estratégias de mitigação.

As etapas desse processo de gestão, incluem a identificação de ativos críticos e ameaças; a avaliação de impacto financeiro e operacional; a implementação de controles preventivos; o monitoramento contínuo e a realização de auditorias, além de planos de contingência e recuperação de desastres.

Um exemplo prático a ser citado como sugestão é a implementação de planos de contingência e backups redundantes em instituições financeiras, de forma a reduzir o tempo de inatividade em ataques cibernéticos de 48 horas para menos de 2 horas.

Desse modo, a gestão de riscos integrada à segurança da informação garante continuidade operacional, minimiza perdas financeiras e fortalece a confiança de *stakeholders*.

6. SEGURANÇA DA INFORMAÇÃO COMO DIFERENCIAL COMPETITIVO

Além de proteger dados, a segurança da informação é um diferencial estratégico. Empresas seguras inovam sem comprometer os dados sensíveis de seu acervo; cumprem legislação, como a LGPD, evitando sanções e garantindo uma comunicação favorecida com países que exigem a proteção dos dados para comercialização, além de aumentar a confiança de clientes, parceiros e investidores.

Nota-se que organizações que incorporam segurança da informação à estratégia empresarial obtêm maior resiliência, capacidade de adaptação e vantagem competitiva sustentável. A questão se distancia apenas da lucratividade para dar espaço para consciência social e o impacto gerado pela invasão de dados em dinâmicas individuais da população atingida.

7. A SEGURANÇA DA INFORMAÇÃO NOS DIVERSOS SETORES

A análise do impacto de um vazamento indevido deve se atentar ao setor de atuação, assim, políticas de planejamento devem ser realizadas diante das informações tratadas e visualização de possíveis vulnerabilidades naquele âmbito.

No setor da saúde, muitos dados, sensíveis ou não, são obtidos através dos prontuários. Assim, quando digitais, a criptografia, backup diário e monitoramento de acessos são meios de reduzir os incidentes. Quando físicos, a guarda em local adequado e de acesso limitado também se mostra eficiente.

Já na área financeira, dados referentes à condição econômica de cada indivíduo podem ser expostos indevidamente, além da possibilidade de fraudes e ataques externos visando transferências de ativos e ganhos financeiros. Assim, uma equipe dedicada ao monitoramento de um sistema digital forte e a autenticação multifator se mostram como condutas adequadas na redução de incidentes críticos e no aumento da confiança dos clientes.

Sabe-se, no entanto, que pequenas e médias empresas possuem um investimento reduzido para a área de segurança da informação, o que não deve ser visto como uma barreira impossível de ser rompida para implementação de políticas. O treinamento de colaboradores e a instalação de antivírus já demonstram eficiência e divulgação de uma política de segurança no meio.

7.1. A Segurança da Informação e a Proteção dos Dados nos Cartórios de Registro Civil

A segurança da informação nas serventias extrajudiciais – os conhecidos cartórios – também é regulada a partir da classificação financeira do cartório. Ou seja, os cartórios que possuem uma lucratividade maior terão maiores exigências a serem cumpridas e fiscalizadas, enquanto aqueles com menor lucratividade devem se adaptar à medida das diretrizes fixadas para sua classe financeira, conforme o Provimento N° 74 de 31/07/2018 do Conselho Nacional de Justiça.

A segurança da informação nesse setor se tornou pauta essencial à medida que a Lei Geral de Proteção de Dados e a própria digitalização do acervo trouxeram uma nova realidade jurídica. Assim, tanto a recuperação das informações, por meio de *backups* e cópias de segurança, quanto a própria proteção contra o vazamento de dados sofreram reformulações para atender às atuais diretrizes.

No âmbito da proteção dos dados, a atividade, que é pautada na publicidade dos atos, teve que se adaptar para garantir que direitos fundamentais não fossem violados pela lida diária com documentos formados por dados sensíveis, que necessitam de uma qualificação prévia de seu requerente. Apesar disso, não perderam sua essência pública e de transparência.

A prática, alterada pela Lei Geral de Proteção de Dados e, posteriormente, pelos Provimentos do Conselho Nacional de Justiça, classificou os atos praticados nos Tabelionatos de Notas e Protestos, bem como nos Ofícios de Registro, regulando quem seriam os legitimados para seu requerimento e emissão, a partir da presença ou não de dados capazes de gerar impactos públicos e/ou privados.

A segurança da informação e a proteção dos dados passaram a ser questão administrativa, uma vez que a ampla orientação e o conhecimento técnico sobre a matéria devem ser medidas imprescindíveis para boa prática da atividade desde as contratações e aquisições.

Nessa toada e a título de exemplo, no âmbito do Registro Civil das Pessoas Naturais, balizas como a qualificação do requerimento e a verificação da legitimidade do requerente para emissão de uma certidão integral do ato – denominadas certidão em inteiro teor - devem ser critérios observados diante do conteúdo de um registro. Os critérios utilizados para análise do registro foram graduados pelo Conselho Nacional de Justiça sob a ótica do impacto de eventual vazamento de dados, como demonstrado pelo artigo 116 do Provimento 149/2023:

Art. 116. As solicitações de certidões por quesitos, ou informações solicitadas independentemente da expedição de certidões, receberão o mesmo tratamento destinado às certidões solicitadas em inteiro teor quando os dados solicitados forem restritos, sensíveis ou sigilosos.

§ 1.º São considerados elementos sensíveis os elencados no inciso II do art. 5.º da Lei n. 13.709/2018, ou outros, desde que previstos em legislação específica.

§ 2.º São considerados elementos restritos os previstos no art. 45 e art. 95 da Lei n. 6.015/1973, no art. 6.º e seus parágrafos da Lei n. 8.560/1992, nas normas de alteração de nome ou sexo no caso de pessoa transgênero, ou outros, desde que previstos em legislação específica.

§ 3.º São considerados elementos sigilosos os previstos no parágrafo 7.º do artigo 57 da Lei n. 6.015/1973, ou outros, desde que previstos em legislação específica.

Foi nesse sentido que os dados que têm um impacto que transcende o âmbito privado, com potenciais efeitos públicos e estatais foram definidos como sigilosos, como é o caso da alteração de nome concedida em razão de fundada coação ou ameaça decorrente de colaboração com a apuração de crime. Nesses casos,

a emissão da certidão dependerá de uma anuência estatal, materializada através de uma decisão judicial, precedida da verificação sobre os riscos da publicização da informação.

Os dados que possuem um abalo inicialmente privado, porém geram efeitos na ordem pública, foram classificados como restritos. Nesse caso, sendo a requisição da certidão realizada pelo titular do dado do registro ou por meio de seu representante ou seu procurador, não haverá óbice para emissão do documento de forma integral. Doutro modo e *a contrario sensu*, terceiros necessitam de uma anuência judicial para a emissão, como demonstrado pelo artigo 114 do referido Provimento:

Art. 114. As certidões de registro civil em geral, inclusive as de inteiro teor, requeridas pelos próprios interessados, seus representantes legais, mandatários com poderes especiais, serão expedidas independentemente de autorização do juiz corregedor permanente.

Para exemplificar o contexto mencionado, um registro de nascimento em que consta a averbação do reconhecimento de uma paternidade ou aquele que possua uma alteração de nome e gênero seguirá dita delimitação e qualificação normativa. O viés protetivo utilizado visa ponderar direitos fundamentais e a própria autodeterminação informativa com o caráter público dos registros. Cabe ressaltar que, até o momento, não há uma relativização expressa dessa restrição em caso de morte do titular.

Por fim, os dados sensíveis possuem, majoritariamente, um impacto na intimidade e na vida privada do indivíduo e seguem o regramento dos dados restritos, uma vez que dependem da legitimidade do requerente para sua emissão de forma integral. A questão, no entanto, apresenta uma nova regulamentação diante do falecimento do titular do dado, uma vez que os dados sensíveis são limitadores da publicidade durante a vida do indivíduo. Sendo assim, o Provimento 149 de 2023, do Conselho Nacional de Justiça dispôs:

Art. 114. As certidões de registro civil em geral, inclusive as de inteiro teor, requeridas pelos próprios interessados, seus representantes legais, mandatários com poderes especiais, serão expedidas independentemente de autorização do juiz corregedor permanente.

§ 1.º Nas hipóteses em que a emissão da certidão for requerida por terceiros e a certidão contiver dados sensíveis, somente será feita a expedição mediante a autorização do juízo competente.

§ 2.º Após o falecimento do titular do dado sensível, as certidões de que trata o caput deste artigo poderão ser fornecidas aos parentes em linha reta, independentemente de autorização judicial

Art. 118. Não é necessário requerimento ou autorização judicial para emissão de certidão de óbito em nenhuma de suas modalidades.

Art. 119. As restrições relativas aos dados sensíveis elencados pelo inciso II do art. 5.º da Lei n. 13.709/2018 não se aplicam ao caso de pessoa falecida.

Resta claro que a observância dos padrões normativos deve ser realizada pelo delegatário, disseminada entre os prepostos e monitorada através de sistemas e auditorias, inclusive pelas Corregedorias. Os padrões a serem seguidos versam tanto sobre a

compra de *softwares* licenciados para uso comercial, antivírus e antissequestro, como também sobre a contratação e orientação de profissionais para absorção e aplicação dos ditames técnicos da matéria, fiscalizando ainda a correta adaptação dos sistemas para a restrição da publicidade em determinados casos, em especial quando os dados são repassados às Centrais e órgãos públicos.

8. A CULTURA DA SEGURANÇA DA INFORMAÇÃO COMO UM PROCESSO MULTISSETORIAL

A análise evidencia que a segurança da informação vai além da proteção técnica. Ela integra processos, tecnologia e cultura organizacional para reduzir riscos e apoiar objetivos estratégicos.

Dentre os principais setores do processo, destaca-se: a necessidade de continuidade operacional, especialmente em setores que prestam serviços essenciais; o compliance legal e regulatório como meio benéfico na condução dos sistemas; a confiabilidade dos usuários; a garantia de uma sustentabilidade segura e a redução de perdas financeiras e de reputação.

A aplicabilidade de cada ferramenta irá depender da qualidade e forma que os dados são tratados, havendo mudanças na ênfase de cada um, a depender da área de atuação da empresa.

CONCLUSÃO

O desenvolvimento de processos de segurança da informação é essencial para proteger ativos, reduzir riscos e alcançar objetivos organizacionais. A combinação de políticas estruturadas, treinamentos contínuos, protocolos de resposta a incidentes e tecnologias avançadas fortalece a governança, assegura a

continuidade do negócio e aumenta a confiança de clientes e parceiros.

Investir em segurança da informação é uma decisão estratégica, transformando proteção de dados em diferencial competitivo. Empresas que integram tecnologia, processos e cultura organizacional estão mais preparadas para enfrentar desafios contemporâneos e garantir sustentabilidade e competitividade no mercado.

No mais, o cumprimento legal, através, por exemplo, da observância da Lei Geral de Proteção de Dados, se coaduna com a imprescindibilidade de um sistema de segurança informativa, devidamente personalizado para o setor de atuação. A utilização técnica e sistêmica adequada evita sanções e impulsiona a empresa para uma seara sustentável, adpta a diligências necessárias e exigidas no mercado nacional e internacional, reforçando o compromisso social da entidade.

REFERÊNCIAS BIBLIOGRÁFICAS

CORTEZ, I; KUBOTA, L. 2013. **Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras.** *Rev. Adm. (São Paulo)* 48 (4). Dez 2013. Disponível em: <https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/?format=html&lang=pt>. Acesso em 08 nov. 2025.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

SORDI, José Osvaldo de.; MIRELES, Manuel; GRIJO, Rogério Nahas. **Gestão da qualidade da informação no contexto das organizações: percepções a partir do experimento de análise da confiabilidade dos jornais eletrônicos.** *Perspectivas em Ciência da Informação*, v. 13, n. 2, 2008, p 168-195. Disponível em: <http://www.scielo.br/pdf/pci/v13n2/a12v13n2.pdf>. Acesso em: 08 nov. 2025.

¹ Bacharel em Direito (FADITU). Pós-graduada em Conciliação e Mediação (UNIBF). Pós-graduada em Direito Notarial e Registral (UNIBF). Mestranda em Administração (MUST).