Empresas & Negócios

Matéria de capa

MF3d_CANVA

SGSI

AUMENTO DAS AMEAÇAS DIGITAIS IMPULSIONA EMPRESAS BRASILEIRAS A ADOTAREM ISO 27001

Já é sabido que o Brasil enfrenta hoje – com uma baixa probabilidade de qualquer mudança futura – uma escalada de ameaças cibernéticas, com um aumento de 21% no número de ataques em relação ao ano anterior, totalizando uma média de 2.667 incidentes semanais por empresa. Diante dessa realidade, tem crescido a busca pela certificação ISO/IEC 27001, que estabelece requisitos rigorosos para um Sistema de Gestão da Segurança da Informação (SGSI).

Sylvio Sobreira Vieira (*)

Embora levantamentos de mercado indiquem que apenas 165 organizações brasileiras possuíam a certificação ISO 27001 até o início de 2023, a tendência tem sido de crescimento, impulsionada pela necessidade de fortalecer a segurança da informação e atender às exigências regulatórias.

E a motivação das empresas vai além da mera proteção técnica. A certificação ISO 27001 tornou-se também uma resposta estratégica às demandas de compliance. Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) e a atuação mais firme da Autoridade Nacional de Proteção de Dados (ANPD), as empresas perceberam que aderir a normas reconhecidas pode facilitar a adequação legal.

A ISO 27001, inclusive, alinha-se a diversas leis de proteção de dados, como a LGPD, ajudando as empresas a cumprir requisitos legais de segurança da informação. Em setores regulados e em empresas que lidam com grande volume de dados pessoais, a busca pela certificação aumentou como forma de demonstrar às auditorias e stakeholders que boas práticas estão implementadas.

Benefícios estratégicos na implementação da norma

Ter a ISO 27001 tem sido visto como um fator importante na conquista e retenção de contratos, especialmente em setores altamente sensíveis à segurança digital, destacando as empresas certificadas em um ambiente competitivo e exigente.

Outro benefício relevante está relacionado à conformidade regulatória. Com o avanço da fiscalização sobre a proteção de dados, especialmente em relação à LGPD e

Divulgação

Sylvio Sobreira Vieira

demais normativas, empresas certificadas na ISO 27001 têm maior facilidade em demonstrar conformidade com leis e regulamentos. A norma estabelece uma estrutura robusta que cobre diversas exigências legais, reduzindo o risco de sanções e fortalecendo a imagem das empresas perante auditorias e autoridades, confirmando o compromisso com padrões rigorosos de segurança.

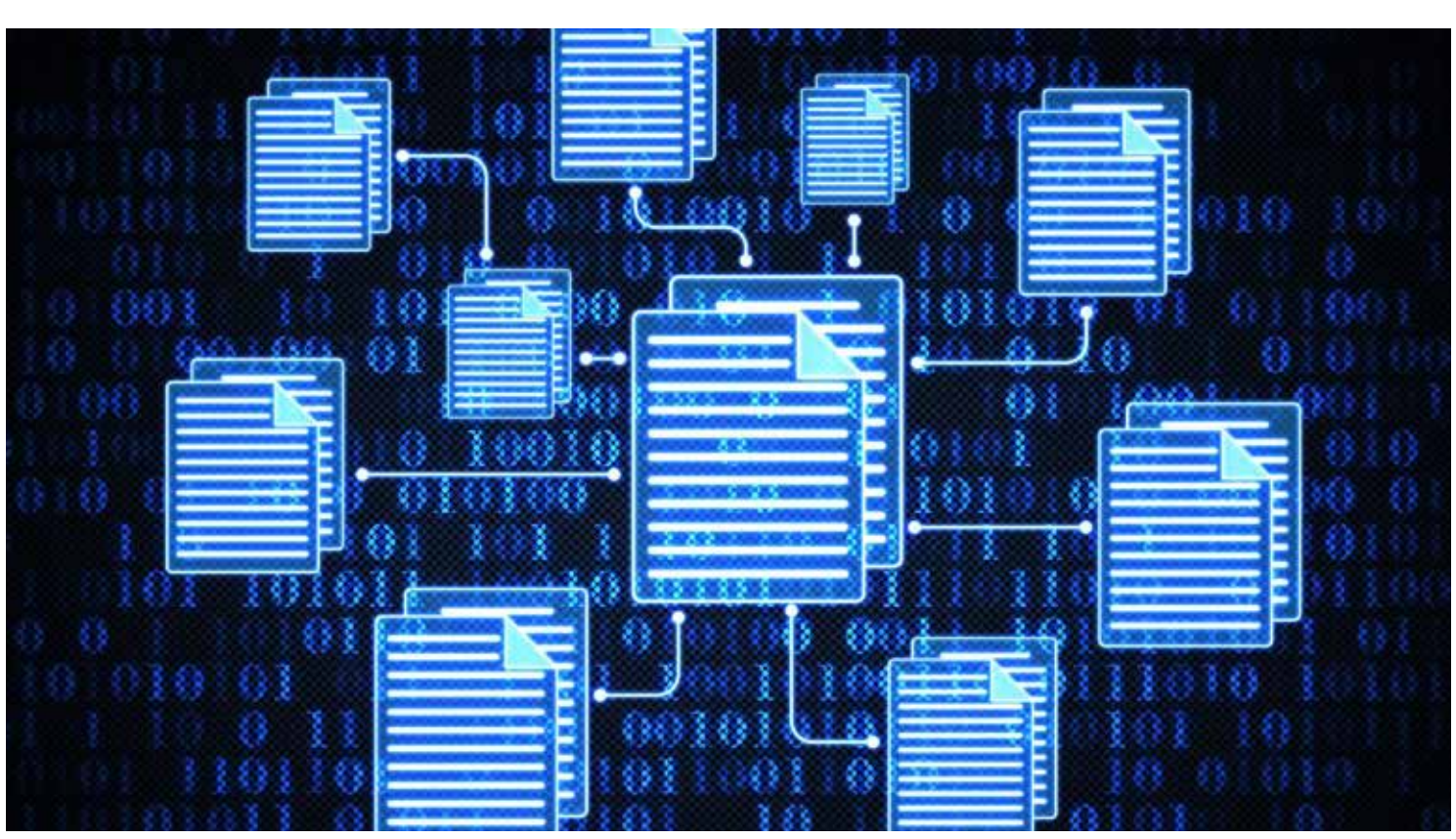
Finalmente, a certificação ISO 27001 promove uma redução significativa de riscos e incidentes de segurança por meio da gestão proativa das ameaças digitais. As empresas certificadas identificam e tratam vulnerabilidades de forma contínua, fortalecem a resiliência frente a ataques e otimizam processos internos de governança e cultura de segurança. Isso não apenas previne danos financeiros e reputacionais, mas também melhora a eficiência operacional geral, facilitando negócios e ampliando oportunidades em mercados nacionais e internacionais que exigem padrões elevados de proteção da informação.

Tendências futuras

A dinâmica da segurança da informação aponta para uma continuidade – e possivelmente aceleração – das tendências atuais. Especialistas preveem que a adoção de sistemas de gestão (como o SGSI da ISO 27001) continuará em alta nos próximos anos, acompanhando tanto a evolução das ameaças quanto o endurecimento das exigências de conformidade. Mundialmente, projeções indicam crescimento robusto nas certificações de segurança: a busca pela ISO 27001 aumentou cerca de 45% recentemente devido a leis globais de proteção de dados mais rigorosas.

Um ponto importante no horizonte próximo é a transição para a nova versão ISO/IEC 27001:2022. Publicada em outubro de 2022, a atualização da norma reflete as mudanças ocorridas na última década – incorporando novos controles para riscos em nuvem, threat intelligence e desenvolvimento seguro de software, entre outros aspectos. Os motivos que levaram à revisão incluíram a evolução tecnológica e o aumento da digitalização dos negócios, além do aprendizado obtido com a aplicação prática da norma nos últimos anos.

As empresas certificadas terão até outubro de 2025 para migrar seus sistemas para a nova edição.



D3Damon_CANVA

Outro fator importante é a integração da segurança da informação com outras dimensões de governança e gestão corporativa. Temas como privacidade de dados e continuidade de negócios estão cada vez mais entrelaçados à segurança.

Normas complementares – como a ISO/IEC 27701, focada em privacidade, expansão da 2700, e a ISO 22301, com foco na gestão da continuidade de negócios – vêm ganhando espaço lado a lado com a 27001. A adoção conjunta desses referenciais cria um ecossistema de governança integrado, capaz de abordar desde a proteção de dados pessoais até a resiliência contra desastres ou indisponibilidades.

Em essência, a gestão de segurança da informação passará a ser tratada não mais como um projeto pontual de certificação, mas como um processo dinâmico e permanente, parte integrante da estratégia de negócios. No ambiente de negócios atual, no qual confiança e resiliência digital são diferenciais competitivos, esse compromisso torna-se não apenas desejável, mas essencial para a sustentabilidade e sucesso de empresas no Brasil.

(*) CEO & Head Consulting da SVX Consultoria.