Governança em Segurança da Informação: por que ela é tão importante para os negócios?

Thaís Cristine dos Anjos Oliveira[1]

Resumo: A Governança em Segurança da Informação visa assegurar a confidencialidade, integridade e disponibilidade das informações por meio de um conjunto de controles, políticas e procedimentos que, coordenados, irão proteger a organização contra vazamentos, ataques cibernéticos e outros incidentes que possam comprometer a continuidade de seus negócios. Este artigo pretende apresentar os benefícios que um programa de governança nestes moldes pode proporcionar para as empresas, como, por exemplo, a redução do risco de violação de informação e de ações fraudulentas de várias naturezas, a criação da cultura de segurança da informação, e a continuidade dos negócios, que mantém a empresa em alto padrão de competitividade. Além disso, serão apresentados os desafios encontrados na implementação da Governança em Segurança da Informação, como a resistência por parte da Alta Liderança em adquirir soluções tecnológicas de segurança, até as barreiras no aculturamento em segurança nas organizações. Por fim, será debatido que a Governança em Segurança da Informação pode iniciar de forma muito simples e amadurecer no mesmo ritmo que a organização adere às boas práticas de mercado, muitas vezes, sem necessidade de tantos ou altos investimentos.

Palavras-chave: governanca; segurancadainformacao; cultura; investimento; continuidadedenegocios.

Information Security Governance: Why is it so important for business?

***Abstract**: Information Security Governance aims to ensure the confidentiality, integrity, and availability of information through a set of controls, policies, and procedures that, when coordinated, will protect the organization against leaks, cyberattacks, and other incidents that may compromise the continuity of its business. This article aims to present the benefits that a governance program of this nature can provide for companies, such as the reduction of the risk of information breaches and fraudulent actions of various kinds, the creation of an information security culture, and business continuity, which keeps the company at a high standard of competitiveness. Additionally, the challenges encountered in implementing Information Security Governance will be presented, such as resistance from Senior Leadership in acquiring security technology solutions, to barriers in security acculturation within organizations. Finally, it will be discussed that Information*

[1] Graduada em Administração de Empresas pela Unihorizontes e Pós-graduada em Gerenciamento Estratégico de Projetos pela Universidade FUMEC. Possui certificações ITIL, ISO27001 e Auditora Líder ISO27001 e ISO27701 pela PeopleCert, Exin e QMS Brasil, respectivamente. Atualmente atua como Assessora de Tecnologia da Informação e Governança na administração pública do Estado de Minas Gerais.

Security Governance can start very simply and mature at the same pace as the organization adheres to good market practices, often without the need for significant or high investments.

***Keywords**: governance; cybersecurity; culture; investments; businesscontinuity.*

1 INTRODUÇÃO

A informação representa um ativo fundamental para qualquer organização, possivelmente o mais valioso, e deve ser protegida com o mesmo cuidado dispensado aos bens físicos. O dicionário Michaelis define informação como “Ato ou efeito de informar(-se)/Conjunto de conhecimentos acumulados sobre certo tema por meio de pesquisa ou instrução/Explicação ou esclarecimento de um conhecimento, produto ou juízo; comunicação/Notícia trazida ao conhecimento do público pelos meios de comunicação”, dentre outros conceitos. A informação acrescenta algo ao conhecimento de uma realidade analisada (Machado, 2014).

Sordi (2015) aponta que a informação é a interpretação de um conjunto de dados segundo um propósito relevante para o leitor. São inúmeros os aspectos que tornam a informação importante para as empresas: orienta a tomada de decisões, permite a identificação de oportunidades de mercado e fornece *insights* sobre as necessidades e preferências dos clientes, fomenta a capacidade empresarial de perpetuar seus negócios mesmo diante das adversidades.

Neste sentido, a segurança da informação é a disciplina dedicada a proteger os ativos de informação contra ameaças, acessos não autorizados, violações e quaisquer outros incidentes que possam comprometer seu valor e sua finalidade. É um conjunto de orientações, normas, procedimentos, práticas, políticas e demais ações que visam proteger as informações, possibilitando que o negócio da organização seja realizado e a sua missão atingida (Fontes, 2012).

A segurança da informação se baseia em três pilares fundamentais: a confidencialidade, que visa garantir que a informação esteja acessível somente a quem necessita com sigilo adequado; a integridade, que assegura que a informação seja confiável, exata e sem modificações não autorizadas; e a disponibilidade, que objetiva manter a informação disponível, em tempo integral, para quem precisa

acessá-la. Esta tríade é conhecida como CIA, sigla da língua inglesa *Confidentiality, Integrity, Availability* (Machado, 2014).

A temática da segurança da informação tem ocupado significativos espaços diante da crescente e contínua transformação tecnológica observada no mundo. O impacto está generalizado; as empresas seguem impulsionadas pela necessidade de adaptação a um ambiente de negócio cada vez mais veloz e competitivo, a sociedade vivenciando as facilidades digitais em diversos segmentos, e os titulares de dados pessoais observando sua privacidade ser protegida pela legislação vigente.

É urgente explanar que a segurança da informação não pode mais ser vista como um assunto secundário ou que trará gastos extras aos orçamentos corporativos, ao contrário, a SI é fundamental para atuar contra as diversificadas ameaças cibernéticas, visando perpetuar a continuidade dos negócios, minimizar os riscos e maximizar o retorno sobre os investimentos. (Manoel, 2014).

A partir disto, a governança em segurança da informação surge como a base crucial para garantir a confidencialidade, integridade e disponibilidade dos ativos de informação. A implementação de controles, políticas, procedimentos e boas práticas de mercado oferta uma considerável elevação da maturidade em processos de SI nas empresas, tornando-as mais competitivas, seguras e confiáveis. De acordo com Fontes (2008) a governança em segurança da informação é uma necessidade organizacional e precisa estar totalmente atrelada à gestão da segurança da informação.

2 METODOLOGIA

Este artigo tem natureza conceitual e qualitativa e se propõe a explorar os princípios, abordagens e aplicabilidade da governança da segurança da informação na realidade das organizações, independentemente de seu nicho de negócio, tamanho, complexidade e demais fatores preponderantes. A escrita está vinculada ao referencial teórico com definições sobre governança de segurança da informação e sua aplicabilidade, por meio de literatura, além da experiência da autora no tema.

3 REFERENCIAL TEÓRICO

3.1 Informação

A informação é um recurso fundamental para os negócios e para alcançar a missão de uma organização (Fontes, 2012). O valor da informação pode ser medido pelo impacto de sua ausência ou pelo uso indevido de terceiros, além da relação de dependência em seus processos de negócios (Manoel, 2014).

> "O valor da informação vai além das palavras, escritas, números e imagens: conhecimentos, conceitos, ideias e marcas são exemplos de formas intangíveis de informação. Em um mundo interconectado, informações e outros ativos associados merecem ou requerem proteção contra várias fontes de risco, sejam naturais, acidentais ou deliberadas. " (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, 2022, p. 9)

As empresas devem estar atentas às vulnerabilidades e ameaças às quais estão sujeitas dentro de seu nicho de mercado, visando, essencialmente, resguardar suas estratégias e segredos de negócios. Dados, informações e conhecimento são o cerne da inteligência competitiva, portanto, devem ser gerenciados com atenção aos seus detalhes particulares e minuciosamente preservados.

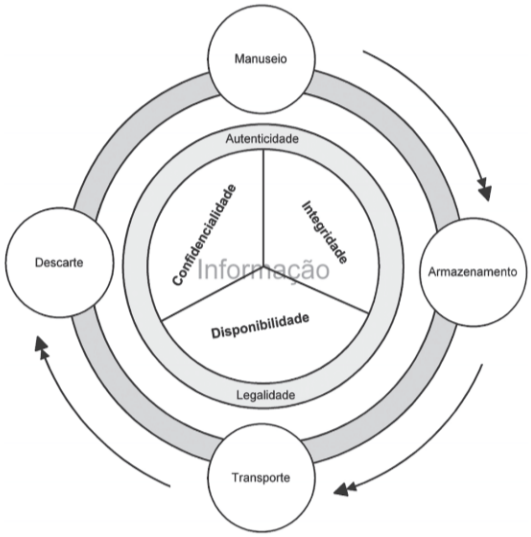
Vancim (2016) aponta que a informação dá sentido às coisas, resolvendo problemas, criando estratégias, tomando decisões e, até, formulando o pensamento humano. É um recurso estratégico para as organizações, podendo levá-la ao sucesso ou ao fracasso.

> "A Era da Informação se desenvolve no momento em que é estabelecida uma plataforma por meio da qual se torna possível a todos os indivíduos com acesso a ela, independentemente de onde estejam, trocar experiências, compartilhar formas diferentes de fazer as coisas, comprar, vender e criar coletivamente". (CABRAL, CAPRINO, 2015, p. 1)

Diante disto, percebe-se o alto grau de dependência das empresas em relação à informação e aos elementos de infraestrutura que a mantém (Sêmola, 2013), o que reforça a necessidade de aprimoramentos e vigília constante, dado o panorama tecnológico e informacional cada dia mais complexo.

A informação deve ser protegida em todo seu ciclo de vida, isto é, em todo seu histórico, desde a concepção até a eliminação definitiva. Sêmola (2013) aponta quatro fases atreladas ao ciclo de vida da informação: a fase de manuseio, quando a informação é criada e manipulada, a fase de armazenamento, que estipula os repositórios de guarda da informação, a fase de transporte, que diz respeito ao método em que são compartilhadas e/ou enviadas e, por fim, a fase de descarte, que dita como a informação deve ser eliminada para que não haja intercepção e/ou recuperação. Cabe ressaltar que estas fases se aplicam a todo tipo de informação, sejam elas físicas ou digitais ou em qualquer formato que se encontram.

Figura 1 – Ciclo de vida da informação



Fonte: Sêmola, 2013

3.2 Segurança da Informação

Dado o cenário apresentado sobre a importância dos ativos de informação no contexto empresarial e, considerando a velocidade vertiginosa em que a tecnologia avança, é vital estabelecer mecanismos para salvaguardar as informações e os dados pessoais. Gerenciar todo este arcabouço informacional de um modo eficaz é um grande desafio para as organizações, e a segurança da informação deixou de ser vista como uma atividade secundária (Gouveia, 2016).

A segurança da informação é o conjunto de normas, procedimentos e políticas que visa proteger informações e dados pessoais para que a empresa possa atingir seus

objetivos estratégicos (Fontes, 2012), além de resguardá-los contra acessos não autorizados, uso indevido, modificação e destruição indesejadas (Batista, 2012).

> "Os objetivos da segurança da informação baseiam-se na identificação adequada dos ativos de informação de uma empresa, atribuindo valores para estes ativos, desenvolvimento, documentação e implementação de políticas de segurança, procedimentos, normas e diretrizes, que devem fornecer integridade, confidencialidade e disponibilidade da informação. " (MACHADO, 2014, p. 12)

Para a norma ABNT ISO/IEC 27002:2022 a segurança da informação é "alcançada por meio da implementação de um conjunto adequado de controles, incluindo políticas, regras, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*". Isso inclui a implementação de *firewalls*, antivírus, criptografia, múltiplo fator de autenticação e outras medidas técnicas de segurança, com o intuito de evitar ameaças cibernéticas como, por exemplo, *malware* e *phishing*, além de vulnerabilidades em sistemas e infraestrutura de tecnologia.

A implementação de medidas técnicas de segurança eficazes assegura que as operações da organização continuem mesmo diante de incidentes de segurança. Isso inclui a proteção contra ataques cibernéticos, desastres naturais e/ou outras ameaças que possam interromper as atividades.

> "Os controles de segurança da informação são contramedidas de gestão, ou operacionais, ou ainda técnicas, recomendadas para os sistemas de informação, para proteger a confidencialidade, integridade e disponibilidade de um sistema e da sua informação. Os controles de segurança, quando utilizados de forma adequada, podem prevenir, limitar ou deter uma ameaça aos ativos de uma organização. " (GOUVEIA, 2016, p.8)

A segurança da informação se baseia em três pilares fundamentais: a confidencialidade, integridade e disponibilidade. A confidencialidade visa garantir o nível necessário de sigilo das informações, evitando divulgações e compartilhamentos não autorizados (Machado, 2014); a integridade preserva a informação para que se mantenha na mesma condição em que foi disponibilizada, em exatidão (Manoel, 2014) e a disponibilidade garante que as informações estejam acessíveis a quem está autorizado a acessá-la, no momento em que necessitarem

(Vancim, 2016). Esta tríade é a base fundamental para implementar a estratégia de cibersegurança nas organizações.

Figura 2 – Pilares da Segurança da Informação

Fonte: https://www.security.ufrj.br/dicas/o-que-e-um-incidente-de-seguranca-da-informacao/

Para definir uma estratégia de segurança, a organização precisa entender o contexto em que está inserida, avaliar questões internas e externas, mapear as expectativas e necessidades de seus *stakeholders*, além de identificar potenciais vulnerabilidades que podem afetar seus negócios. De acordo com Hintzbergen *et al* (2018) para que as empresas conheçam as ameaças às quais estão sujeitas, é necessário aplicar uma metodologia de análise de riscos a fim de identificar os ativos que serão protegidos e como serão protegidos. Um risco está associado à incerteza sobre o futuro, seja no curto ou longo prazo (Gil, 2013); trazendo para a realidade cibernética, um risco é a probabilidade de uma pessoa mal-intencionada tirar proveito de uma vulnerabilidade ou brecha de segurança impactante às atividades daquela organização.

A partir de uma análise de riscos bem elaborada, a empresa poderá visualizar as prováveis ameaças – internas e externas – em seu ambiente e traçar estratégias de contorno e mitigação. Neste momento surge um programa de segurança da informação atrelado a uma governança robusta e estruturada, tema que será discorrido no tópico a seguir.

3.3 Governança em Segurança da Informação

A palavra governança, em linhas gerais, diz respeito ao ato de governar, administrar ou determinar o rumo de uma ou mais atividades, uma empresa e, até, uma nação. Apontando para o universo empresarial, a Governança Corporativa é estruturada por processos, pessoas e tecnologia, visando o atingimento dos objetivos estratégicos de uma organização. De acordo com Tomiatti (2012), a governança corporativa "fundamentou-se para criar um conjunto eficiente de mecanismos para assegurar que o comportamento dos executivos esteja sempre alinhado com o interesse dos acionistas".

> "Governança corporativa é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. " (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA - IBGC, 2023, p.17)

Neste sentido, a Governança em Segurança da Informação implementa controles, políticas e procedimentos que protegem a confidencialidade, integridade e disponibilidade das informações, a fim de assegurar que as necessidades de segurança da informação numa empresa estejam alinhadas com sua estratégia de negócio. Um modelo de governança bem estruturado é crucial para proteger essas informações de ameaças como vazamentos de dados, ataques cibernéticos e outros riscos de segurança.

> "A governança da segurança da informação é a utilização de recursos para garantir a implementação eficaz da segurança da informação e proporciona garantias de que as diretivas relativas à segurança da informação serão seguidas e o órgão diretivo receberá relatórios confiáveis e relevantes sobre atividades relacionadas à segurança da informação. " (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT, ISO/IEC 27014, 2020, p. 5)

São inúmeros os benefícios percebidos ao estabelecer uma Governança em Segurança da Informação estruturada e contínua, como a proteção de informações confidenciais e sensíveis, a melhoria da conformidade regulatória e legal, a redução do risco de violações de dados e a criação de uma cultura de segurança. O advento da Lei Geral de Proteção de Dados – LGPD, neste sentido, proporcionou benefícios não apenas aos titulares de dados pessoais, mas também às organizações. Adequar-

se às regras da legislação visa resguardar sua reputação, elevar seu diferencial competitivo e transformação digital, além de estabelecer alianças cada vez mais transparentes e sólidas.

Um ponto importante a ser elucidado é o grande benefício ao determinar um programa de conscientização e cultura em segurança na organização. De acordo com Sêmola (2013) "os recursos humanos são considerados o elo mais frágil da corrente, pois são responsáveis por uma ou mais fases de processo de segurança da informação", ou seja, o comportamento humano pode comprometer consideravelmente a operação corporativa, por erros intencionais ou não intencionais. Investir em treinamento e conscientização do corpo funcional poderá minimizar riscos de vazamentos de senhas, ataques como engenharia social e *phishing*, redução de custos com incidentes de segurança, aumento da reputação da empresa perante suas partes interessadas, dentre outros.

> "Torna-se necessário a cada dia capacitar um número maior de profissionais nos conceitos e boas práticas em segurança da informação e, assim, fazer com que os processos necessários para a redução dos riscos e a proteção dos ativos sejam criados e que a cultura de segurança se espalhe cada vez mais pelas empresas. " (MACHADO, 2014, p.10)

Apesar de seus benefícios, a implementação da Governança em Segurança da Informação também oferece grandes desafios. Como dito anteriormente, os objetivos da segurança da informação devem estar atrelados à estratégia de negócio da empresa e, para isso, é necessária a visibilidade da Alta Direção sobre os riscos cibernéticos aos quais a organização está sujeita, além dos requisitos legais. Torna-se, portanto, o primeiro grande desafio enfrentado: apresentar aos tomadores de decisão o cenário cibernético e suas vulnerabilidades e convencê-los sobre as benesses de um programa de cibersegurança efetivo, com investimentos eficazes, agregando valor. Este papel é usualmente do CISO (*Chief Information Security Officer*) ou por quem responde pela área de segurança na organização. Diante de uma realidade tão preocupante, é crucial que a Alta Liderança abandone a ideia de que a cibersegurança é uma simples (e alta) despesa e a enxerguem como uma necessidade vital para a proteção da Companhia.

Outro grande desafio enfrentado é a constante evolução das ameaças cibernéticas. À medida que a tecnologia avança, os cibercriminosos desenvolvem métodos mais sofisticados para explorar vulnerabilidades, das mais diversificadas e modernas. Para enfrentar este cenário tão volátil, é fundamental adotar uma abordagem proativa e adaptável como atualizações das tecnologias de segurança, monitoramento e análise contínuos e educação e treinamento recorrentes. A maioria destas ações requer consideráveis investimentos, o que retoma à preocupação do primeiro desafio, detalhado acima. Tzu (2019) aponta que "(...) se conhecermos nosso inimigo (ambiente externo) e a nós mesmos (ambiente interno), não precisaremos temer o resultado de uma centena de combates".

3.3.1 Modelo de governança em segurança da informação

Existem vários modelos de governança em segurança da informação que podem ser aplicados nas organizações, cuja proposta é direcionar esforços sobre como esta governança deve ser gerenciada e implementada e quem será o responsável. Não existe modelo ideal; o necessário é identificar aquele que seja mais aderente à realidade da organização, considerando fatores como o mercado em que está inserida, seu porte e seu nível de maturidade em segurança da informação. Este modelo deve assegurar que as informações financeiras, operacionais e gerenciais são íntegras e confiáveis e que há cumprimento das exigências legais e regulatórias (Albertin, Moura, 2004).

> "Cada modelo de governança é um componente integrante da governança corporativa de uma organização, que enfatiza a importância do alinhamento com os objetivos estratégicos do negócio, gerando valor para as partes interessadas". (MANOEL, 2014, p.14)

O ponto chave nesta implementação é o comprometimento da Alta Liderança. Gestores e tomadores de decisão engajados e comprometidos com os objetivos da segurança da informação em sua Companhia serão essenciais para o sucesso da governança e seus sub-processos, além de se tornarem exemplo para todos os colaboradores na solidez da cultura em segurança.

Partindo deste princípio, é fundamental elaborar diversas análises do contexto empresarial. A seguir serão apresentados itens essenciais que podem compor um

modelo de governança em segurança da informação de acordo com a realidade organizacional.

- Análise contextual

A primeira análise macro a ser realizada é a Matriz SWOT (Sigla inglesa para *Strengths, Weaknesses, Opportunities e Threats*) onde serão avaliados aspectos do ambiente interno e externo: as forças, oportunidades, ameaças e fraquezas da organização de acordo com suas especificidades, o que já apresentará um panorama relevante para a segundo diagnóstico, que é a análise riscos de segurança.

Figura 3 – Matriz SWOT

Fonte: https://rockcontent.com/br/blog/como-fazer-uma-analise-swot/

A análise de risco de segurança é um processo sistemático para identificar, avaliar e tratar riscos que podem comprometer os ativos de informação. A partir da análise de riscos e, tendo claras todas as ameaças às quais está sujeita, a organização poderá traçar suas estratégias e medidas de segurança para fornecer uma resposta eficaz a tais vulnerabilidades, por meio – mas não se limitando – a um plano de resposta a incidentes. Este plano é essencial para que a empresa possa lidar adequadamente com incidentes de segurança, minimizando danos e recuperando rapidamente suas operações.

- Normas e *frameworks* internacionais

São diretrizes e normatização de condutas de alto nível, muito utilizadas para apoiar a organização a identificar o seu nível de maturidade em segurança da informação e proteção de dados. A implementação destes *frameworks* potencializará a conformidade aos requisitos de segurança da informação e proteção de dados, o que

pode, ainda, proporcionar certificações de padronização de normas e elevar o patamar das empresas a níveis internacionais.

Tabela 1 – Detalhamento das normas ABNT (Associação Brasileira de Normas Técnicas)

Normas	Definição	Finalidade
ABNT NBR ISO/IEC 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos	Estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação	Adoção de um conjunto de controles de segurança da informação, incluindo orientação para implementação.
ABNT NBR ISO/IEC 27014:2021	Segurança da informação, segurança cibernética e proteção da privacidade - Governança da segurança da informação	Conceitos, objetivos e processos para a governança da segurança da informação.
ABNT NBR ISO/IEC 27005:2023	Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação	Realizar atividades de gestão de riscos de segurança da informação, especificamente avaliação e tratamento de riscos de segurança da informação.
ABNT NBR ISO/IEC 27701:2019	Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.	Estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da privacidade da informação na forma de extensão para a ISO/IEC 27001 e ISO/IEC 27002

Fonte: Elaborado pela autora

Tabela 2 – Detalhamento de *frameworks* internacionais que apoiam a segurança da informação

Framework	Definição	Finalidade
NIST *Cybersecurity (National Institute of Standards and Technology)*	Agência do governo dos Estados Unidos que desenvolve padrões, diretrizes e melhores práticas para ajudar organizações a gerenciar e reduzir	Melhorar a segurança da informação e o gerenciamento de riscos cibernéticos.

	riscos de segurança cibernética.	
COBIT *(Control Objectives for Information and Related Technologies)*	Governança e gestão de TI.	Desenvolver, implementar, monitorar e melhorar práticas de governança e gestão de TI.
ITIL V4 (*Information Technology Infrastructure Library*)	Gestão de serviços de TI.	Gestão eficaz dos serviços de TI gerando valor agregado aos clientes.

Fonte: Elaborado pela autora

- Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é uma das diretrizes mais importantes para formalizar o tema segurança da informação numa Companhia. Usualmente é um documento normativo oficial, assinado pela Alta Direção e deve especificar termos e definições consideráveis para garantir a compreensão clara e uniforme entre todos os colaboradores a respeito do tema, além de papéis e responsabilidades dos envolvidos. A Política de Segurança da Informação deve ser visitada continuamente e revisada sempre que houver mudanças expressivas no ambiente externo, ou por atualização de tecnologias, avanços legais, incidentes de segurança, dentre outros fatores.

> "Uma política de segurança da informação deve ser sólida, considerando com extrema particularização e detalhamento as características de cada processo de negócio, perímetro e infraestrutura, materializando-a através de diretrizes, normas, procedimentos e instruções que oficializarão o posicionamento da empresa ao redor do tema (...)" (SÊMOLA, 2013, p.33)

A PSI, como um documento corporativo de maior peso informacional, pode estar acompanhada de outras políticas/normativos que sustentarão demais condutas que devem ser seguidas no ambiente empresarial. Podemos citar, neste contexto, políticas de senhas seguras, de classificação da informação, de uso seguro de internet, correio eletrônico, *backups*, acessos físico e lógico, dentre outras diretrizes relativas. Relevante apontar que a PSI como um arcabouço de informações procedimentais e comportamentais, deve fazer menção ou estar atrelada à temas complementares, como Código de Ética e Conduta e Política de Privacidade e Proteção de Dados.

- Cultura e conscientização em segurança da informação

O fator de sucesso de um programa de segurança da informação numa Companhia é investir em cultura e conscientização dos empregados. A maioria dos incidentes de segurança é oriunda de falhas humanas, como, por exemplo, clicar em *links* maliciosos, utilizar senhas fracas, compartilhar informações indevidamente, dentre outras ações, o que pode acarretar em perdas financeiras, prejudicar a reputação da empresa e desencadear sanções legais.

Por meio da conscientização, o corpo funcional compreenderá a importância da segurança da informação – não somente no âmbito profissional, mas também na vida pessoal – se tornará mais vigilante e capaz de reconhecer possíveis ameaças e incidentes de segurança. Proteger os ativos valiosos da organização é responsabilidade de todos, deve fazer parte do DNA da empresa, assim, todos estarão alinhados com a missão e poderão garantir um ambiente seguro para si e para os clientes.

A jornada de cultura e conscientização em segurança da informação começa no topo, com líderes engajados e comprometidos em elevar a segurança e se tornarem exemplo para suas equipes. A implementação desta jornada requer uma abordagem estratégica, com métodos de aprendizagem inclusivos que alcancem todos os empregados, dos cargos mais simples até os mais complexos, utilizando ferramentas como palestras, cartilhas, treinamentos, vídeos interativos, plataformas de gamificação, dentre outros. Não necessariamente estas ações demandam custos; podem iniciar de forma simples, sempre visando o nivelar o conhecimento de todos na empresa com o mesmo objetivo de elevar a maturidade em segurança da informação na Companhia.

4 CONSIDERAÇÕES FINAIS

Neste artigo foram apresentados os conceitos de informação, segurança da informação e governança em segurança da informação de acordo com grandes autores e especialistas na área, visando demonstrar a importância do tema no contexto empresarial dado o cenário tecnológico cada dia mais avançado e inconstante.

Compreender todas as vulnerabilidades e ameaças cibernéticas às quais as organizações estão sujeitas não é tarefa fácil e requer monitoramento e aprimoramento constante e, ao implementar um programa de governança robusto e estruturado, as chances de mitigação destes incidentes tornam-se mais tangíveis e controláveis. A segurança da informação é a disciplina crucial para a continuidade dos negócios de uma Companhia e deve ser encarada como investimento primário e essencial no orçamento corporativo.

As principais conclusões apontam que um modelo de governança em segurança da informação consolidado não apenas protege os ativos de informação e os dados pessoais dos titulares, como preserva a reputação da empresa, eleva o nível de maturidade em segurança na organização e garante a conformidade regulatória. Para escolher o modelo que mais se adequa à realidade da organização, é fundamental analisar seu ambiente interno e externo, seu nível atual de maturidade cibernética e sua capacidade em atuar em defesa de seus processos de negócios, serviços e produtos.

Além disto, investir em cultura e conscientização em segurança da informação também é um fator fundamental para reduzir incidentes de segurança com origem de falhas humanas e transformar cada colaborador em uma linha de defesa ativa. Um corpo funcional treinado e engajado, combinado com as tecnologias de ponta implementadas, cria um ambiente propício a elevar os padrões de segurança na empresa, estimula a cultura em cibersegurança e fortalece a confiança dos *stakeholders*. A longo prazo, esta abordagem é a chave para construir uma organização resiliente e preparada para enfrentar os desafios cibernéticos do futuro.

Em suma, a governança em segurança da informação permite que as organizações identifiquem, avaliem e mitiguem ameaças e incidentes de maneira proativa, alinhando as diretrizes de segurança com os objetivos de negócios. A colaboração entre todas as áreas da empresa, a adoção de políticas, diretrizes e normativos claros e a promoção da cultura de segurança são elementos essenciais para o sucesso dessa governança. Ao investir em governança de segurança da informação, as empresas

não só protegem seus dados e sistemas, mas também constroem uma base sólida para crescimento e inovação sustentáveis.

REFERÊNCIAS

ALBERTIN, Alberto L.; MOURA, Rosa M. de. *Tecnologia de Informação*. Grupo GEN, 2004. *E-book.* ISBN 9786559770601. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786559770601/. Acesso em: 08 mai. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002 - *Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação*. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27014 – *Segurança da informação, segurança cibernética e proteção da privacidade – Governança da segurança da informação.* Rio de Janeiro, 2021.

BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Izabelly S.; *et al. Fundamentos de segurança da informação*. Grupo A, 2018. E-book. ISBN 9788595025875. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595025875/. Acesso em: 08 mai. 2024.

BATISTA, Emerson .O. *Sistemas de Informação: o uso consciente da tecnologia para o gerenciamento*, 2ª ed. São Paulo. Editora Saraiva, 2012.

CABRAL, Carlos, CAPRINO, Willian Okuhara. *Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados*. Rio de Janeiro: Brasport, 2015. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=CeInBgAAQBAJ&oi=fnd&pg=PA1&dq=fundamentos+de+seguran%C3%A7a+da+informa%C3%A7%C3%A3o&ots=txs3OPbd2R&sig=03zDgNH3iZdOn-ZcWduCEk0xCro&redir_esc=y#v=onepage&q&f=false. Acesso em: 08 mai. 2024.

FONTES, Edison L. G. *Praticando a Segurança da Informação*. Rio de Janeiro: Brasport, 2008. Disponível em: https://www.google.com.br/books/edition/Praticando_a_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o/Gh82CgAAQBAJ?hl=pt-BR&gbpv=1. Acesso em: 16 abr. 2024.

FONTES, Edison L. G. *Segurança da informação - 1ª edição*. SRV Editora LTDA, 2012. E-book. ISBN 9788502122185. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788502122185/. Acesso em: 08 mai. 2024.

GIL, Antonio de L.; ARIMA, Carlos H.; NAKAMURA, Wilson T. *Gestão: controle interno, risco e auditoria*. SRV Editora LTDA, 2013. E-book. ISBN 9788502197558. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788502197558/. Acesso em: 03 jun. 2024.

GOUVEIA, Luis B. *Gestão da Segurança da Informação*. Portugal, 2016. Disponível em: https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf. Acesso em: 05 jun. 2024.

HINTZBERGEN, J; HINTZBERGEN. K; SMULDERS, A; BAARS, H.; *et al*. Tradução Alan de Sá. *Fundamentos da segurança da informação com base na ISO 27001 e na ISO 27002.* Rio de Janeiro. Brasport, 2018.

INFORMAÇÃO. *In*: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/informa%C3%A7%C3%A3o/. Acesso em: 06 mai. 2024.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. *Código das Melhores Práticas de Governança Corporativa.* 6ª ed. São Paulo, 2023. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640&assessment=1. Acesso em: 05 jun. 2024.

MACHADO, Felipe N. R. S*egurança da informação - princípios e controle de ameaças - 1ª edição - 2014*. SRV Editora LTDA, 2014. E-book. ISBN 9788536531212. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788536531212/. Acesso em: 08 mai. 2024.

MANOEL, Sergio S. *Governança de segurança da informação: Como criar oportunidades para o seu negócio.* Rio de Janeiro. Brasport, 2014.

MORAIS, Izabelly S.; GONÇALVES, Glauber R. B. *Governança de tecnologia da informação.* Grupo A. *E-book.* ISBN 9788595023437. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788595023437/. Acesso em: 05 jun. 2024.

MORETTI, Cláudio S. *Segurança das informações: as pessoas são o elo mais fraco.* USA. Monee, Illinois. Editora: Independently published. 2020. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/10/seguranca-das-informacoes-as-pessoas-sao-o-elo-mais-fraco.pdf. Acesso em: 24 abr. 2024.

SÊMOLA, Marcos. *Gestão da Segurança da Informação - Uma Visão Executiva. 2ª edição.* Rio de Janeiro: GEN LTC, 2013. Disponível em: https://www.dropbox.com/s/xko32pz3wfj3o8i/Livro_Gestao_de_Seguranca_da_Informacao_uma%20visao%20executiva_por_Marcos_Semola_Dominio_Publico_Jun2021.pdf?e=1. Acesso em: 08 mai. 2024.

SORDI, José O de. *Administração da informação: fundamentos e práticas para uma nova gestão do conhecimento.* SRV Editora LTDA, 2015. E-book. ISBN 9788502634817. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788502634817/. Acesso em: 08 mai. 2024

TOMIATTI, Thalita. S. *Governança de TI.* 2012. Faculdade de Tecnologia de São Paulo, São Paulo, 2012. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc00048.pdf>. Acesso em: 05 jun. 2024.

TZU, Sun. *A arte da guerra*. 3ª ed. Jandira, São Paulo. Ciranda Cultural, 2019.

VANCIM, Flavia. *Gestão de Segurança da Informação. 1ª ed*. Rio de Janeiro, SESES, 2016.