Administração de Empresas em revista unicuritiba
Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-7548

A INTERSECÇÃO DA SEGURANÇA DA INFORMAÇÃO E A GOVERNANÇA CORPORATIVA

EDUARDO OLIVEIRA AGUSTINHO
Professor Titular de Direito Empresarial no Curso de Graduação e Pós-graduação em Direito da Pontifícia Universidade Católica do Paraná (PUCPR). Doutor em Direito Econômico e Desenvolvimento pela Pontifícia Universidade Católica do Paraná (PUCPR). Pesquisador visitante da Université Paris I – Panthéon-Sorbonne. Membro do Grupo de Estudos em Análise Econômica do Direito (GRAED). Sócio do NGA Advogados.

GREGÓRIO DE OLIVEIRA FURQUIM
Mestrando em Direito e Desenvolvimento pela Pontifícia Universidade Católica do Paraná (PUCPR). Membro do Grupo de Estudos em Análise Econômica do Direito (GRAED). Advogado.

HENRIQUE CARRARO BREMER
Mestrando em Direito pela Pontifícia Universidade Católica do Paraná. Graduado em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR). Advogado nas áreas de contratos, societário, trabalhista e cível. Além de experiência em consultoria empresarial e jurídica envolvendo metodologias de compliance e proteção de dados pessoais.

RESUMO:
Com o desenvolvimento da tecnologia, as organizações se tornam cada vez mais dependentes de sistemas e ferramentas tecnológicas que otimizam suas operações comerciais e organizacionais. Nesse sentido, o presente artigo tem como objetivo principal estabelecer alguns conceitos básicos relacionados à Segurança da Informação e a Governança Corporativa, demostrando a unificação do primeiro e do segundo tema nas questões atuais de tecnologia e atividade econômica. Evidencia-se que, muito além da preservação da integridade das informações, a Segurança da Informação, desde que estruturada de modo correto, agrega muitos benefícios a Governança Corporativa e a visão do mercado sobre a empresa, identificando-se como a Governança da Segurança da Informação, que é indispensável para as estruturas de governança atuais.

Palavras-chaves: Tecnologia; Organizações; Segurança da Informação; Governança Corporativa; Integridade.

1 CONSIDERAÇÕES INICIAIS

Na Era Digital, em que os meios de comunicação alcançaram uma proporção nunca vista e o próprio tráfego e armazenamento de informações assumiu a natureza

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: 2316-7548

eletrônica, a Segurança da Informação ou *Cibersegurança* assume uma posição indispensável para a operação das empresas e a própria estruturação e manutenção da Governança Corporativa.

Isso porque à medida que a tecnologia avança, os negócios se tornam cada vez mais digitais. Atualmente, sabemos que a tecnologia é uma grande aliada no desenvolvimento e na gestão das empresas, por esse motivo, a grande maioria das empresas são dependentes de recursos e técnicas da computação que otimizam e organizam suas operações comerciais, seja através da simples utilização de computadores, servidores de e-mail e sistemas ou então da utilização de ferramentas mais complexas, como por exemplo o *Business Intelligence (B.I).*

O fato é que todas as empresas que utilizam recursos tecnológicos, sejam eles os mais básicos ou avançados, necessitam ter uma estrutura mínima de Segurança da Informação (S.I) que proporcione a proteção dessas ferramentas e recursos contra possíveis ameaças ou eventuais incidentes de segurança.

1.1 CONCEITOS E DEFINIÇÕES

Nesse aspecto, quando falamos em Segurança da Informação, devemos entender como um conjunto de ações e ferramentas que visam a “Preservação da confidencialidade, integridade e disponibilidade da informação.”[1]

Com o objetivo de fortificar a *Cibersegurança*, atualmente algumas empresas estão aderindo ao modelo de Governança de T.I., entretanto, para entender esse conceito precisamos aprofundar no entendimento do significado de Governança Corporativa, que pode ser entendida como um “sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.” [2]

Em suma, Governança Corporativa é um conjunto de boas práticas, pautadas nos princípios da transparência, equidade, prestação de contas e da responsabilidade corporativa. Esses preceitos, materializados através das ações dentro das empresas, visam profissionalizar a gestão organizacional, trazendo o controle, transparência e

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005 Tecnologia da informação: técnicas de segurança. Rio de Janeiro, 2006.
[2] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. IBGC. Código das Melhores Práticas de Governança Corporativa. 5. ed. São Paulo: IBGC, 2015. P20

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

promoção da cultura, além de promover o cumprimento das leis e de todas as normas internas que regem a corporação, de modo que possa atingir sua missão e visão, garantindo a sua integridade e confiabilidade frente ao mercado e as partes interessadas (*Stakeholders)*.

Já a Governança de T.I (G.T.I.), é um componente da Governança Corporativa, também sendo "de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização."[3]

Ou seja, é o alinhamento estratégico entre Alta Administração e a área de T.I. da organização, resultando na implementação de processos, otimização da aplicação de recursos (humanos e financeiros), além de fornecer suporte para a tomada de decisões e assegurar a confidencialidade, integridade e disponibilidade das informações.

Apesar das terminologias carregarem certa semelhança, possuem objetivos completamente distintos, pois, a Governança de T.I. possui o foco específico nas boas práticas voltadas para o desenvolvimento e manutenção especificadamente do setor de Tecnologia da Informação da organização.

2 A INFORMAÇÃO COMO ATIVO DAS ORGANIZAÇÕES

Essa preocupação especifica com a área de T.I. das empresas, surge devido ao crescimento exponencial da utilização de tecnologias que permitem coletar, tratar e organizar dados. Dentro desse panorama, tem sido cada vez mais comum as empresas utilizarem esses conjuntos de informações para desenvolver ou atualizar novos produtos e serviços, além de acirrar a competitividade no mercado.

Esse conjunto de informação reunidas possibilita estratificar dados relevantes para as empresas, como: estatísticas de mercado, dados de macro e microeconomia, prospecção de clientes, expansão ou mudança do direcionamento do negócio, melhoria e desenvolvimento de produtos e serviços, marketing dentre outras finalidades.

[3] ITGI. COBIT 4.1: Objetivos de Controle para Informações e Tecnologias Correspondentes. Rolling Meadows, IL (EUA): IT Governance Institute, 2007. 212p.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

Esses conjuntos de dados, denominados de forma geral como “informação”, podem ser considerada um dos ativos mais importantes das empresas, principalmente quando envolve o tratamento de dados pessoais. Com a vigência da Lei Geral de Proteção de Dados, nº 13.709/2018 – LGPD, as empresas passaram a ter a obrigatoriedade de implementar medidas técnicas e organizacionais que garantam a proteção desses dados, bem como o comprimento dos direitos dos respectivos titulares de dados pessoais.

3 SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA ESTRATÉGICA DE NEGÓCIO

Por esses motivos, fica evidente que a S.I tem se tornado uma necessidade e uma oportunidade no ambiente corporativo. Prova disso é que não somente as grandes organizações já tem direcionado seus esforços para estruturar seus programas de Segurança da Informação, como também as *Startups* e empresas da Nova Economia que tratam dados como seu principal ativo.

Podemos entender como Segurança da Informação o conjunto de estratégias e ferramentas, baseada em três princípios fundamentais, sendo eles:

- **Confidencialidade**: Determina que os acessos devem ser concedidos somente aos usuários legitimamente autorizados, ou seja, a restrição de acesso deve ser aplicada com o objetivo de limitar o acesso de pessoas não-autorizadas;
- **Integridade:** Estabelece que os dados não serão indevidamente alterados. Em outras palavras, esse princípio garante que os dados não serão editados nem excluídos, seja de forma acidental ou propositalmente;
- **Disponibilidade:** Indica que a informação deve estar sempre disponível e acessível aos usuários autorizados. Isso só é possível se todos os sistemas (software) e equipamentos (hardware) estejam em pleno funcionamento, livre de falhas e sempre disponíveis para os usuários.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

Esses pilares são fundamentais para a definição e elaboração dos processos, políticas e treinamentos que possibilitarão estabelecer um programa sólido de Segurança da Informação. Entretanto, somente isso não basta. É necessário que todos os colaboradores entendam a relevância da Cibersegurança e respeitem as diretrizes estabelecidas pela organização, já que todos os agentes são peças fundamentais para um sistema efetivo de Segurança da Informação.

Portanto, a Governança de T.I. não é somente uma área de suporte aos processos da organização, mas sim uma parte fundamental no contexto do planejamento estratégico das empresas que possibilita fortificar a S.I e criar vantagens competitivas através da otimização dos recursos de Tecnologia da Informação das organizações.

Essas boas práticas devem ser implementadas, disseminadas pela alta administração e fiscalizadas, já que a não observância das diretrizes estabelecidas no sistema de Segurança da Informação podem ocasionar diversos prejuízos, como vulnerabilidade técnica e consequentemente um ataque cibernético ou vazamento de informações pessoais/confidenciais que podem até acarretar danos financeiros, reputacionais e, nos casos mais graves, resultar o fechamento do empreendimento pelo impacto direto ao seu negócio.

4 A REALIDADE DA CIBERSEGURANÇA NAS EMPRESAS

Nesse sentido, recentemente o DataFolha realizou uma pesquisa[4], avaliando as respostas de mais de 350 gestores da área de Tecnologia da Informação (T.I.) de empresas que atuam no seguimento da educação, tecnologia e telecomunicação, saúde e financeiro, varejo e seguros.

O resultado da pesquisa demonstra que apesar de 80,6% das respostas afirmarem que as empresas se preocupam com a Cibersegurança, na prática, somente 31% delas realmente priorizam o setor de T.I. no plano de investimento da empresa. As respostas apontam que apesar das empresas reconhecerem a relevância da S.I., as áreas de T.I. não têm sido priorizadas na hora de receber

[4] INVESTIMENTO em cibersegurança ainda não é prioridade para empresas, aponta Datafolha. Estúdio Folha, [S. l.], p. 1-3, 1 jun. 2021. Disponível em: https://estudio.folha.uol.com.br/mastercard/2021/06/investimento-em-ciberseguranca-ainda-nao-e-prioridade-para-empresas-aponta-datafolha.shtml. Acesso em: 4 maio 2022.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

investimentos. Em vista disso, 57% dessas mesmas empresas afirmaram que já foram alvo de ataques digitais e/ou fraudes com uma frequência média ou alta, conforme demostrado no gráfico abaixo:

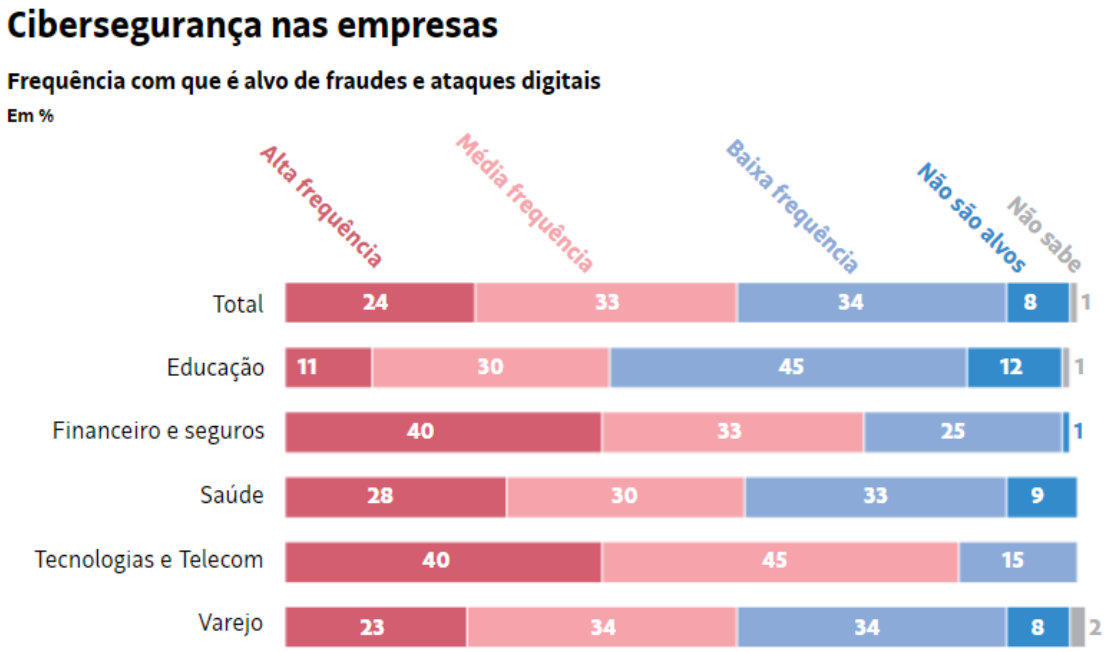

Gráfico 1 - representando a frequência com que as empresa entrevistadas sofreram ataques virtuais – Reprodução Folha[5]

5 ATAQUES CIBERNÉTICOS

É cada vez mais comum ler notícias a respeito de invasões aos sistemas das empresas, sequestro e vazamento de dados e ataques *hackers* em geral. Atualmente, existem diversos tipos de ataques cibernéticos, que podem ser evitados através da estruturação de um programa consistente de Segurança da Informação, porém é importante ressaltar que nenhum sistema é completamente vedado à uma invasão, sendo uma tarefa contínua o monitoramento, remediação e correção de eventuais incidentes. Entre as tentativas mais recorrentes de invasão cibernética, temos como exemplo:

[5] CIBERSEGURANÇA é vista como prioridade em empresas, mas falta investimento. Estúdio Folha, [S. l.], p. 1-3, 30 jul. 2021. Disponível em: https://www1.folha.uol.com.br/seminariosfolha/2021/07/ciberseguranca-e-vista-como-prioridade-em-empresas-mas-falta-investimento.shtml. Acesso em: 4 maio 2022.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

- ***Ransomware*:** Considerado um dos ataques cibernéticos que mais tem crescido nos últimos anos, o *Ransomware* permite que os criminosos "sequestrem" os dados contidos nos servidores ou computadores das empresas. Graças as brechas no sistema segurança da informação, os *hackers* conseguem acessar os dados da empresa e em seguida realizar a criptografia dessas informações, tornando-as inacessíveis. Para devolver as informações através da chave criada, os criminosos geralmente pedem um valor altíssimo para o pagamento do "resgate", geralmente em moedas na *blockchain*.

- ***Phishing*:** Realizado na maioria das vezes através do e-mail, o *Phishing* é um ciberataque que consiste em "pescar" dados sigilosos das vítimas. Geralmente esse e-mail direciona o usuário para uma página falsa, porém, semelhante a original, seja de um banco, página do governo inclusive do judiciário, *marketplace* com promoções etc. e o indivíduo acessa o link malicioso sem saber, deixando seu equipamento desprotegido para o acesso do hacker, que consegue extrair diversos dados das vítimas, como senhas, dados pessoais, credenciais de acesso e demais informações sigilosas.

- **DoS e DDoS:** *Denial Of Service* ou **DoS**, é conhecido no Brasil como ataque de "negação de serviço". Isto porque os *hackers* sobrecarregam o servidor/computador através do envio de inúmeras solicitações para o alvo, através de um computador, ao ponto desses recursos ficarem indisponíveis para seus usuários. Já o *Distributed Denial of Service* ou **DDos,** apesar de ocorrer de forma similar ao mencionado anteriormente, utilizando uma rede de computadores controlados por um computador 'mestre', que comanda e dispara solicitações a esses servidores/computadores, de forma que sobrecarreguem e se tornem inacessíveis.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

Esses ataques cibernéticos têm aumentado de modo geral, entretanto, no Brasil os dados são ainda mais alarmantes. Uma pesquisa[6] realizada pela alemã Roland Berger, aponta que no primeiro trimestre de 2021 foram registrados mais de mais de 9,1 milhões de ocorrências de ataques cibernéticos, um número maior do que o total registrado no ano de 2020.

Com o crescimento exponencial desses ataques, o Brasil saltou para a quinta posição no ranking de países que mais sofreram com crimes cibernéticos, ficando atrás somente dos EUA, Reino Unido, Alemanha e África do Sul.

Em consequência, a referida pesquisa estima que os prejuízos globais ocasionados por esses ataques podem chegar a U$ 6 trilhões no ano de 2021. Além de se tornarem mais frequentes, os ataques cibernéticos também têm se tornado cada vez mais sofisticados, os criminosos constantemente buscam aprimorar suas técnicas com o objetivo de buscar novas vulnerabilidades e mais efetividade nos seus ataques.

6 GOVERNANÇA CORPORATIVA, TECNOLOGIA, SEGURANÇA, E ADMINISTRAÇÃO DE DADOS[7]

Dentro de todo o tema de segurança da informação, temos como norte todo o conjunto de controles e organização orientado pelos preceitos de governança corporativa, que direcionam, dirigem e monitoram os interesses alinhados dos *stakeholders*, com a finalidade de preservar e otimizar o valor da organização.

Como princípios da governança corporativa, temos: a transparência em relação às partes interessadas independente da obrigação legal; a equidade quanto ao tratamento não discriminatório de todos os sócios; a prestação de contas e responsabilização pelos seus atos; e a responsabilidade corporativa ligado à garantia de sustentabilidade da organização, considerando a ordem social e ambiental na definição dos negócios e das operações.

[6] BRASIL foi 5º país com mais ataques cibernéticos no ano: relembre os principais. Isto É Dinheiro, [S. l.], p. 1-3, 20 dez. 2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/. Acesso em: 4 maio 2022.

[7] Instituto Brasileiro de Governança Corporativa - Papéis e responsabilidades do conselheiro na gestão de riscos cibernéticos / Instituto Brasileiro de Governança Corporativa. - São Paulo, SP: IBGC Orienta, 2019, Acesso em 17 de maio de 2022. Disponível em: <papeis-e-responsabilidades-do-conselho-na-gestao-de-riscos-ciberneticos.pdf (bibliotecadeseguranca.com.br)>

Como um guarda-chuva, a governança corporativa abraça aquelas relacionadas às informações que a empresa trata, sendo de cunho estratégico ou pessoal. Temos, portanto, a figura da governança da tecnologia da informação, que é o conjunto de controles que tem como objetivo fornecer uma estrutura para os dirigentes utilizarem na avaliação, administração e fiscalização do uso da tecnologia da informação na sua organização, assim como disponibilizar um conjunto de informações para uma correta avaliação e tomada de decisão.

Temos, ainda, a figura da governança de administração de dados, que define padrões para estruturar a forma como os dados são coletados, armazenados, processados e descartados, ajudando a definir o controle de acesso, segregação de funções, gestores e operadores de informação, e implantação de controles que assegurem que os dados possam estar seguros, disponíveis e íntegros.

Por fim, temos a figura da governança da segurança da informação e cibersegurança, que se debruça em alinhar os objetivos e estratégia da segurança da informação com os objetivos e estratégia do negócio, agregando valor para as partes interessadas, assegurando que os riscos inerentes ao tratamento das informações estão devidamente mapeados e mitigados.

A existência de políticas de segurança da informação e da cibersegurança, aprovadas pela alta administração é um exemplo de conformidade da das frentes de segurança da informação com a governança corporativa, atendendo aos princípios de transparência, equidade e responsabilidade corporativa. É indissociável a gestão da segurança da informação com os controles da governança corporativa.

7 CULTURA DE PROTEÇÃO DE DADOS PESSOAIS PELO *TONE AT THE TOP*.

Visto isso, para que a mudança de cultura seja concretizada, alguns fatores precisam ser observados, dentre eles, a própria LGPD nos orienta sobre questões referente às boas práticas e governança, conforme se verifica no artigo 50 da Lei, vejamos:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

> segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Cabe aqui mencionar que existem diversas definições de governança corporativa, entretanto de forma geral possuem a mesma essência teórica. Neste sentido, no Código de Melhores Práticas, divulgado pelo Instituto Brasileiro de Governança Corporativa - IBGC, governança corporativa é definida da seguinte forma:

> Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.[8]

Desta forma, cabe aos agentes de tratamento definirem um conjunto de boas práticas, as quais são estabelecidas em políticas, que devem ser lideradas e suportadas pelos responsáveis pela gestão da organização, demonstrando um comprometimento com o Sistema de Privacidade e Proteção de Dados implementado, para que assim haja o engajamento dos demais envolvidos na operação, visando um nível de proteção de dados pessoais adequado e esperado pelos titulares.

A expressão *tone at the top*, pode ser definida como: “o exemplo de liderança ética que vem de cima”, em outras palavras significa o engajamento da alta administração da organização, primordial na estruturação de um sistema de privacidade e proteção de dados pessoais, pois, além de ser o necessário exemplo dos mais altos níveis de hierarquia, também tem a função de perdurar a cultura de proteção de dados na organização.

Assim, para que um Sistema de Privacidade e Proteção de Dados possua engajamento, e consequentemente sucesso em suas atividades, se faz necessário que a alta administração não só se manifeste em apoio à implementação do Sistema, mas sim que adote medidas concretas para fornecer os meios e recursos necessários para que seja implementado de maneira efetiva.

[8] IBGC (2018). *Código das melhores práticas de governança corporativa,* pg. 20. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=23895. Acesso em: maio de 2022.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

Para isso, é fundamental que os agentes de governança estabeleçam estratégias de comunicação, treinamentos e dispositivos normativos que versem sobre proteção de dados visando difundir o posicionamento da alta administração em relação ao tema.

Neste sentido é o que os especialistas José Saldanha, sócio-líder de Alianças Microsoft e Soluções em Nuvem da KPMG no Brasil e Leandro Augusto Marco Antonio, sócio-líder de *Cyber Security* da KPMG no Brasil expressam:

> Muito além do desafio das organizações atenderem aos requerimentos da LGPD, está a oportunidade de utilizarem este novo referencial legal para fortalecer a conduta corporativa. Se bem liderada, e preferencialmente executada de forma estratégica e integrada, essa questão garantirá um salto de qualidade na incorporação de boas práticas de comunicação, transparência, segurança jurídica e eficiência operacional.[9]

Sendo assim, a partir dessa conduta corporativa juntamente com a aplicação de normativas e procedimentos de proteção de dados, a confiança dos titulares no mercado é reestabelecida, bem como é criado um ambiente seguro para os agentes de tratamento de dados, resultando no sucesso do Sistema de Privacidade e Proteção de Dados.

Visto que para o engajamento da cultura de privacidade e proteção de dados ser concretizado dentro de uma organização há a necessidade do *tone at the top* liderar de forma eficiente o tema, é fundamental a abordagem sobre a alocação da estrutura responsável pela governança de dados.

Cumpre destacar que a LGPD expressa que o agente de tratamento deverá observar no mínimo que o Sistema de Privacidade e Proteção de Dados esteja integrado a sua estrutura geral de governança, além de demonstrar o comprometimento com as normativas internas e boas práticas com relação à proteção de dados pessoais, vejamos:

> Art. 50. §2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - Implementar programa de governança em privacidade que, no mínimo:

[9] KPMG (2020). *LGPD exige atuação estratégica e integrada*, pg. 2. Disponível em: https://assets.kpmg/content/dam/kpmg/br/pdf/2020/10/lgpd-atuacao-estrategica.pdf. Acesso em: maio de 2022.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos.

Conforme mencionado no artigo 41 da LGPD, o controlador deverá indicar um Encarregado pelo tratamento de dados pessoais, ou também conhecido como *Data Protection Officer* (*DPO*), o qual será responsável por garantir a conformidade à LGPD, e avaliar os riscos relacionados à proteção e privacidade de dados de uma organização.

Seguindo as melhores práticas com relação às decisões envolvendo tratamento de dados pessoais, é indicado que a função de DPO seja exercida por alguém com autonomia e ausência de conflito de interesses**.**

Além disso, para que o DPO consiga desempenhar suas atividades da melhor forma, é possível que seja implementada uma estrutura organizacional de proteção de dados, que deverá monitorar os riscos, as legislações e questionamentos pertinentes ao tema, bem como os processos de tratamento de dados da organização. Neste sentido é o que dispõe o Guia Orientativo da ANPD, vejamos:

> 73. Também é importante observar que a LGPD não proíbe que o encarregado seja apoiado por uma equipe de proteção de dados. Ao contrário, considerando as boas práticas, é importante que o encarregado tenha recursos adequados para realizar suas atividades, o que pode incluir recursos humanos. Outros recursos que devem ser considerados são tempo (prazos apropriados), finanças e infraestrutura.[10]

Desta forma, para a efetividade do Sistema, é fundamental que a estrutura organizacional reporte diretamente à Alta Administração no organograma da empresa e que seja independente, sem a necessidade de submissão a quaisquer outras áreas, e que esses profissionais tenham os recursos necessários para a implementação de suas políticas, como também, que as suas decisões sejam respeitadas e cumpridas.

Sendo assim, conforme expressado anteriormente, a tarefa de adequação à LGPD é responsabilidade que deve ser assumida pela organização como um todo, ou seja, por todas as pessoas que fazem parte dela, contribuindo a estrutura

[10] ANPD (2022). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. pg. 22. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf Acesso em: maio de 2022.

organizacional de proteção de dados de forma especial nesse processo de adequação e monitoramento constante à LGPD.

8 CONSIDERAÇÕES FINAIS

Podemos concluir que a Segurança da Informação, estruturada através de um processo de Governança de T.I., é uma ferramenta fundamental para a efetividade do sistema de Governança Corporativa. Entretanto, a diretrizes da S.I. precisam estar alinhadas os objetivos da empresa. Além do incentivo da alta administração, investimento e atualizações constantes, é necessário realizar o monitoramento contínuo do sistema de Segurança da Informação, levando em consideração o cenário em que a empresa está atuando, os riscos e vulnerabilidades que a organização está exposta assim como a maturidade em relação à infraestrutura e T.I. para lidar com as iminentes ameaças. Somente assim é possível realizar o gerenciamento de riscos e aprimoramentos necessários para garantir a efetividade da governança da segurança da informação.

Perante a evolução constante da tecnologia e considerando que a maioria das empresas utilizam sistemas de armazenamento externo (nuvem), é fundamental que essas organizações estejam adequadamente protegidas, minimizando potenciais riscos dentro da sua estrutura tecnológica, especialmente quando envolvem terceiros no processo.

A S.I. já tem sido vista como uma necessidade para as empresas que realizam o tratamento de um grande volume de dados. Entretanto, devido as crescentes de ameaças tecnológicas, as pequenas empresas também já estão buscando implementar processos, políticas e sistemas que garantam o mínimo em segurança da informação.

Podemos perceber que assim como a proteção de dados pessoais, a segurança da informação como um todo é muito mais do que um processo de adequação, se trata na verdade de um processo robusto e complexo de aculturamento.

Muito além de seguir as regras, os indivíduos envolvidos na operação da empresa precisam entender, respeitar e auxiliar a fiscalizar as diretrizes de S.I. instituídas pela empresa. Dessa forma é possível criar um conjunto de mecanismos

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

eficientes para manter em segurança e conformidade as áreas de T.I. e consequente a manutenção de uma governança corporativa sólida e eficiente.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005 Tecnologia da informação: técnicas de segurança. Rio de Janeiro, 2006.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. IBGC. Código das Melhores Práticas de Governança Corporativa. 5. ed. São Paulo: IBGC, 2015. P20

ITGI. COBIT 4.1: Objetivos de Controle para Informações e Tecnologias Correspondentes. Rolling Meadows, IL (EUA): IT Governance Institute, 2007. 212p.

INVESTIMENTO em cibersegurança ainda não é prioridade para empresas, aponta Datafolha. Estúdio Folha, [S. l.], p. 1-3, 1 jun. 2021. Disponível em: https://estudio.folha.uol.com.br/mastercard/2021/06/investimento-em-cibersegurança-ainda-nao-e-prioridade-para-empresas-aponta-datafolha.shtml. Acesso em: 4 maio 2022.

CIBERSEGURANÇA é vista como prioridade em empresas, mas falta investimento. Estúdio Folha, [S. l.], p. 1-3, 30 jul. 2021. Disponível em: https://www1.folha.uol.com.br/seminariosfolha/2021/07/ciberseguranca-e-vista-como-prioridade-em-empresas-mas-falta-investimento.shtml. Acesso em: 4 maio 2022.

BRASIL foi 5º país com mais ataques cibernéticos no ano: relembre os principais. Isto É Dinheiro, [S. l.], p. 1-3, 20 dez. 2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/. Acesso em: 4 maio 2022.

Instituto Brasileiro de Governança Corporativa - Papéis e responsabilidades do conselheiro na gestão de riscos cibernéticos / Instituto Brasileiro de Governança Corporativa. - São Paulo, SP: IBGC Orienta, 2019, Acesso em 17 de maio de 2022. Disponível em: <papeis-e-responsabilidades-do-conselho-na-gestao-de-riscos-ciberneticos.pdf (bibliotecadeseguranca.com.br)>

IBGC (2018). *Código das melhores práticas de governança corporativa.* Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=23895.

KPMG (2020). *LGPD exige atuação estratégica e integrada*. Disponível em: https://assets.kpmg/content/dam/kpmg/br/pdf/2020/10/lgpd-atuacao-estrategica.pdf.

ANPD (2022). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

Submetido em: 25/04/2024
Aprovado em: 30/04/2024
Avaliação: Double Blind Reviewe
ISSN: **2316-7548**

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

PIRONTI, Rodrigo. Lei Geral de Proteção de Dado no Setor Público. 1. ed. Belo Horizonte: 2021.

MALDONADO, Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Pessoais. São Paulo: 2019.