FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS

CURSO: ADMINISTRAÇÃO

LINHA DE PESQUISA:

ÁREA: GESTÃO DE PESSOAS

WILLIAM PENNA MARINHO DE ABREU SILVA

21652793

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: FATORES INTERVENIENTES NA APLICAÇÃO PELAS ÁREAS DE RECURSOS HUMANOS

Brasília

2020

WILLIAM PENNA MARINHO DE ABREU SILVA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: FATORES INTERVENIENTES NA APLICAÇÃO PELAS ÁREAS DE RECURSOS HUMANOS.

Trabalho de Curso (TC) apresentado como um dos requisitos para a conclusão do curso de Administração de Empresas do Centro Universitário de Brasília – UniCEUB.

Orientador: Prof. MSc. Igor Guevara Loyola de Souza

Brasília
2020

WILLIAM PENNA MARINHO DE ABREU SILVA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: FATORES INTERVENIENTES NA APLICAÇÃO PELAS ÁREAS DE RECURSOS HUMANOS.

Trabalho de Curso (TC) apresentado como um dos requisitos para a conclusão do curso de Administração de Empresas do Centro Universitário de Brasília – UniCEUB.

Brasília, _____ de _____ de 20____.

Banca Examinadora

_____

Prof. (a):Igor Guevara Loyola de Souza

_____

Prof. (a):
Examinador(a)

_____

Prof. (a):
Examinador(a)

Brasília
2020

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: FATORES INTERVENIENTES NA APLICAÇÃO PELAS ÁREAS DE RECURSOS HUMANOS.

William Penna Marinho de Abreu Silva[1]

Igor Guevara Loyola de Souza[2]

RESUMO: O presente estudo tem por objetivo identificar fatores intervenientes na aplicação da Lei Geral de Proteção de Dados Pessoais (13.709/18), pelas áreas de Recursos Humanos. Com foco numa análise qualitativa a pesquisa mostrou a complexidade do processo de implementação da referida lei pelas empresas. A coleta de dados se deu por meio de questionários com três empresas, Uma consultoria que presta serviços para o atendimento aos requisitos da nova lei, dentre outras ações, um escritório de advocacia especializado em Direito Digital e uma empresa especializada em Segurança da Informação. Os resultados mostraram a complexidade desse processo, a necessidade de interação entre as diversas áreas da empresa, bem como o envolvimento de todos que nela trabalham. Mostrou também como os custos são altos e a necessidade de um planejamento alinhando as ações de todos os setores.

Palavras-chave: LGPD. Segurança da Informação. Gestão de RH

1 INTRODUÇÃO

Em 2014, foi instituído o Marco Civil da Internet. Essa lei, que regula o uso da Internet no país, estabelece princípios de proteção da privacidade dos usuários bem como dos seus dados pessoais, garantindo também inviolabilidade e sigilo das comunicações privadas armazenadas (TJDFT, 2014). Com o desenvolvimento acelerado da tecnologia da informação outras necessidades surgiram e, em 2018, é sancionada pelo Presidente da República a Lei Geral de Proteção de Dados Pessoais

[1] Estudante do 8º semestre do curso de Administração de Empresas da FATECS/ UniCEUB. w.penna8@gmail.com

[2] Docente FATECS/ UniCEUB. Mestre em Administração (UnB), na área de Estudos Organizacionais e Gestão de Pessoas. Bacharel em Administração (UnB). igor.souza@ceub.edu.br.

(LGPDP). Ela se refere ao tratamento de dados pessoais nos meios físicos e digitais objetivando o direito fundamental da liberdade e privacidade de tais dados. (BRASIL, 2018)

Tal lei, primeiramente com semelhante em vigor na Europa, fez com que muitos processos internos fossem revistos em instituições públicas e privadas, principalmente nos setores de Recursos Humanos das empresas onde se concentram os dados pessoais e funcionais dos trabalhadores.

Com isso, questiona-se o que as áreas de Recursos Humanos (RH) das empresas estão fazendo para se adaptar aos requisitos da nova lei, para proteção de dados de seus funcionários e colaboradores. Neste caso, também é importante compreender, quais são os fatores que facilitam e dificultam a aplicação da lei nas organizações.

Tem-se, portanto, como objetivo geral deste estudo identificar fatores intervenientes na aplicação da Lei Geral de Proteção de Dados Pessoais (13.709/18), pelas áreas de Recursos Humanos

Considerando o acelerado desenvolvimento e uso de meios eletrônicos por onde trafegam e são armazenadas milhões de informações, bem como as vulnerabilidades a que estão sujeitos ambientes, processos, tecnologias e pessoas é necessário verificar, no âmbito da administração de empresas, como se dão os controles e a proteção dos dados das pessoas que nelas trabalham diante da legislação em vigor.

Entende-se que este estudo é pertinente às áreas de RH, pois estas armazenam informações sensíveis de funcionários tais como salários e benefícios, endereços, dados bancários dentre outras. O presente estudo pode contribuir para a revisão de aspectos gerenciais como os procedimentos de proteção das informações sob a custódia das áreas de RH, assim como propiciar na área acadêmica, outros estudos e discussões em sala de aula, enriquecendo a formação dos estudantes e propiciando a busca de soluções para novas questões que podem advir desses estudos e discussões. Várias são as rotinas relacionadas a gestão de Recursos

Humanos contidas em processos internos. A capacitação das equipes bem como o cuidado com os ativos sob sua responsabilidade, são fatores críticos para o sucesso da proteção dos dados dos empregados em atendimento aos requisitos da nova lei.

A necessidade de conhecer e entender esses processos e as responsabilidades a eles pertinentes, leva para o universo acadêmico a Lei Geral de Proteção de Dados para que, no caso do curso de Administração de Empresas, os futuros profissionais sejam atualizados naquilo que vai permear seu dia a dia no trabalho.

2 EVOLUÇÃO DA ÁREA DE RECURSOS HUMANOS

Segundo Marras (2016), a área de Recursos Humanos (RH) das empresas evoluiu ao longo dos anos. Na Fase Contábil, antes de 1930, os trabalhadores eram vistos sob um ponto de vista contábil. Eles eram considerados exclusivamente como mão de obra e geravam custos que precisavam ser absorvidos pelas empresas ainda sob o impacto da revolução industrial nos modelos do século 19. Com as guerras na Europa, parte desses trabalhadores era de mulheres que precisavam do dinheiro uma vez que seus pais, irmãos, filhos ou companheiros estavam nos campos de batalha.

Com o incremento da indústria e do comércio, inicia-se a fase denominada Legal, 1930 - 1950. No Brasil, Getúlio Vargas prepara a Consolidação das Leis do Trabalho (CLT) unificando toda a legislação da área e em 1 de maio de 1943 ele assina o Decreto-Lei nº 5.452, ainda no período do Estado Novo. Nessa época, ainda segundo Marras (2016), surge o Chefe de Pessoal cuja função é aplicar as leis trabalhistas conforme decretado pelo então presidente da República. O autor destaca que as atividades do Chefe de Produção agora são compartilhadas com o de Pessoal.

O período entre 1950 e 1965 é chamado de Fase Tecnicista quando o Brasil implanta um modelo de gestão de pessoas adaptado dos Estados Unidos da América. Gomes (2016) destaca que entre essas décadas “embora ainda em nível operacional-tático, aparece o papel de gerente de pessoal”. Aqui, a função de RH é

desvinculada do gestor de recursos industriais, que era quem cuidava das questões administrativas. É nessa época que começam a ser implantados os serviços de recrutamento e seleção, treinamento, cargos e salários, higiene e segurança do trabalho, dentre outras questões relacionadas com benefícios ao trabalhador.

Com a evolução das necessidades e o amadurecimento dos processos, entre 1965 e 1985 tem-se a fase Administrativa. Segundo Gomes (2016) “esta fase tem como principal característica as "revoluções" movidas pelos trabalhadores impulsionados pelo movimento sindical”. Com o chamado novo sindicalismo, o gestor da antiga área de pessoal passa a ser denominado Gerente de Recursos Humanos. A ênfase agora é nas questões humanísticas, embora não perca o foco nos procedimentos burocráticos e operacionais, numa visão mais multidisciplinar com trabalhadores que estão aprendendo a negociar.

Mas, a partir de 1985, com os primeiros programas de planejamento estratégico, a gestão de RH passou a um nível também estratégico com um diretor que integrava as esferas de decisão mais altas das empresas. Segundo, Ferreira e Loos (2019) “A área de Recursos Humanos tem sido desafiada a atuar estrategicamente nas organizações, influenciando assim o desempenho organizacional e, para isso, vêm sendo necessária a redefinição do seu papel nos últimos anos”

Tal evolução exigia cada vez mais processos, registros e arquivamento de documentação. Informações como salários, por exemplo, eram sensíveis e a custódia dessa documentação passou a ser rigorosa, muito mais pelas exigências da legislação trabalhista e auditorias e fiscalizações do Ministério do Trabalho, que propriamente por respeito ao trabalhador. Segundo Chiavenato (2010 apud Gomes, 2016) “a moderna Gestão de Pessoas consiste em várias atividades integradas entre si no sentido de obter efeitos sinergéticos e multiplicadores tanto para a organização, como para os colaboradores”. Já em 2010 essa preocupação se fazia presente em estudos portugueses, com relação ao Código do Trabalho do país, como destaca Mori (2010) quanto às previsões relativas a: “proteção de dados pessoais, os meios de

vigilância à distância, as possíveis exigências de testes e exames médicos, a confidencialidade de mensagens e de acesso à informação.”

Com o advento das novas tecnologias de comunicação e armazenamento de informações, vários dos processos internos foram sendo aprimorados e a legislação foi se tornando mais rigorosa até os dias de hoje com a implementação da Lei Geral de Proteção de Dados Pessoais pelas instituições. Ainda citando Chiavenato(2010), Gomes (2016) afirma que um dos processos básicos é o de monitorar pessoas. Tal o processo é usado para “acompanhar e controlar as atividades de cada funcionário, e verificar resultados, tais como banco de dados e sistemas de informações gerenciais”.

Para melhor compreensão, é necessário trazer alguns dos conceitos de segurança da informação.

2.2 Principais conceitos relativos a segurança da informação

A segurança da informação "visa a proteção de ativos que contém informações" (Ramos *et all*, p.19, 2008), considerando-se ativos "aqueles que produzem, processam, transmitem ou armazenam informações" segundo os mesmos autores.

Primeiramente alguns conceitos precisam estar claros. São eles, conforme Ramos et al(2008):

Quadro 1 - Termos básicos de Segurança da Informação

Termo	Conceito
Confidencialidade	Consiste em garantir que só tenham acesso às pessoas que necessitam tomar conhecimento e que poderão acessar a informação ou ativo que a contém.
Integridade	Pressupõe preservar a informação em seu estado original
Disponibilidade	A informação deve estar disponível para os que dela necessitam e no momento que precisam.
Valor	Importância do ativo para a organização
Ameaça	Evento que tem potencial em si par comprometer o objetivo

Vulnerabilidade	Ausência de um mecanismo de proteção ou falha no existente
Impacto	Tamanho do prejuízo conforme parâmetros pré-estabelecidos
Risco	Probabilidade da ameaça explorar a vulnerabilidade

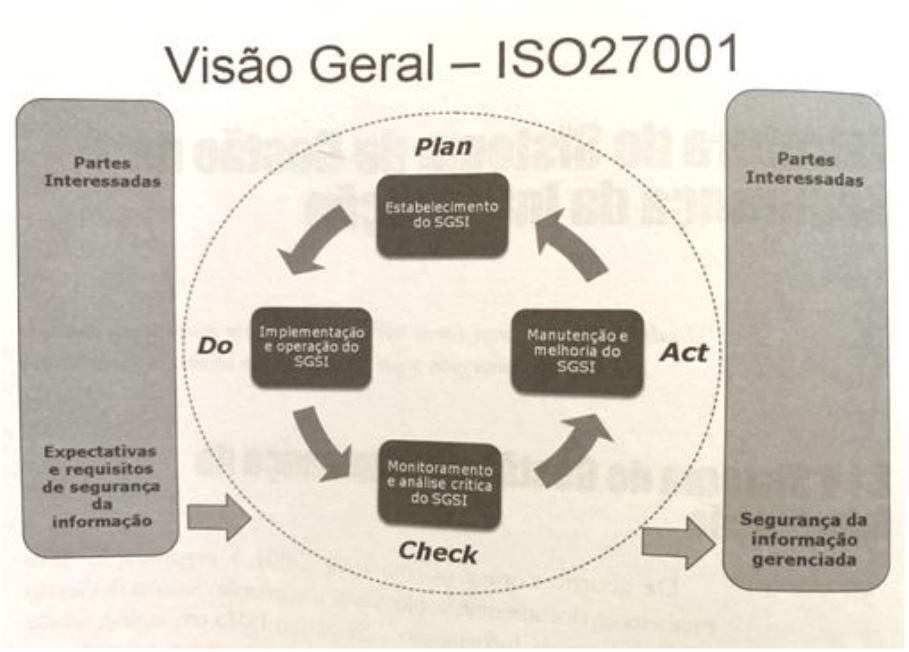
Fonte: Ramos et al, 2008.

Os componentes básicos para isso são o valor atribuído à informação ou ativo, a ameaça a ser considerada e suas vulnerabilidades, bem como o impacto e o risco a que estão sujeitos.

Nesse contexto se considera a interação entre os componentes. A cada ativo é atribuído um valor conforme os proprietários das informações. Sendo o RH custodiante dessas informações dos funcionários precisa definir padrões de proteção que minimizem os riscos. Para isso é necessário identificar as ameaças e seus agentes e conhecer as vulnerabilidades. Uma informação pode ser alvo de interesse de pessoas ou grupos mal intencionados e seu proprietário pode ser alvo de chantagens ou qualquer tipo de pressão. Considerando que risco é a probabilidade da ameaça explorar vulnerabilidade, cabe a empresa e ao RH em particular, proteger os ativos considerando suas forças e fraquezas relativa à proteção desses dados sob sua custódia. Tais conceitos têm por base a família ISO 27000 que estabelece os elementos para a gestão dos processos relativos a proteção das informações. Segundo Ramos et al (2008, p.27) “as origens dos problemas de segurança podem ser, basicamente, divididas em três categorias: natural, acidental ou intencional, sendo as duas últimas relacionadas ao fator humano”.

A ISO/IEC 27000, por exemplo, apresenta uma visão geral de segurança da informação incluindo um glossário com os significados dos termos utilizados. Já a ISO/IEC 27001 é a norma que define os requisitos para o sistema de gestão da segurança da informação (SGSI). Tal sistema consiste em:

Figura 1: Visão geral do processo de gestão



Fonte:BASTOS; CAUBIT (2009, p.32)

Cabe ao SGSI definir as políticas, os processos e procedimentos para a gestão da segurança das informações, incluindo aí as normas e procedimentos relativos aos funcionários, colaboradores e parceiros da organização. A área de RH passa a ser o custodiante, dessas informações.

A LGPD destaca que o tratamento de dados somente poderá ocorrer em duas hipóteses. A primeira delas é quando houver o consentimento de titular ou de seu responsável legal.A segunda é por cumprimento de obrigações legais ou regulatórias (BRASIL, 2018)

No RH, estão disponíveis informações de: a) processos de recrutamento e seleção; b) integração entre os contratados; c) avaliações de desempenho; d) treinamento e desenvolvimento; e) rotinas do setor; e f) elaboração de estratégias e integração com os demais setores da organização, seja ela pública ou privada.

Erthal e Diehl (2015) citando Chiavenato (2007) destaca que “ na era da informação, as pessoas são vistas como seres inteligentes, dotadas de conhecimentos e habilidades, sendo o ativo mais importante das organizações”.

Assim, sendo o capital humano o mais importante, os dados desde o recrutamento e seleção até o desligamento de um funcionário, passando pelos registros pessoais, filhos, saúde, salários, férias, atribuições, dentre outros, precisam ser protegidos e o funcionário tranquilizado quanto a segurança de suas informações. Qualquer vazamento desses dados sob a custódia do RH pode gerar desconfiança que desequilibra o ambiente interno. Tal situação poderá impactar nos negócios da empresa e na vida pessoal do funcionário.

A Lei Geral de Proteção de Dados está relacionada com qualquer atividade que utilize dados pessoais incluindo a internet, dados de consumidores e empregados dentre outros conforme especificado em seu Art. 1º “Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (BRASIL, 2018). Como já visto, para o uso desses dados é necessário que se obtenha o consentimento de seu proprietário para legitimar o seu uso.

A referida lei cria a figura do Controlador. Enquanto na ISO 27000 o responsável era o Gestor ou Comitê Gestor de Segurança da Informação (GSI), conhecido internacionalmente como *Security Officer* ou *Information Security Officer*, o controlador é indicado por um gestor, não necessariamente de SI. No caso da ISO, o Comitê de Segurança da Informação é de natureza deliberativa, “possuindo poder de decisão sobre os assuntos relativos a Segurança da Informação ou riscos de TIC, e do tipo estratégico, devendo assegurar que a área de TIC do tribunal opere no mais alto nível de segurança para proteção da informação para todas as áreas do egrégio” (SETIC). No Capítulo VI, Seção I, a lei destaca as responsabilidades do controlador e do operador. Ambos devem manter os registros de todas as operações que envolvam os dados pessoais.

O controlador, quando solicitado, deve elaborar um relatório de impacto à proteção dos dados pessoais, sensíveis ou não. Já o operador, será instruído pelo controlador a respeito de como tratar esses dados seguindo não só a lei, mas

também a regulamentação interna da organização. O art 40, ressalta que “A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança”. Considerando a necessidade e a transparência a tal autoridade também poderá definir o tempo de guarda dos registros (BRASIL, 2018)

No caso das informações relativas a pessoal, cabe ao RH, de acordo com a Política de Segurança da Informação da organização, manter ajustados os procedimentos da área e um estreito relacionamento com o operador e o controlador, em conformidade com a legislação em vigor. Em algumas empresas, pode ser definido um responsável específico para esse contato em cada um dos setores.

Essa legislação prevê que todas as empresas nacionais ou não, estão sujeitas a esse regramento, a qual se aplica a qualquer incidente de segurança envolvendo os dados pessoais. Recomenda ainda a realização de avaliação de impacto à proteção desses dados, o registro periódico em relatório e a punição para infrações que vão desde advertências a multa.

Assim como a sociedade muda, as leis também acompanham essa evolução. No caso específico do presente estudo, o foco é a adaptação das empresas para atender às exigências da Lei Geral de Proteção de Dados, sancionada em 2018 pelo presidente da República, e que entra em vigor a partir de agosto de 2020. Tal movimento implica numa mudança no gerenciamento das empresas, mais especificamente em seus processos internos relativos às informações e dados de seu quadro de pessoal.

Para isso, é necessário um processo com métodos e técnicas específicas para ajudar a organização e os funcionários na mudança do estado atual para um estado futuro. Isso pressupõe um descongelamento das práticas utilizadas, a definição dos novos padrões em conformidade com a lei e depois a implantação dos novos processos até que uma outra mudança se faça necessária (Rosa, 2001).

2.3 Mudança Organizacional

Todo processo de mudança pode gerar crises principalmente internas. Nesse caso, ainda segundo Rosa (2001, p.132-133), a organização deve estar preparada para: a)Crises de informação que consistem em falsos rumores, boatos e intrigas; acusações sobre direito de propriedade; acusações de concorrentes ou de instâncias públicas contra a organização; b) Falhas em equipamentos ou construções poir podem ocorrer colapsos na rede de computadores e na de provedores, telefones; falhas provocadas por funcionários; quebra no sistema de segurança dentre outros; c) Crises de natureza legal como ações judiciais contra a organização; pedidos de indenização ou de condenação por parte de funcionários, consumidores, governo; d) Crise de reputação com denúncias de corrupção, informação privilegiada, escândalos de todos os tipos. vazamento de documentos internos; e) Crise regulatórias como regulamentação adversa de leis, na esfera do Congresso ou do governo" dentre outros.

Considerando o exposto é necessário levar em conta a cultura organizacional, o que se necessita mudar e definir o como fazer avaliando os impactos dessa mudança nas rotinas da empresa ou de um setor específico. O ponto de partida é seu objetivo de tal maneira que este esteja alinhado aos objetivos estratégicos da organização. A partir daí define-se um plano de comunicação interno ou externo, se for o caso, um plano para orientar e treinar as equipes gestoras dessa mudança bem como orientar e esclarecer as dúvidas de outros envolvidos. Para evitar a crise provocada por falhas em equipamentos ou relacionada a pessoas é importante implementar uma estrutura de apoio e depois avaliar o processo de mudança como um todo.

3 MÉTODO

Quadro 2 - Procedimentos metodológicos de pesquisa

Etapa	Objetivos de Pesquisa	Abordagem	Instrumentos	Amostragem	Amostra	Análise
1	Identificar como as áreas de	Qualitativa	Questionário	Por acessibilidade	profissionais que trabalha	Análise de conteú

	Recursos Humanos das empresas estão procedendo para o atendimento ao proposto na LGPD				m com a implementação da lei nas empresas.	do

Fonte: Elaboração própria

Quanto aos objetivos o referido estudo se classifica como descritiva uma vez que, “esse tipo de estudo pretende descrever os fatos e fenômenos de determinada realidade” (Triviños, 1987 apud Silveira e Córdova, 2009). Quanto a abordagem é Qualitativa pois se propõe a estudar as particularidades e experiências dentre outras questões.

Tal abordagem caracteriza a amostragem por saturação teórica pois, “considera-se saturada a coleta de dados quando nenhum novo elemento é encontrado e o acréscimo de novas informações deixa de ser necessário, pois não altera a compreensão do fenômeno estudado”. (Nascimento et al, 2018)

Para a obtenção de dados e informações foram selecionadas três empresas cujos nomes foram substituídos por letras. O histórico e escopo de atuação são os especificados a seguir conforme as informações por elas fornecidas:

A Empresa A: Sediada em São Paulo, é uma empresa de consultoria especializada em segurança da informação e cibersegurança. Seus sócios têm 30 anos de experiência na área de tecnologia da informação, dos quais mais de 20 anos foram destinados à segurança da informação. A experiência com LGPD envolve a avaliação da condição de maturidade de empresas de diversos segmentos. Com base nesta avaliação, a empresa um Plano de Ação, que contempla a descrição de ampla quantidade de atividades que são necessárias para que seu cliente alcance a conformidade e tenha maturidade para mantê-la. Sendo assim, as respostas serão apresentadas, levando-se em consideração a experiência prática de sua equipe de

especialistas com projetos em empresas de diversos segmentos: Indústria, Comércio Eletrônico, logística, Financeiro, agro-indústria, energia, etc.

Empresa B: Fundado em 1997 na cidade de São Paulo, é um escritório de advocacia com foco em Direito Digital prestando serviços especializados em todas as áreas que envolvam questões tecnológicas, fraudes cibernéticas, compliance digital, proteção e gerenciamento de dados, contratos de tecnologia, propriedade intelectual e telecomunicações, garantindo a melhor qualidade técnica, alinhada com a legislação e jurisprudência vigentes no País e no mundo. Além de atuarem no contencioso, consultivo e administrativo, auxiliam os clientes no desenvolvimento de novos negócios, com treinamentos especializados, implementação de projetos de proteção de dados e políticas corporativas de segurança virtual, abarcando toda a gama de serviços demandada pelo universo digital..Em razão da atuação nacional e internacional, tem representantes em diversas cidades do Brasil, além de parceiros internacionais, proporcionando aos clientes um atendimento global e customizado, de acordo com as necessidades do negócio.

Empresa C: Com Matriz no Rio de Janeiro e filiais em Brasília e São Paulo é uma empresa brasileira com mais de 30 anos de mercado, especializada em Automatização de Governança, Gestão de Riscos e Conformidade. Desde 1985 atua nas áreas de software, consultoria e educação oferecendo soluções inovadoras e customizadas para cada negócio. Tais soluções compreendem Segurança Cibernética, Comando e Controle, e Conformidade e Fiscalização. Tem ainda soluções para integração automatizada de informações e comunicação, visualização em mapas e data analytics, gestão de eventos e incidentes, ambiente em nuvem e segurança cibernética.É certificada como Empresa Estratégica de Defesa pelo Ministério da Defesa, Gold Partner da Microsoft, membros do CIS – Center for Internet Security, além de Qualified Security Assessor pelo PCI SSC. Participou de projetos internacionalmente reconhecidos como as eleições eletrônicas brasileiras, a entrega de imposto de renda via Internet, XV Jogos Pan Americanos Rio 2007, a Copa do Mundo 2014 e as Olimpíadas 2016, além de projetos de grande porte em empresas dos setores financeiro, telecomunicações, utilities e governo.

As perguntas foram encaminhadas por escrito e cada empresa indicou o profissional de contato com o pesquisador. Nas empresas aqui identificadas como A e C os respondentes eram sócios fundadores, e na empresa B foi indicada, pelo sócio fundador, uma advogada do escritório encarregada pelo tratamento de dados pessoais. Em função do isolamento social determinado como estratégia de prevenção a disseminação do Covid-19, os funcionários estavam trabalhando em sistema de rodízio sendo respondidas as questões apresentadas por profissionais que integram as equipes de implementação dos requisitos da nova lei na empresa.

As questões foram estruturadas e organizadas considerando quatro dimensões quanto ao atendimento aos requisitos da LGPD: as fase de preparação, implementação, impacto da referida lei na organização e os primeiros resultados obtidos.

A empresa A respondeu com foco no trabalho de consultoria junto aos seus clientes e as empresas B e C com relação a implantação e atendimento aos requisitos da lei em seus próprios setores e processos.

A análise das informações obtidas considerou as respostas com as experiências das empresas B e C comparando-as com a visão geral apresentada pela A a partir do trabalho de consultoria realizado junto aos seus clientes numa apreciação qualitativa. As informações foram agrupadas conforme as dimensões propostas.

4 APRESENTAÇÃO E DISCUSSÃO DOS DADOS

Apesar do impacto de uma pandemia mundial, foi possível coletar dados relevantes, que contribuíram para esta pesquisa. A análise está organizada considerando as quatro dimensões propostas.

Preparação

A empresa A que presta consultoria nessa área de Segurança da Informação, Governança, Riscos e *Compliance*, verificou que o processo de mudança é complexo

e que há dificuldade de encontrar no mercado profissionais qualificados para lidar com essa questão.

Dentre as empresas pesquisadas, observa-se que o escritório de advocacia especializado em Direito Digital, Empresa B, já tem desenvolvida uma cultura de segurança e considerou o processo de mudança como necessário concebendo-o e implantando de maneira lógica. Assim como a empresa C, essa mudança teve um sócio como coordenador da equipe de implementação. Ambas as empresas já possuíam uma política interna de segurança da informação com comitês e softwares de apoio a gestão de seus processos .

A empresa A identificou que muitos de seus clientes ainda estão se organizando e buscam orientação especializada para a adequação aos requisitos da LGPD e especialistas para atuar em conformidade com os novos parâmetros.

As três empresas envolvem nesse processo de mudança não apenas o RH, mas outros setores como TI (Tecnologia da Informação), Segurança da Informação, Governança de Dados além da análise da possível necessidade de mudança e/ou ajustes em seus processos. Essa medida pode ajudar a evitar problemas relativos às questões de *compliance*, conformidade, uma vez que amplia a visão gerencial e contempla os processos relacionados a cada requisito da lei.

Quanto a treinamento e capacitação, as empresas pesquisadas possuem no seu rol de serviços essa oferta e reconhecem a necessidades de orientar de maneira mais sistemática e metódica, não só as equipes de seus clientes, mas as suas próprias, mesmo a empresa B, cujos advogados já lidam com o tema. A empresa A destaca que nessa fase inicial, advogados têm sido os principais instrutores e a empresa C, apesar de especializada promove, por via eletrônica, reuniões de debates com suas próprias equipes e a de seus clientes. Esta última também se utiliza de softwares próprios como ferramentas de apoio nesse processo de ensino-aprendizagem. Essa iniciativa colabora para que se evite crises de informação, uma vez que unifica o discurso e cria oportunidades para esclarecer dúvidas e alinhar conceitos e parâmetros.

Implementação

Para implementação dos requisitos da Lei as empresas B e C prepararam um planejamento a partir do mapeamento de seus registros e definiram um escopo inicial, organizando logicamente seus procedimentos para essa implementação. A empresa A selecionou 112 controles para determinar o grau de maturidade de suas empresas clientes identificando índices de conformidade apenas entre 8 e 15%, o que demonstra que muito ainda precisa ser feito para a implementação. Tal resultado mostra que alguns dos fatores que levam às crises identificadas por Rosa (2001) precisam ser monitorados preservando não só os dados e informações , mas também a imagem da empresa que apresenta essa vulnerabilidade.

A empresa A, identificou ainda que alguns RH´s estão buscando profissionais especializados e que não sabem exatamente o que necessitam fazer com relação ao atendimento dos requisitos da lei. Melhor preparadas, as empresa B e C reviram seus processos e pouco precisou ser ajustado. No escritório de advocacia, empresa B, nada precisou ser alterado no RH, mas na empresa C processos e políticas precisaram ser ajustados principalmente no tocante a plano de saúde, contratação e demissão. Tal preocupação demonstra estar atento às relações de conformidade contribuindo para evitar crises de natureza legal.

A tecnologia de suporte é fonte de preocupação conforme constatou junto aos seus clientes a empresa A. Ao mesmo tempo a empresa B identificou que necessitará de melhor suporte tecnológico e C, que desenvolve e utiliza seus próprios softwares bem como o de parceiros, já se considera atendida nesse quesito. O colapso de sistemas pode derivar para a indisponibilidade de dados e/ou comprometer sua integridade, o que contribui para o não cumprimento das políticas internas de segurança da informação. Tal situação pode também gerar desconfiança por parte dos proprietários dos dados e informações sob a custódia da empresa.

Quanto ao Operador e o Controlador, profissionais definidos como necessários de acordo com o texto da LGPD, na empresa C foi definido um executivo para essas funções enquanto na A são pessoas diferentes conforme a área e as necessidades

de cada processo. De qualquer maneira, a empresa de consultoria, A, destaca que “ambos são responsáveis pela garantia da proteção de dados, privacidade, e tratamento de dados em harmonia com a finalidade” conforme definido na LGPD.

Impacto

Toda e qualquer mudança pode gerar alguma sensação de incerteza. Isso foi destacado pela empresa A que ressalta, ainda, que há um sentimento de alívio por existir agora uma lei que respalda a necessidade da implementação dos processos de segurança. Tanto a empresa B quanto a C destacaram que não houve resistência dos funcionários quanto à implementação dos requisitos da lei uma vez que ambas já trabalham com segurança da informação. Essa cultura empresarial diminui a resistência aos processos de mudança.

Para o escritório de advocacia, empresa B, os processos de mudança de implementação de tecnologias e medidas reguladoras é uma constante. Sua necessidade já é percebida pelas equipes. Para C, o processo de maneira formal começou em 2019 e ainda está em andamento considerando-se a matriz e as filiais. Já a empresa A destacou que suas empresas clientes estão estimando de 6 meses a 2 anos para que os planos de mudança e ajustes sejam plenamente cumpridos. Uma das questões postas é o custo. Conforme A, os projetos para atendimento aos requisitos podem variar de R$ 100 a R$ 500 mil, podendo chegar a um milhão ou mais dependendo do porte da empresa. Tais valores, além dos processos e tecnologias, precisa de um planejamento financeiro e muitas das empresas não estão preparadas.

Apesar dos custos envolvidos, a empresa B afirma que não há necessidade de investimentos na sua área de RH uma vez que seus processos e tecnologias de suporte disponíveis são suficientes. Já a empresa C. apesar do foco em tecnologia e segurança da informação, destaca que a fase é de implementação mas que “as configurações técnicas nos sistemas foram imediatas”. A empresa de consultoria A reforça que identifica em seus clientes que os processos não estão dominados pelos RH´s, o que pode caracterizar a necessidade de uma campanha interna de

divulgação dos procedimentos e requisitos ou mesmo treinamentos específicos com as equipes envolvidas.

Primeiros resultados

A três empresas destacam que, mesmo não estando todos os requisitos implementados, é sensível a melhora nos processos de segurança. Constatam que seus clientes estão preocupados e também implementando e/ou ajustando suas políticas e procedimentos internos. Identificaram ainda que existe uma maior atenção por parte de seus funcionários quanto aos protocolos estabelecidos e às suas responsabilidades enquanto custodiantes de dados de outrem.

Ao mesma tempo as empresas percebem como um diferencial competitivo o cuidados e o cumprimeto dos requisitos da LGPD, fortalecendo os laços de confiança com seus clientes. Tais resultados são considerados positivos e as empresas acreditam que as necessidades de atualização e o comprometimento dos profissionais vão aumentar, uma vez que o uso de meios eletrônicos vem crescendo diariamente. Para eles, esse comprometimento com as novas exigências caracteriza uma postura ética de compromisso como outro.

5 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados vem determinando ajustes e mudanças nas empresas, principalmente no tocante às áreas de Recursos Humanos. A integração entre processos, tecnologia, ambientes e pessoas de toda a organização tem se mostrado uma estratégia para a proteção de dados e informações pessoais. Essa nova dinâmica minimiza os riscos e força uma mudança, não só dos processos, mas principalmente de comportamento dos colaboradores.

Não é simples se adequar às exigências da lei, principalmente considerando os custos envolvidos, mas é certo que ela impõe um padrão, inclusive ético, objetivando a segurança dos dados pessoais.

As áreas de Recursos Humanos armazenam uma infinidade de informações de funcionários. Informações essas, muito sensíveis, não só para os que trabalham nas empresas, mas também para os que se candidatam a uma vaga ou mesmo aqueles que já saíram. Envolvidos em muitas rotinas e sempre buscando o bem estar dos funcionários, os gestores dessas áreas também necessitam estar atentos às mudanças impostas não só pela legislação trabalhista. A proteção dos dados e demais informações de cada um na empresa podem afetar as relações de confiança e isso causar algum tipo de insatisfação ou desconforto.

O objetivo geral deste estudo foi identificar fatores intervenientes na aplicação da Lei Geral de Proteção de Dados Pessoais (13.709/18), pelas áreas de Recursos Humanos e o que se pode verificar é que as áreas de RH encontram dificuldade no processo de seleção de profissionais especializados e conhecedores dos requisitos da nova lei. Verificou também que os custos de implementação são altos e o atendimentos aos requisitos envolvem outras áreas da empresa, principalmente as de governança, de tecnologia, de *compliance* e jurídica. Destaca-se ainda a necessidade de treinamento e conscientização de todos na empresa envolvendo não só os funcionários de nível básico, mas também a alta gerência e os executivos em geral.

A mudanças e ajustes são dão em todos os níveis e exigem o envolvimento de todos, a revisão dos processos, a segurança física dos ambientes, a utilização de tecnologias confiáveis além do conhecimentos dos novos requisitos legais.

A presente pesquisa é um estudo inicial sobre o problema da segurança de dados no âmbito das áreas de Recursos Humanos das empresas à luz da nova Lei Geral de Proteção de Dados Pessoais sancionada pelo presidente da República, em 2018, e que entrará em vigor em agosto de 2020. Sendo assim, as empresas ainda estão em fase de estudos e adaptação de seus processos. Dessa forma nem todos os executivos estão dispostos a conceder entrevistas sobre o assunto.

Associado a isso, toda a pesquisa ocorreu durante um período inicial da pandemia de Covid-19, quando a maioria das empresas estão com suas atividades suspensas cumprindo a determinação de isolamento social, dificultando assim o acesso deste pesquisador aos responsáveis pelas empresas.

De todas as organizações contatadas apenas três atenderam às solicitações, duas de São Paulo e uma do Rio de Janeiro. Dessas, que estão funcionando parcialmente em sistema de *home office,* as questões foram solicitadas pelos sócios, que optaram por responder por escrito.

Devido a lei ter sido sancionada recentemente e ainda não implementada pela maioria das empresas e organizações do país, não há muitos estudos nem pesquisas sobre esse assunto. Assim, a busca por informações se deu a partir de referências como normas ISO, adotadas no Brasil, literatura sobre segurança da informação e teorias e procedimentos sobre recursos humanos.

Considerando-se as informações colhidas, sugere-se como agenda futura, que seja realizada uma pesquisa de como está sendo feito o controle dos novos processos após a implementação da LGPD pelas empresas.

REFERÊNCIAS

BASTOS, Alberto; CAUBIT, Rosângela. **ISO 27001 e 27002: gestão de segurança da informação - uma visão prática**. Porto Alegre, RS: Zouk, 2009

BRASIL. **Marco Civil da Internet**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 01.03.2020 às 19h

BRASIL. **Lei Geral de Proteção de Dados Pessoais.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 03.03.2020 às 12h30

ERTHAL, Amanda; DIEHL, Liciane. **Evolução Histórica da Administração de Recursos Humanos: Um Estudo com Empresas do Vale do Taquari/RS**. 2015. Disponível em: https://www.univates.br/bdu/bitstream/10737/1008/1/2015AmandaErthal.pdf, acesso em 24.05.2020, às 21h.

FERREIRA, Beatriz Sandrim; LOOS, Mauricio Johnny. **O olhar do profissional de RH frente ao papel estratégico da área nas organizações**. Revista Expressão Católica 2019. Disponível em: http://publicacoesacademicas.unicatolicaquixada.edu.br/index.php/rec/article/view/3165. Acesso em 03.04.2020 ás 17h30

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6. ed. - São Paulo : Atlas, 2008.

COMES, Juliana. **As Fases Evolutivas e os Processos da Gestão de Pessoas.** 2016. Disponível em: https://www.linkedin.com/pulse/fases-evolutivas-e-os-processos-da-gest%C3%A3o-de-pessoas-falconi-gomes. Acesso em 24.05.2020, às 20h.

ISO. ORG. **ISO / IEC 15408-1: 2009.** ***ISO / IEC*** *Information Technology Task Force*. Disponível em: https://www.iso.org/standard/50341.html. Acesso em 02.03.2020 às 20h30

MARRAS, Jean Pierre. **Administração de Recursos Humanos - do operacional ao estratégico**. 15 ed, 2016, São Paulo: Saraiva

MORI, Amaury Haruo. **O direito à privacidade do trabalhador no ordenamento jurídico português.** Universidade de Lisboa. 2010. Disponível em: https://repositorio.ul.pt/handle/10451/3424. Acesso em 03.04.2020 às 18h13

NASCIMENTO, LCN; SOUZA TV; OLIVEIRA, ICS; MORAES, JRMM; AGUIAR, RCB; SILVA, LF. **Saturação teórica em pesquisa qualitativa: relato de experiência na entrevista com escolares.** Universidade Federal do Rio de Janeiro.. Rio de Janeiro-RJ, 2018. Disponível em:

http://www.scielo.br/pdf/reben/v71n1/pt_0034-7167-reben-71-01-0228.pdf Acesso em 07.04.2020 às 16h15

RAMOS, Anderson (org); BASTOS, Alberto; LYRA, Alexandre; ANDRUCIOLI, Alexandre; AFFONSO, Carlos; POGGI, Eduardo; PINTO, Elaine; BLUM. Renato Opice; ALEVATE, William; MARINHO, Zilta. **Security Officer 1 - Guia Oficial para Formação de Gestores em Segurança da Informação**. Porto Alegre, RS: Zouk; 2008

ROSA, Mário. **A Síndrome de Aquiles**. São Paulo: Editora Gente, 2001

SETIC. **Comitê Gestor de Segurança da Informação**. Disponível em: https://governanca.trt11.jus.br/index.php/estrutura-de-ti/comit%C3%AAs/comit%C3%AA-gestor-de-seguran%C3%A7a-da-informa%C3%A7%C3%A3o.html Acesso em 24.05.2020, às 22h

SILVEIRA, Denise Tolfo e CÓRDOVA, Fernanda Peixoto . **A Pesquisa Científica**. *in* Métodos de pesquisa / [organizado por] Tatiana Engel Gerhardt e Denise Tolfo Silveira; coordenado pela Universidade Aberta do Brasil – UAB/UFRGS e pelo Curso de Graduação Tecnológica – Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS. – Porto Alegre: Editora da UFRGS, 2009. Disponível em: http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf, acesso em 07.04.2020 às 15h48

SOUZA, Igor Guevara Loyola de. **Tentativa de Operacionalização do Modelo de Gestão por competências na Administração Direta**. UNB: 2013. Disponível em: http://bdm.unb.br/bitstream/10483/5188/1/2013_IgorGuevaraLoyoladeSouza.pdf. Acesso em 25.03.2020 às 15h30

TJDFT. **Marco Civil da Internet**. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet. Acesso em 01.03.2020 às 19h30.

APÊNDICES

Apêndice A

ENTREVISTA

Identificação:

Nome completo:_____
Sexo: _____ Idade: _____
Empresa: _____
Segmento: _____ Localidade:_____
Cargo/Função:_____
Tempo no cargo:_____

Processo de implementação da Lei Geral de Proteção de Dados na empresa:

Preparação:

- Como ocorreu esse processo de mudança?
- Quem foi responsável por implementar a mudança na empresa?
- Foi necessário criar algum setor ou área específica para gerenciar o que a lei prevê?
    - Quais outros setores, equipes ou pessoas foram envolvidas?
- Houve treinamento e definição prévia de um plano de comunicação interna e/ou externa?

Implementação:

- Que requisitos da LGPD foram implementados em sua empresa?
- O que foi alterado e o que se manteve nos processos de RH?
    - Quais processos da área de RH foram contemplados?
- Foi necessário desenvolver alguma tecnologia de suporte para essas mudanças?
    - Em caso positivo, qual (is)?

- A lei prevê um responsável pela operacionalização e proteção das informações. Como foram escolhidos o controlador e o operador?

Impacto:

- Como os funcionários reagiram às mudanças propostas?
- Foi detectado algum indício de resistência ou crise interna em função dessas alterações?
- Quanto tempo durou o processo de mudança?
- Qual o custo inicial dessa modificação?
- Os processos ajustados/implementados na área de RH já estão dominados pelo pessoal do setor?

Primeiros resultados:

- Já foi possível colher algum resultado?
    - Qual(is)?
    - Foi positivo ou negativo para a organização?
- Foi possível implementar todas a mudanças previstas?
    - Em caso parcial ou negativo, o que ainda falta?

Apêndice B

Termo de Consentimento Livre e Esclarecido- TCLE

Lei Geral de Proteção de Dados Pessoais: fatores intervenientes na aplicação pelas áreas de Recursos Humanos.
Instituição do pesquisador: UniCEUB
Professor responsável: MSc. Igor Guevara Loyola de Souza
Pesquisador assistente: William Penna Marinho de Abreu Silva.

Você está sendo convidado(a) a participar do projeto de pesquisa citado acima. O documento abaixo contém todas as informações necessárias sobre a pesquisa que estamos fazendo. Sua colaboração neste estudo será de muita importância para nós, mas se desistir a qualquer momento, isso não causará nenhum prejuízo.

Antes de decidir se deseja participar (de livre e espontânea vontade) você deverá ler e compreender todo o conteúdo. Ao final, caso decida participar, você será solicitado a assiná-lo e receberá uma cópia do mesmo.

Antes de assinar faça perguntas sobre tudo o que não tiver entendido bem. A equipe deste estudo responderá às suas perguntas a qualquer momento (antes, durante e após o estudo).

Natureza e objetivos do estudo

- O objetivo deste estudo é Identificar fatores intervenientes na aplicação da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), pelas áreas de Recursos Humanos.
- Você está sendo convidado a participar exatamente por ser um especialista no assunto.
- O presente trabalho de pesquisa faz parte de uma das atividades de avaliação da disciplina de Trabalho de Conclusão do Curso de Administração.

Procedimentos do estudo

- Sua participação consiste em relatar a experiência na aplicação da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), pelas áreas de Recursos Humanos, vivenciada na empresa em que atua.
- O procedimento será: por meio de entrevista documentada.
- Não haverá nenhuma outra forma de envolvimento ou comprometimento neste estudo.
- O tempo de participação total será de, no máximo, 1 hora.
- A pesquisa poderá ser realizada por telefone ou outro meio digital conforme sua preferência e disponibilidade.

Riscos e benefícios

- Caso esse procedimento possa gerar algum tipo de constrangimento, você não precisa realizá-lo.

- Sua participação poderá ajudar para maior conhecimento com relação aos processos internos de implantação e administração dos requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Participação, recusa e direito de se retirar do estudo

- Sua participação é voluntária. Você não terá nenhum prejuízo se não quiser participar.
- Você poderá se retirar desta pesquisa a qualquer momento, bastando para isso entrar em contato com um dos pesquisadores responsáveis.

Confidencialidade

- Seus dados serão manuseados somente pelos pesquisadores e não será permitido o acesso a outras pessoas.
- O material com as suas informações ficará guardado sob a responsabilidade de William Penna com a garantia de manutenção do sigilo e confidencialidade. Os dados e instrumentos utilizados ficarão arquivados com o pesquisador responsável até Dezembro de 2020, e após esse tempo serão destruídos.
- Os resultados deste trabalho poderão ser apresentados em encontros ou revistas científicas.
- No caso de dúvidas ou se quiserem informações sobre a sua participação no estudo, entre em contato com o pesquisador assistente pelo e-mail william.penna@sempreceub.com ou pelo WhatsApp: (61) 99294-1551.

Se houver alguma consideração ou dúvida referente aos aspectos éticos da pesquisa ou caso queira informar ocorrências irregulares ou danosas durante a sua participação no estudo, entre em contato com o professor responsável pela pesquisa: MSc. Igor Guevara Loyola de Souza pelo e-mail: igor.souza@ceub.edu.br

Eu, _____ RG _____, após receber uma explicação completa dos objetivos do estudo e dos procedimentos envolvidos concordo voluntariamente em fazer parte deste estudo.

Este Termo de Consentimento encontra-se impresso em duas vias, sendo que uma cópia será arquivada pelo pesquisador responsável, e a outra será fornecida ao senhor(a).

Brasília, ____ de _____de _

_____

Participante

_____

Pesquisador assistente: William Penna Marinho de Abreu Silva

_____

Professor Responsável: MSc. Igor Guevara Loyola de Souza

Apêndice C

Transcrição da respostas

Preparação	
Como ocorreu esse processo de mudança?	
Empresa A	O processo de mudança está acontecendo, e é bem complexo. OS RH´s estão com muita dificuldade de encontrar profissionais qualificados para execução das atividades essenciais para a elaboração de um plano de ação que ajude as empresas a seguir de forma estruturada na jornada de adequação LGPD. Algumas empresas designaram um profissional de outra área para a assumir a função como "Encarregado de Proteção de Dados e Privacidade (Jurídico, Segurança da Informação, TI, Governança de Dados, etc)
Empresa B	O escritório é especializado em Direito Digital e dentre os seus serviços, auxilia a adequação de empresas à LGPD. Por essa razão, a adequação do próprio escritório foi um processo lógico e considerado necessário por todos.
Empresa C	Desde a GDPR (Lei europeia de proteção de dados) a Empresa vem estudando o tema como especialista em *compliance* e *Cybersecurity*. Com o lançamento da LGPD no Brasil, precisamos preparar a empresa para atender a lei e apoiar os clientes.
Quem foi responsável por implementar a mudança na empresa?	
Empresa A	De acordo com a LGPD, um encarregado de proteção de dados e privacidade precisa ser designado e ser o responsável pela implementação das mudanças. Na prática, algumas empresas estão criando comitês multidisciplinares para organizar ações em conjunto, mesmo após a designação de um Encarregado.
Empresa B	Os sócios.
Empresa C	Sócio-fundador [...] tem sido o responsável pela definição da estratégia bem como orientação da empresa.

Foi necessário criar algum setor ou área específica para gerenciar o que a lei prevê?	
Empresa A	As empresas estão cautelosas quanto à criar uma área. Isso representa aumento de custos. Porém, após uma avaliação das necessidades frente à processos e ferramentas tecnológicas existentes, tem sido cada vez mais comum a aceitação de criação de processos e adoção de ferramentas tecnológicas para atender as exigências legais. Ainda assim, mesmo que uma área seja criada, outros departamentos precisarão se envolver rotineiramente nos processos de proteção de dados e privacidade (TI, Segurança da Informação, Jurídico, Governança de Dados, etc.)
Empresa B	O escritório já contava com uma Política de Segurança da Informação e com um Comitê de Segurança da Informação. Com a nomeação do DPO iniciou-se o processo de estruturação de governança em privacidade. O antigo Comitê de Segurança da Informação foi convertido em um Comitê de Segurança da Informação e da Privacidade e os coordenadores de equipes tornaram-se pontos focais de *compliance*, os "embaixadores da privacidade".
Empresa C	A Empresa funciona com uma visão sistêmica matricial, nenhuma nova área foi criada, o atendimento à lei foi pelo processo Gestão e Planejamento
Quais outros setores, equipes ou pessoas foram envolvidas?	
Empresa A	TI Jurídico Segurança da informação Governança de dados Processos
Empresa B	Todos os setores e todas as equipes estão envolvidas no *compliance* à LGPD.
Empresa C	Gestão de Pessoas (RH) TI e Segurança
Houve treinamento e definição prévia de um plano de comunicação interna e/ou externa?	

Empresa A	Não. Identificamos muita necessidade de entendimento dos requisitos legais e o que isso significa efetivamente em termos de ações práticas do cotidiano. Alguns treinamentos estão sendo apresentados por advogados especializados, mas com pouca propriedade em Tecnologia e segurança de dados. E no geral, as empresas não sabem o que fazer em termos de comunicação institucional, caso ocorra um incidente de vazamento de dados, ou uma denúncia de má utilização de dados pessoais. Não há um padrão de comunicação definido, onde esteja contida previamente um conjunto de respostas à questões comuns, tais como: · Qual é a metodologia de gestão de riscos utilizada pela empresa? · Como a empresa se prepara para tratar um incidente de segurança · O que a empresa está fazendo para atender os direitos do titular? · Quais critérios estão sendo utilizados para garantir que o tratamento de dados ocorra em harmonia com a finalidade?
Empresa B	Sim, apesar dos advogados serem já especialistas em proteção de dados, desde o começo houve treinamento, além das naturais discussões sobre o tema. Realizamos também uma campanha de comunicação interna sobre pontos de destaque de nossa política, em que todas as segundas-feiras nos *wallpapers* de todos aparece um novo infográfico com uma dica de Segurança da Informação ou da Privacidade. Chamamos de "*Privacy Mondays*".
Empresa C	Reuniões e *webinars* diversos realizados para os clientes e uso de uma solução de automatização (Modulo *Risk Manager*) e uma plataforma própria pra colaboração: Lei Digital LGPD.

Implementação

Que requisitos da LGPD foram implementados em sua empresa?

Empresa A	Temos um *framework* com 112 controles que foi criado com o propósito de determinar a maturidade em termos de capacidade de atendimento aos requisitos legais. A grande maioria das empresas tem o seu índice de maturidade variando entre 8% a 15%
Empresa B	Implementamos já a estruturação de governança, o mapeamento e o registro das atividades de tratamento de dados pessoais, e elaboramos aditivos contratuais sobre proteção de dados, além de atualização da Política e dos Avisos de privacidade.

Empresa C	A fase 1 do projeto foi a definição de escopo e aplicabilidade para definir que requisitos são aplicáveis a Empresa.
O que foi alterado e o que se manteve nos processos de RH? Quais processos da área de RH foram contemplados?	
Empresa A	Por enquanto os RH´s estão preocupados em encontrar profissionais experientes do assunto e em lidar com uma ampla quantidade de dados pessoais armazenados em seus repositórios, sem saber exatamente o que fazer.
Empresa B	Os processos de RH não precisaram ser alterados. Mapeamos todos os processos da área, mas nenhum deles precisou de ajustes adicionais, pois já havia o cuidado com o tema no escritório.
Empresa C	Políticas e procedimentos técnicos para tratamento de dados pessoais, por exemplo envio anonimizado de planilhas. Processos do Departamento Pessoal, plano de saúde, contratação e demissão.
Foi necessário desenvolver alguma tecnologia de suporte para essas mudanças? Em caso positivo, qual (is)?	
Empresa A	As empresas admitem que há a necessidade de suporte tecnológico para atendimentos aos requisitos *legis*. Entretanto, não há uma solução que contemple a capacidade de atender todas as necessidades. As ferramentas mais comentadas atualmente são: · *BigID – Data mapping, data Discovery*, gestão do consentimento, *Business Porcessing*, inventário de tados; · *DLP´s – Data Loss Prevention* – Ferramentas de prevenção quanto ao uso indevido de dados classificados; · *OneTrust* – Plataforma de soluções para Governança de Proteção de Dados e Privacidade;
Empresa B	Temos mapeados alguns pontos, notadamente de segurança da informação, que necessitarão de suporte tecnológico.
Empresa C	Utilização da própria tecnologia existente da Empresa para implementar a LGPD nos clientes bem como configuração dos recursos de segurança do ambiente de TI. · Modulo *Risk Manager* e Lei Digital LGPD.

	· Recursos de segurança e proteção de dados do ambiente em nuvem da Microsoft (Azure e M365)
A lei prevê um responsável pela operacionalização e proteção das informações. Como foram escolhidos o controlador e o operador?	
Empresa A	O perfil da empresa como Controlador é dado principalmente pelo fato de essa empresa ser a responsável pela coleta e tratamento de dados pessoais. O Operador é um terceiro, subcontratado pelo controlador, para executar parte da operação de tratamento de dados pessoais. Ambos são responsáveis pela garantia da proteção de dados, privacidade, e tratamento de dados em harmonia com a finalidade;
Empresa B	O controlador e o operador não são escolhidos. Eles são definidos de acordo com as atividades de tratamento de dados pessoais que realizam. Se um agente decide sobre o tratamento de dados ele é considerado pela lei como controlador; se apenas age sob a decisão de outrem, cumprindo seu mandato, é operador.
Empresa C	O encarregado (DPO) da empresa foi escolhido um executivo com foco no negócio da empresa.

Impacto	
Como os funcionários reagiram às mudanças propostas? Foi detectado algum indício de resistência ou crise interna em função dessas alterações?	
Empresa A	Há um sentimento de incerteza, e incapacidade de atender os requisitos legais. Ao mesmo tempo, há um certo alívio, diante do fato de que ter processos, tecnologias e pessoas especializadas para proteger informações – especialmente dados pessoais – agora é lei.
Empresa B	Não houve resistência, pois como o escritório dedica-se ao tema, todos já estão habituados com a sua importância.
Empresa C	Sendo uma empresa de segurança, os colaboradores já possuíam conscientização sobre a necessidade de proteger os dados, no caso específico da LGPD, o foco foi para privacidade. Não, a implementação seguiu incorporando as práticas nos processos atuais bem como reforço da tecnologia de segurança do ambiente informatizado.

Quanto tempo durou o processo de mudança?	
Empresa A	As empresas estão encontrando planos de mudança que podem levar de 6 meses até 2 anos, até conseguir alcançar condições de adequação à LGPD;
Empresa B	O processo de *compliance* é contínuo, está em permanente aperfeiçoamento.
Empresa C	Ainda em andamento. O projeto teve início em setembro/2019.
Qual o custo inicial dessa modificação?	
Empresa A	Difícil mensurar: Os custos de consultoria para diagnóstico podem variar de R$ 100 a R$ 500 mil, a depender do tamanho da empresa. Se houver necessidade de aquisição de sistemas, contratação de pessoas e serviços terceirizados para implantação, o investimento poderá passar de R$ 1 Milhão por ano, dependendo do tamanho da empresa;
Empresa B	Não respondeu
Empresa C	Sem custo adicional, utilizando recursos próprios
Os processos ajustados/implementados na área de RH já estão dominados pelo pessoal do setor?	
Empresa A	Não absolutamente;
Empresa B	Como dito, não houve necessidade de ajustes específicos no setor de RH.
Empresa C	Em implementação. As configurações técnicas nos sistemas foram imediatas.

Primeiros resultados	
Já foi possível colher algum resultado?Qual(is)? Foi positivo ou negativo para a organização?	
Empresa A	As empresas que já realizaram os serviços de diagnóstico, já possuem uma ideia de onde estão e do esforço necessário para alcançar a adequação; É positivo por que a empresa passa a saber o que precisa fazer e quanto terá que investir para conseguir a conformidade, e é negativo por que as empresas não haviam se preparado para investimentos tão elevados, sem aumento de receita, especialmente diante de uma pandemia mundial;
Empresa B	A preocupação com proteção de dados é muito positiva, pois denota preocupação com o impacto de nossas atividades na vida de colaboradores e clientes. É certamente um diferencial competitivo e uma postura ética adotada pelo escritório.
Empresa C	Melhoria da segurança geral da empresa e conhecimento interno para oferecer como solução para nossos clientes. Já executamos mais de 20 projetos de implementação de LGPD nos clientes, várias palestras e desenvolvimento de uma solução inédita para colaboração via *WEB*. Muito positivo, reforçou o posicionamento da empresa e colocou a Empresa como líder em automatização para LGPD.
Foi possível implementar todas a mudanças previstas? Em caso negativo, o que ainda falta?	
Empresa A	Não. As mudanças previstas serão implementadas nos próximos 18 meses, na grande maioria das empresas; · Algumas coisas ainda faltam, como por exemplo: o Elaboração de uma política de proteção de dados e privacidade; o Estabelecimento de rotinas de atendimento aos direitos do titular; ● Designação de um encarregado de proteção de dados; o Especificação de métodos de proteção de dados; o Atribuição de bases *legis* para uso de dados existentes nos processos atuais; o Contratação de pessoal especializado; o Elaboração de Processos de Gestão de Incidentes; o Elaboração do Plano de Comunicação o Constituição de um Comitê Multidisciplinar de Proteção de Dados Pessoais

	○ Etc.
Empresa B	Estamos permanentemente adotando novas melhorias.
Empresa C	Em andamento. Falta ainda algumas implementações técnicas e mudanças em processos.