Uma introdução sobre Cyber Security e LGPD – Parte 2

Published on October 14, 2019

Waldemir Cambiucci

Technical Sales Manager | Director at Microsoft Technology Center São Paulo

No artigo anterior iniciamos nosso bate-papo sobre segurança no espaço digital. Falamos sobre diversas propriedades, conceitos e ferramentas em segurança da informação, além de posicionar os principais componentes da plataforma Microsoft para uma estratégia em segurança no ambiente corporativo. Neste artigo, vamos continuar com o tema, explorando com alguma profundidade a **LGPD – Lei Geral de Proteção de Dados**, sempre com uma abordagem focada em tecnologia. Não iremos focar aspectos jurídicos da nova Lei, mas sempre que possível, espero conectar os pontos dessa estratégia que exige uma integração entre times de diferentes segmentos, seja jurídico, legal, conformidade, compras, contratos e tecnologia. No final do artigo, vamos explorar novos componentes de uma infraestrutura preparada para LGPD e terminar com alguns roteiros de certificações e estudos em segurança da informação, para interessados na área. Vamos lá?

Privacidade de dados

Começar por privacidade de dados é bastante adequado! Manter a privacidade de dados é muito mais que apenas garantir que informações sensíveis estejam protegidas de acessos indesejáveis

ou vazamentos; manter a privacidade das informações pode proteger pessoas, crianças e organizações de situações irreversíveis de prejuízo de imagem, saúde ou financeiros.

O desafio é que atualmente, qualquer empresa conectada no ambiente de negócio digital precisa de dados pessoais em diferentes momentos, seja para informações previstas legalmente para execução do negócio, como seu endereço e CPF para a abertura de contas em banco digital, ou informações médicas para prescrição de medicamentos corretos, ou simplesmente o número de sapato que você calça, para lançamentos de promoções futuras, quando dado o consentimento. O problema acontece quando empresas coletam e manipulam mais informações do que realmente precisam para executar seus serviços, ou até compartilham indevidamente informações que foram previamente fornecidas por seus clientes para um uso específico.

Vejamos alguns exemplos de quebra de privacidade, sem o envolvimento de ferramentas de tecnologia, mas apenas de processos:

Caso 1: você visita um shopping center em comemorações de Natal. O shopping contratou uma empresa de marketing que elaborou uma campanha e desenvolveu totens com inteligência artificial para troca de notas fiscais por bilhetes para um sorteio. Para compras acima de 300 reais, você pode apresentar a nota fiscal e receber um bilhete para concorrer a um belo carro, exposto no centro do shopping. Você se anima, realiza suas compras acima de 300 reais e vai até o *kiosk* para receber seu bilhete e concorrer. Você é orientado a preencher um formulário num *toten* de autoatendimento simpático, desenvolvido pela empresa de marketing, que irá ao final imprimir seu número para concorrer ao carro.

Situação: durante o preenchimento, o formulário exige não apenas uma foto da nota fiscal com o valor acima de 300 reais, mas também inúmeras informações sobre você, seu endereço, RG, CPF, sua foto tirada na hora, sua idade, se você está trabalhando, seus gostos pessoais, seu *facebook*, *linkedin*, se você é casado, se mora de aluguel ou tem casa própria, se tem um cachorro ou um gato, se usa óculos, etc. Essas informações são armazenadas no sistema e ao final, você recebe um bilhete com 1 número para concorrer ao carro. E boa sorte! 😊

Problema: por que a empresa pediu tantas informações para um serviço de impressão de um bilhete possivelmente premiado? O que a empresa irá fazer com tantas informações? O anunciado pelo shopping era que seria apenas necessário apresentar o cupon com valor acima de 300 reais e você receberia um bilhete.

Impacto: em caso de vazamento de dados, qual é a responsabilidade de cada empresa sobre esse caso? O shopping é responsável em caso de vazamento ou é a empresa terceirizada para realizar a campanha? E se o shopping ou a empresa vender os dados para outras campanhas de marketing, onde então acontecer um vazamento durante a transação? Quem será responsável?

Infelizmente, empresas coletam dados além do necessário para seus serviços. Em alguns casos, empresas compram dados de forma irregular de outras empresas, sem o consentimento prévio de usuários e clientes, que haviam fornecido seus dados para um ato específico, para uma empresa em específico e não foram questionados sobre a permissão para transações extras sobre esses

dados. Nossos dados pessoais têm sido manipulados, persistidos ou negociados de forma imprudente, muitas vezes sem um cuidado quanto a privacidade ou segurança desses dados, seja pela ausência de ferramentas e infraestrutura técnica para segurança da informação, seja pela ausência de processos e políticas administrativas que protejam esses dados no ambiente de negócio.

Caso 2: um grupo de pesquisadores coleta dados de voluntários para uma pesquisa médica, acompanhando o comportamento e evolução desses pacientes ao longo de um tratamento específico. Esses pacientes sofrem de uma doença rara e até então desconhecida do grande público. O laboratório tomou todas as providências administrativas e recebeu o consentimento dos pacientes para manipular diversas informações pessoais, incluindo histórico clínico de cada pessoa, doenças na família, hábitos alimentares, informações íntimas diversas, etc.

Situação: por ser um laboratório famoso, a mídia constantemente recebe jornalistas para visitas guiadas. Em uma dessas visitas, um médico havia deixado um notebook desbloqueado com uma planilha repleta de nomes e status clínicos na tela. Um jornalista em visita tirou uma foto sem ser percebido e na semana seguinte, publicou um caso sobre inúmeras pessoas sofrendo de uma doença rara e desconhecida, gerando pânico na cidade e constrangimentos ainda maiores para os envolvidos. Nada contra jornalistas; é apenas uma situação hipotética em outro país! 😊

Problema: ferramentas de TI e processos administrativos não são capazes de proteger dados pessoais sozinhos. É preciso uma cultura de segurança e privacidade na empresa, adotada e aplicada no dia-a-dia por todos os funcionários e colaboradores. Apesar do laboratório usar as últimas tecnologias em criptografia, proteção de *endpoints* e estações de trabalho, monitoração ativa contra ataques, sistemas de *EDR, SOAR, SIEM*, políticas corporativas de segurança em servidores e redes, etc., o vazamento aconteceu. Apesar do laboratório ter tomado todas as medidas administrativas, recebendo o consentimento por escrito de cada pessoa participante da pesquisa, o vazamento aconteceu simplesmente através de uma tela de uma máquina aberta em área de visitação, deixada por um médico não treinado em segurança da informação.

Impacto: vazamentos de dados em cenários de saúde podem gerar repercussões gigantescas, para pessoas, empresas e até governos.

Nesse cenário, fica claro que faltou treinamento e conscientização dos médicos e colaboradores sobre uma cultura de segurança. Bastaria manter uma mesa limpa de documentos ou um notebook bloqueado quando desassistido que o vazamento seria evitado. Mais de 70% dos vazamentos de dados são devidos a cenários de negligência e não por dolo ou ação intencional.

Momento para reflexão!

O que você acha disso? É um cenário incomum? Ou acontece normalmente hoje em dia no Brasil? E no mundo? Você está confortável em fornecer informações sensíveis para uma empresa não confiável? Sua empresa compra dados pessoais no mercado, para realizar suas campanhas e negócios? E como está a cultura de segurança em sua empresa? É possível capturar

informações críticas na mesa de seus funcionários e colaboradores? Dados pessoais de clientes ou de funcionários são facilmente expostos pelos corredores ou murais de sua empresa? Seus funcionários compartilham informações em áreas públicas, como elevadores, corredores e espaços abertos? Existem tantas outras perguntas que poderíamos fazer, que deixo o exercício para o leitor.

Esse é o contexto para segurança da informação e LGPD – Lei Geral de Proteção de Dados, que ultrapassa em muitos quilómetros apenas a segurança de TI.

Antes de prosseguir, importante comentar que esse texto não é um guia definitivo sobre LGPD. Você pode encontrar na web uma diversidade de fontes de conteúdo, treinamentos, palestras, vídeos, certificações e literatura extensa sobre LGPD e seus aspectos jurídicos, legais e técnicos.

Mas espero trazer minha colaboração para o leitor, destacando pontos de forma prática, ajudando você e sua empresa nos primeiros passos para uma jornada de segurança e conformidade com LGPD. O caminho será longo, mas não é impossível!

O que significa realmente privacidade?

Em nosso contexto, a privacidade de dados está relacionada a todos os dados pessoais que uma organização coleta para executar seus negócios e serviços, **aceitando o compromisso de manipular esses dados com responsabilidade.**

Apenas essa definição já pode explicar a necessidade de uma regulamentação sobre dados pessoais. Nos últimos anos, vimos inúmeros casos de mau uso de dados pessoais no mercado, gerando situações críticas e punições com impacto direto para pessoas e organizações, como nos exemplos que vimos anteriormente.

O que são dados pessoais?

Para trabalharmos a privacidade de dados, precisamos definir o que são **dados pessoais**. Dados pessoais são muito mais do que os chamados **PII (*Personally Identifiable Information*)** ou **Informações de identificação pessoal**. Um PII pode ser um dado de relacionamento direto com sua identidade, como seu endereço, seu RG ou CPF.

Dados pessoais podem ser quaisquer dados vinculados ou vinculáveis a uma pessoa em particular, de forma direta ou indireta.

Os dados pessoais incluem dados autenticados e não autenticados, vinculados ou vinculáveis a um indivíduo, um ID do dispositivo ou ainda qualquer ID semelhante que indique um usuário. Veja que dados pessoais incluem quaisquer dados vinculados direta ou indiretamente a uma pessoa, por exemplo:

· *um identificador único, como nome, número de identificação RG, CPF, dados de localização GPS, identificador on-line em redes sociais, etc.;*

· *um ou mais fatores específicos à identidade física, psicológica, genética, mental, de etnia, econômica, cultural ou social desse indivíduo;*

Considerando todas essas informações, uma pessoa pode se sentir prejudicada ou constrangida ao ter um dado pessoal compartilhado ou vazado, além da fronteira previamente consentida para manipulação desse dado.

Privacidade é um direito fundamental do homem

Privacidade é muito mais que apenas um conceito envolvendo informações sensíveis de pessoas.

Privacidade é também um componente crítico e previsto na **Declaração Universal dos Direitos Humanos (DUDH),** de 1948.

https://www.direitocom.com/declaracao-universal-dos-direitos-humanos/artigo-12o

No artigo XII da DUDH temos o seguinte texto:

Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.

Esse artigo deixa claro o impacto e importância da privacidade para a dignidade humana. Todos nós temos direito a manutenção de dados sensíveis sob sigilo, exigindo o uso desses dados com responsabilidade.

Finalmente, o **artigo 5 inciso X da Constituição Federal de 1988** destaca o impacto da privacidade para os brasileiros, onde lemos:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

*X - **são invioláveis a intimidade, a vida privada,** a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

Novamente, a privacidade é destacada como um direito legal, inviolável e caro para as pessoas, exigindo cuidado e atenção em sua observação.

O que é o GDPR – General Data Protection Regulation?

Vimos nos últimos anos violações de privacidade acontecendo de forma sistemática em diferentes mercados. Casos diversos de vazamentos de dados e manipulação indevida de informações sucederam na mídia, o que gerou no **Mercado Comum Europeu** a preocupação pela proteção dos dados pessoais de forma mais intensa desde o início da década. Esse movimento fez surgir o **GDPR – General Data Protection Regulation** - ou **Regulamento Geral sobre a Proteção de Dados 2016/679**, um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu.

Esse projeto foi idealizado em 2012 e seguiu anos de discussões, sendo aprovado em 2016, entrando em vigor a partir de **25 de maio de 2018.** Em diversos aspectos, a GDPR já mudou o ambiente de negócios de forma global. Inúmeras empresas não se limitaram na observação da GDPR apenas para serviços executados na zona do euro, ampliando sua aplicação para todo o mundo. A Microsoft, por exemplo, adotou as orientações de GDPR para todos os territórios onde realiza negócios, não apenas para serviços aplicados no mercado europeu. Outras empresas mudaram suas políticas de contratação e parcerias, aceitando apenas outras empresas que observam os critérios de GDPR como guia para segurança e privacidade de dados, ou mesmo escolheram fazer negócios apenas com empresas de países onde leis e regulamentos oficiais similares ao GDPR estão implementados.

Como impacto direto no Brasil, empresas brasileiras que não observarem a LGPD poderão com grande certeza perder negócios internacionais com empresas que irão exigir provas de adoção de uma estratégia de privacidade e proteção a dados pessoais. Não observar LGPD irá tirar empresas do ambiente de negócios a partir de 2020.

Para fazer sua primeira leitura sobre a **GDPR – General Data Protection Regulation**, veja o link a seguir: https://gdpr-info.eu/

O que é a LGPD - Lei Geral de Proteção de Dados?

A LGPD ou Lei no 13.709/2018 é a legislação brasileira que regula as atividades de tratamento de dados pessoais, válida em todo território nacional.

A LGPD foi publicada em agosto de 2018 e entrou em ***Vacatio Legis***, que do grego significa ***"vacância da lei",*** pelo período de 24 meses para a preparação e adoção por parte das empresas no mercado.

Assim, a lei entrará em vigor em **agosto de 2020**, quando diversas rotinas de segurança da informação e políticas de privacidade deverão ser observadas, com risco legal para empresas denunciadas.

Muito já tem se falado no mercado sobre a LGPD e seu impacto no Brasil, posicionando a lei como nossa versão local da GDPR. Nada mais correto do que esse posicionamento: a LGPD terá sim grande impacto para empresas no Brasil e de fato, é nossa versão local para a GDPR, que já vem mudando as relações comerciais em diversos mercados pelo mundo.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

· http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Alguns comentários antes de prosseguirmos:

1. **Não ignore a LGPD.** Ela irá realmente criar uma nova realidade sobre o tratamento de dados pessoais e políticas de privacidade no Brasil, exigindo adaptações para empresas e processos de negócio;

2. **Não faça um projeto *"só para inglês ver"* para LGPD.** Procure realmente entender o impacto da Lei para seus negócios e processos, iniciando desde agora sua jornada para adoção de padrões de privacidade e conformidade com a nova legislação;

3. **Não, a LGPD não é um monstro de 56 cabeças quânticas que irá devorá-lo.** É realmente possível criar uma estratégia de segurança e privacidade que irá deixá-lo coberto sobre os componentes previstos na Lei. Mas para isso, é importante começar agora com um time virtual ou dedicado de LGPD;

4. **Ao longo dessa jornada, envolva toda a empresa**, de diferentes áreas como marketing, compras, jurídico, imprensa, tecnologia, negócios, etc. LGPD não é definitivamente uma Lei apenas para áreas de tecnologia ou jurídico. **LGPD é para toda a empresa!**

Feitas essas considerações, vamos olhar um pouco mais de perto alguns aspectos da Lei.

Qual será o alcance da LGPD?

A lei será válida para todo território nacional, sendo aplicada sobre qualquer operação de **tratamento em dados pessoais** realizada por pessoa natural (indivíduo) ou jurídica (empresa), de direito público (órgão de governo) ou privado (empresa comercial).

Esse tratamento sobre dados pessoais prevê os cenários de coleta de dados, assim como manipulação para o oferecimento de bens e serviços para indivíduos localizados no território nacional.

Esse formalismo jurídico na definição de termos, contexto, aplicação, vigência e alcance é importante, uma vez que o impacto da nova legislação sobre empresas denunciadas pode ser

grande. As multas em processos por denúncias de mau uso de dados pessoais podem chegar a valores de até **50 milhões de reais por infração**, o que em muitos casos poderá determinar o fim das operações da empresa.

Existem diversas questões sobre a forma como multas e advertências serão aplicadas a partir de agosto de 2020, sempre dependendo de cada caso.

O que são dados pessoais sensíveis?

Vimos anteriormente que dados pessoais são informações relacionadas a pessoas identificadas ou identificáveis através desses dados.

Dados pessoais sensíveis adicionam um elemento ao dado pessoal, categorizando dados cujo conteúdo e valor podem oferecer vulnerabilidade ao indivíduo. Essa vulnerabilidade também pode variar, chegando ao risco de morte.

Por exemplo: em certos países, a informação sobre a religião de um indivíduo pode ser classificada como pública, sendo amplamente divulgada em diferentes meios. Em outras regiões, essa informação sobre a religião praticada por uma pessoa poder ser uma questão de vida ou morte, por perseguições ou discriminações existentes naquela sociedade. Assim, religião proferida por alguém é um dado pessoal sensível.

A LGPD prevê **dados pessoais sensíveis** diversos como etnia, posicionamento político, filiação ou convicção religiosa, dados clínicos, dados genéticos, dados de menores de idade, dados biométricos, entre outros.

Tratamento de dados pessoais

O tratamento de dados pessoais conforme previsto na LGPD abrange um grande conjunto de operações efetuadas sobre dados pessoais, por meios manuais ou automatizados, incluindo a coleta, o registro, a organização, a classificação, a persistência, a manipulação ou alteração, a recuperação, a consulta, a utilização, a publicação por transmissão, ou qualquer outra forma de disponibilização, a remoção ou a destruição de dados pessoais de arquivos, seja em meios digitais ou físicos.

Aqui, novamente a LGPD amplia sua atuação para além dos meios digitais. Uma empresa que manipula e faz o tratamento de dados pessoais apenas em meios físicos, como formulários em papel, questionários em fichários físicos ou cadernetas de apontamentos, estão igualmente expostas às determinações da Lei.

Quem são os participantes da LGPD?

Uma vez que dados pessoais serão tratados por empresas, a LGPD define papéis e entidades envolvidas no processo de aplicação da lei, como vemos a seguir:

· **TITULAR:** refere-se ao indivíduo ou pessoa natural identificado pelos dados pessoais. Eu e você somos titulares de dados pessoais sendo tratados;

· **CONTROLADOR:** a LGPD define o **controlador** como sendo a pessoa natural ou jurídica, de direito público ou privado, que é responsável pelas decisões relacionados ao tratamento de dados pessoais. Em nosso exemplo, o shopping center da campanha de Natal com bilhete premiado seria o **controlador** para a LGPD,;

· **OPERADOR:** a LGPD também define o conceito de um **operador**, como sendo a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do **controlador**. Novamente em nosso exemplo, a empresa de marketing contratada pelo shopping é o **operador** desse cenário, coletando dados pessoais através de totens de atendimento para emissão dos bilhetes para o sorteio;

· **CONTROLADOR** e **OPERADOR** podem ser chamados igualmente de **AGENTES DE TRATAMENTO DE DADOS PESSOAIS**, sendo as principais entidades envolvidas no tratamento de dados cobertos pela LGPD;

· Finalmente, a LGPD ainda define o conceito de **ENCARREGADO** ou **DATA PROTECTION OFFICER (DPO)** que é a pessoa apontada pelo **controlador** para atuar como canal de comunicação entre o **controlador**, os **titulares** de dados pessoais e a chamada **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS**;

· A **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD** – deve ser o órgão representativo que irá aceitar denúncias do mercado e direcionar processos cabíveis, de acordo com o impacto para vazamentos e uso indevido de dados pessoais.

Quem é o DPO?

O DPO tem um papel importante como interface entre a empresa **controladora** de dados e os diferentes papeis previstos, exigindo do DPO um cuidado e dedicação intensos.

Diferentemente do **CISO – Chief Information Security Officer**, que possui uma dedicação maior para a segurança da informação, cobrindo técnicas e ações de proteção contra ameaças cibernéticas no ambiente corporativo, o **DPO – Data Protection Office** – será responsável pela interface da empresa controladora com a ANPD, além de ser responsável pela condução da estratégia de LGPD na empresa. Parte importante dessa estratégia será o portfolio de projetos diversos em execução, para conformidade da empresa com a LGPD. Esses projetos não serão apenas de TI, quando a interface com o CISO será importante. Também deverão ser previstos projetos de revisão de contratos, processos de obtenção de consentimento para uso de

dados, inventários de dados persistidos e realmente necessários para a execução do negócio, entre inúmeras outras atividades.

Sem dúvida, o CISO será um grande aliado do DPO para a LGPD.

A Lei ainda prevê a possibilidade de um DPO ser terceirizado, através de uma pessoa ou empresa prestadora de serviços. Isso será importante para empresas de pequeno e médio porte, que não possuem orçamento para suportar um DPO dedicado em sua empresa. Organizações comerciais e cooperativas poderão explorar os trabalhos de um DPO que suportar mais de uma empresa na jornada de conformidade com a LGPD.

Podemos já afirmar que a carreira de DPO apresenta-se como uma grande oportunidade para os próximos anos, exigindo grande formação em diferentes pilares de informação, segurança, conformidade, processos, contratos, etc., além de amplo conhecimento da própria lei LGPD. Já existem certificações e carreiras para treinamentos de um DPO. Falaremos disso ainda no texto.

Artigos importantes da LGPD

Novamente, o objetivo desse artigo não é de aplicar intenso debate jurídico sobre LGPD, mas apontar alguns caminhos para o leitor iniciar essa jornada. Assim, para uma leitura mais dedicada sobre a LGPD, recomendo o link a seguir:

Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

· http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Alguns artigos de destaque da Lei comento a seguir:

· **Artigo 6:** define princípios importantes que devem ser perseguidos para o **tratamento de dados pessoais**, em relação a finalidade, adequação, necessidade, qualidade, transparência, segurança, prevenção, não discriminação, entre outros.

· **Artigo 7:** sobre o consentimento que deve ser fornecido pelo TITULAR para a realização de tratamento de dados pessoais;

· **Artigo 10:** sobre o consentimento dado pelo TITULAR para o CONTROLADOR fazer uso de seus DADOS PESSOAIS, no exercício de operação de seus serviços, como **legítimo interesse** para o fornecimento de bens e serviços contratados.

· **Artigo 11:** sobre o **tratamento de dados pessoais sensíveis** e a forma como o TITULAR pode permitir esse tratamento;

· **Artigo 16, 18:** sobre o direito ao **esquecimento**. O TITULAR tem direito de exigir esquecimento de seus dados pessoais pelo CONTROLADOR, o que exige a interrupção de tratamento de dados pessoais do TITULAR pelo CONTROLADOR, por diversas razões possíveis, como revogação de consentimento, determinação da ANPD, fim de contratação de serviços, etc.

· **Artigo 50:** o artigo 50 da LGPD é importante e deve ser conhecido, pois explica diferentes regras de boas práticas e de governança que devem existir na empresa, suportando um tratamento de dados pessoais seguro;

· **Artigo 52:** aqui são previstas as sanções administrativas para o descumprimento da LGPD, com impacto direto para as empresas denunciadas. Entre as medidas citadas destacamos:

o *I - advertência, com indicação de prazo para adoção de medidas corretivas;*

o *II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;*

o *III - multa diária, observado o limite total a que se refere o inciso II;*

o *IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;*

o *V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;*

o *VI - eliminação dos dados pessoais a que se refere a infração;*

Um ponto importante sobre a LGPD é que ela possui cenários previstos **onde a lei não se aplica**, como o tratamento de dados para *fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais*. Para esses casos e outros colocados no texto da Lei, a LGPD não se aplica.

Destaco aqui a importância de cada empresa ter seu corpo jurídico ciente da LGPD, assim como a necessidade de formação de um time de trabalho *multi-disciplinar* em torno de um projeto de LGPD na empresa, para início imediato caso ainda não exista.

Uma abordagem para esse time de projeto é colocar como alvo **agosto de 2020** como data fim do projeto em sua versão 1.0. Até agosto de 2020, a empresa deveria seguir um cronograma de execução, prevendo diversas ações conforme os artigos da Lei, envolvendo diferentes segmentos da empresa, para que a criação de um **relatório de impacto sobre a LGPD** em sua empresa. Veja a seguir esse importante componente também previsto pela LGPD.

Relatório de Impacto na LGPD

O RELATÓRIO DE IMPACTO na LGPD pode ser definido como o documento gerado pelo CONTROLADOR, contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos à privacidade e direitos fundamentos de pessoas ou TITULARES, assim como as medidas e projetos em execução para ampliar a segurança e manutenção da privacidade na empresa. O DPO é o responsável pela condução e consolidação desse documento, que deve ser vivo e mantido atualizado ao longo da jornada de LGPD na empresa e pronto para divulgação quando requisitado pela ANPD, em alguma situação de risco ou denúncia.

Um bom começo para as empresas é consolidar uma estrutura para o documento RELATÓRIO DE IMPACTO, onde todos os cenários da LGPD e tratamento de dados pessoais estão descritos, assim como medidas em meio digital para ampliar a segurança e proteger os dados sensíveis de pessoas durante o processamento de dados na empresa.

A Lei não oferece um documento padrão como *template* para esse RELATÓRIO DE IMPACTO. Por isso, recomendo o exercício imediato dentro da empresa, envolvendo os times jurídicos e de TI, para cobertura dos projetos que serão conduzidos até agosto de 2020.

E assim cobrimos alguns aspectos importantes da LGPD, mas não completamente. De forma prática, a Lei deve mudar a forma como muitas empresas pensam dados pessoais, seja de clientes ou de funcionários. Será uma grande mudança de paradigma, comparável com a adoção da **Lei de Defesa do Consumidor**, como já comentado.

No artigo a seguir, você irá encontrar um mapa ampliado sobre aspectos da LGPD. Não deixe de visitar esse material:

Começando a sua jornada em torno da Lei Geral Brasileira de Proteção de Dados Pessoais (LGPD)

- Ref.: https://www.microsoft.com/pt-br/lgpd

Suportando a LGPD com tecnologia Microsoft 365

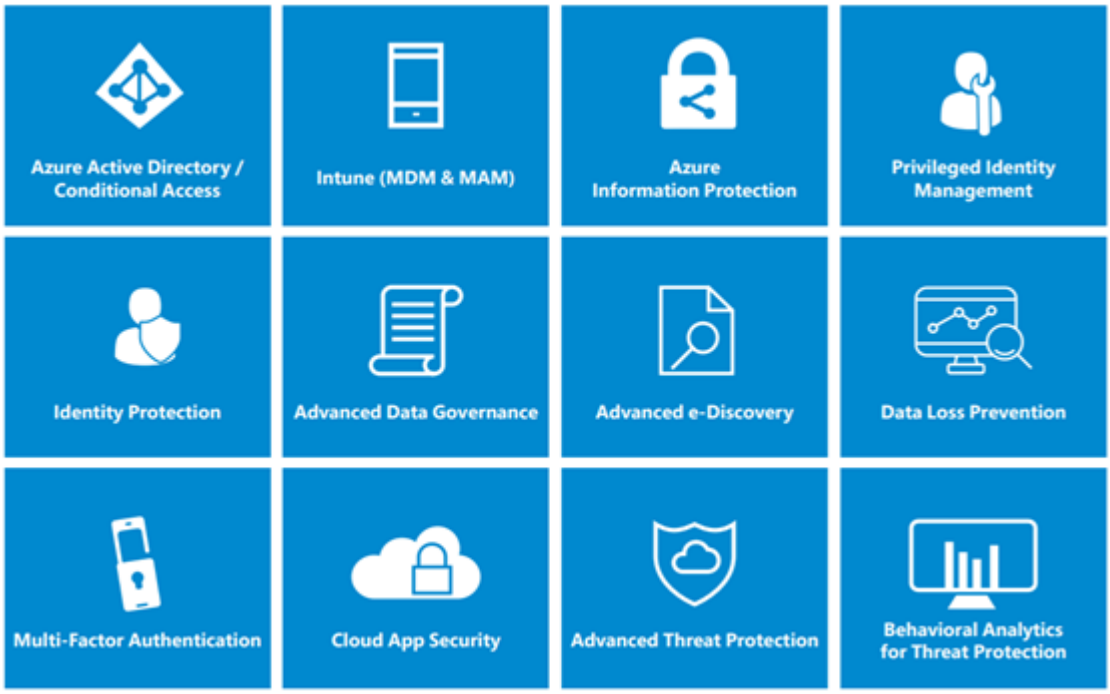
No artigo anterior, vimos um mapa de tecnologias aplicadas para segurança da informação no ambiente corporativo. A seguir, vamos explorar diversos componentes adicionais que suportam cenários de LGPD, para a manutenção da privacidade de dados e segurança da informação.

Como comentado diversas vezes ao longo do artigo, LGPD não é apenas para TI. Mas o uso e aplicação de ferramentas de tecnologia para proteção de ameaças é um componente crítico na estratégia de conformidade e governança de dados, conforme previsto no Artigo 50 da LGPD.

Veja a seguir:

- *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 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.*

Pensando em plataforma Microsoft, podemos destacar os seguintes componentes:



Vemos aqui diferentes componentes que podem suportar cenários diversos de aplicação e conformidade da LGPD.

· Azure Active Directory / Conditional Access:

o https://docs.microsoft.com/pt-br/azure/active-directory/conditional-access/overview

· Intune (MDM/MAM):

- https://docs.microsoft.com/pt-br/Intune/

- Azure Information Protection:

- https://docs.microsoft.com/pt-br/azure/information-protection/what-is-information-protection

- Privileged Identity Management:

- https://docs.microsoft.com/pt-br/azure/active-directory/privileged-identity-management/pim-configure

- Identity Protection:

- https://docs.microsoft.com/pt-br/azure/active-directory/identity-protection/overview

- Advanced Data Governance:

- https://docs.microsoft.com/pt-br/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center

- Advanced e-Discovery:

- https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-advanced-ediscovery

- Data Loss Prevention:

- https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies

- Multi-Factor Authentication:

- https://docs.microsoft.com/pt-br/office365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

- Cloud App Security:

- https://docs.microsoft.com/pt-br/cloud-app-security/what-is-cloud-app-security

- Advanced Threat Protection:

  - https://docs.microsoft.com/pt-br/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

- Behavioral Analytics for Threat Protection:

  - https://docs.microsoft.com/pt-br/advanced-threat-analytics/what-is-ata

Esses componentes podem ser aplicados de forma combinada para cenários comuns previstos na LGPD, como:

1. Necessidade de encontrar os dados pessoais de um TITULAR quando requisitado, dentro de uma repositório de dados não estruturados;

2. Necessidade de assegurar a proteção dos dados em estrutura local, na nuvem e em dispositivos móveis, sempre com máxima proteção de *endpoints* em diferentes cenários de acesso;

3. Necessidade de garantir e restringir o acesso aos dados pessoais, limitando-se esse acesso para pessoas autorizadas, através de condições a partir de dispositivos, horários, autenticação ou localidades;

4. Garantir o acompanhamento sobre os dados armazenados em aplicações na nuvem, através da monitoração de acessos e conexões entre ambientes diversos;

5. Garantir a monitoração ativa da infraestrutura, detectando ameaças antes que causem danos maiores para a organização;

6. Garantir o acompanhamento e registro de esforços de conformidade sendo realizados ao longo do tempo, através de ferramentas de auditoria e log de atividades;

7. Garantir a execução imediata de requisições de titulares de dados pessoais sobre seus dados presentes na plataforma de negócios da empresa, seja para os casos de consulta, alteração ou esquecimento, entre outros.

Cada cenário pode contemplar uma arquitetura específica de Microsoft 365, combinando os recursos da plataforma. De fato, cada um merece um artigo especial dedicado, cobrindo boas práticas de projeto, exemplos de arquitetura, desafios de campo, roadmap de adoção e benefícios. Fica assim a provocação para outros autores de plantão! *;)*

Certificações em segurança e material de estudo

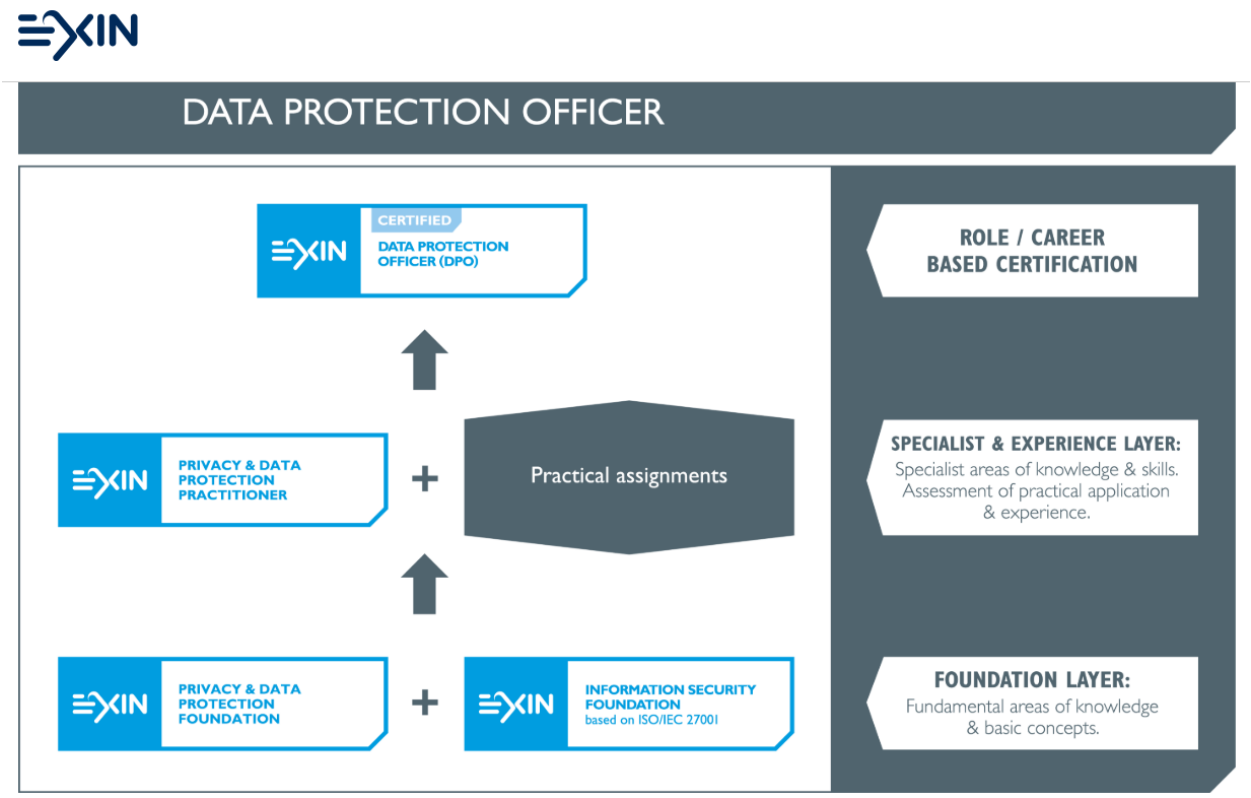
Para completar essa jornada, certificações são fundamentais para profissionais e para empresas. Assim, vamos dedicar um tempinho para olhar alguns roteiros de certificações que recomendo para você que está interessado nessa jornada.

EXIN

· https://www.exin.com/data-protection-officer?language_content_entity=en

A EXIN é um instituto global independente para profissionais de TI que oferece inúmeras certificações importantes para boas práticas e governança de serviços em ambiente corporativo. Um grande conhecido da EXIN é a certificação ITIL - Information Technology Infrastructure Library, que cobre inúmeros cenários de processos para implantação e execução de serviços de TI, suportando o negócio da empresa.

De igual modo, a EXIN possui um roteiro de provas para formação de um DPO – Data Protection Office, que no contexto da LGPD é chamado de ENCARREGADO. A figura a seguir ilustra a sequência de provas esperadas para a formação de um DPO pela EXIN:



· EXIN – PRIVACY & DATA PROTECTION FOUNDATION

· EXIN – INFORMATION SECURITY FOUNDATOIN (baseada na ISO/IEC 27001)

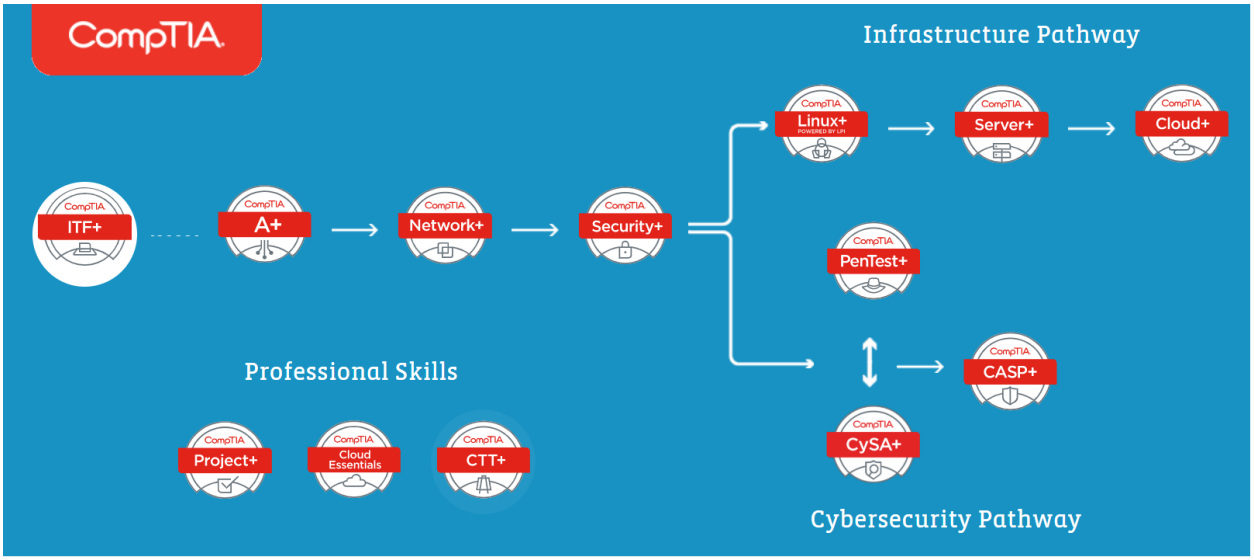
- EXIN – PRIVACY & DATA PROTECTION PRACTITIONER
- EXIN – DATA PROTECTION OFFICER CERTIFIED

O material para cada uma dessas certificações é vasto e exige dedicação e disciplina de estudo. Fica o convite!

COMPTIA

- https://www.comptia.org/pt/certificacoes/security

O **CompTIA Security+** é uma certificação global que valida as habilidades básicas que você precisa para executar as principais funções de segurança e buscar uma carreira de segurança de TI. Pensando no time de segurança da informação diretamente envolvido nos projetos de LGPD, essa certificação oferece um mapa completo sobre ameaças e medidas de mitigação de risco no ambiente de TI, que podem fazer parte dos projetos de implantação da LGPD. Veja a seguir um roadmap de certificações em segurança cibernética:



Como vemos no desenho acima, **CompTIA Security+** é apenas uma de inúmeras certificações para uma carreira de cybersecurity, oferecendo assim um roteiro bastante completo de formação e estudo continuado.

ISO 19600

- http://www.abnt.org.br/noticias/4794-iso-19600

Mais do que nunca, é necessário que as organizações tenham mais transparência em sua gestão, compartilhando processos e fluxos de dados enquanto realizam negócios no mercado brasileiro.

Nesse contexto, a ABNT publicou a **ISO 19600** em português, que fornece orientações para o estabelecimento, desenvolvimento, implementação, avaliação, manutenção e melhoria do sistema de gestão de **Compliance** ou **Conformidades**.

Aplicar as diretrizes da ISO 19600 facilita enormemente a rotina em torno da LGPD nas empresas, sendo assim um material fortemente recomendado.

ISO 27001

- https://www.27001.pt/

A **ISO/IEC 27001** é um padrão para sistema de gestão da segurança da informação *(ISMS - Information Security Management System)* publicado em outubro de 2005 pelo *International Organization for Standardization* e pelo *International Electrotechnical Commission*.

O seu nome completo é **ISO/IEC 27001- Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação** - requisitos, mais conhecido como **ISO 27001**.

Esta norma foi elaborada para oferecer um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um **Sistema de Gestão de Segurança da Informação (SGSI).** A adoção de um SGSI deve ser uma decisão estratégica para uma organização e é bastante importante atualmente, pensando na rotina de projetos em torno da LGPD.

A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização. A seguir, veja alguns benefícios da implantação de ISO 27001 nas empresas:

Empresas certificadas em ISO 27001 são beneficiadas com processos mais estruturados, cobrindo facilmente diversos dispositivos previstos pela LGPD.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

- https://www.cert.br/

Para completar, recomendo visitar o site da CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, que é mantido pelo NIC.BR, do CGI – Comitê Gestor da Internet no Brasil. No site, você irá encontrar vasto material sobre fóruns, publicações, palestras, cursos e estatísticas atualizadas sobre a segurança da informação no Brasil.

Considerações

O artigo de hoje completou a série sobre segurança da informação e LGPD.

Na data de fechamento deste artigo, faltavam 11 meses para a LGPD entrar em vigor.

Vimos que a jornada pode ser longa, por isso, o objetivo da série foi de conscientizar as empresas e profissionais para o início de uma estratégia de segurança e LGPD de forma consistente.

Desde agosto de 2018, tenho encontrado times em diferentes estágios de adoção em relação a LGPD. Algumas empresas já contam com um projeto em fase avançada, possuindo websites revisados, formulários de consentimento ativos, documentação e processos de negócio corrigidos, além de treinamentos regulares sobre políticas de segurança para seus funcionários. Muitas empresas do setor financeiro estão nessa categoria. De igual modo, tenho visto empresas deixando para depois do Carnaval, em muitos casos sem ao menos conhecer o impacto esperado pela nova legislação, o que é um enorme risco para seus negócios.

Desse modo, procurei consolidar diversas fontes de informação e conteúdo sobre LGPD para que o leitor tenha um primeiro contato, assim como um guia inicial sobre o tema. Não foi objetivo do artigo falar exclusivamente sobre o teor e rigor da Lei, mas apenas cobrir alguns tópicos. Recomendo fortemente que consulte o advogado de sua empresa e time jurídico, questionando como está o projeto de LGPD em sua empresa. Se seu advogado não está acompanhando esse tema, recomendo fortemente que o alerte!

No Brasil infelizmente temos o conceito de **“*lei que pega*”** e **“*lei que não pega*”.** De fato, acredito que LGPD irá **“*pegar*”.** 😊 Mesmo que a ANPD não consiga fiscalizar diretamente todas as empresas e transações de negócio em território nacional, as pessoas e a sociedade irão abraçar a LGPD. Fenômeno similar aconteceu com a Lei de Defesa do Consumidor, onde vimos a sociedade pronta para denunciar abusos de conduta nas relações de compra e venda de produtos. Algo semelhante deve acontecer a partir de agosto de 2020, em relação a defesa pela privacidade e proteção para dados pessoais.

Vale lembrar também que a partir do **Direito Civil**, **“ninguém se escusa de cumprir a lei, alegando que não a conhece”**, ou seja, **“a ninguém é dado o direito de alegar desconhecimento da lei”.**

Por isso, é crítico que as empresas no Brasil façam uma reflexão sobre como estão tratando e manipulando **dados pessoais** hoje, fazendo uma autocrítica seguida de um projeto real e prático de adoção de medidas para cumprimento da LGPD. Todas essas medidas deverão constar no **RELATÓRIO DE IMPACTO DA LGPD** como falamos, desde o primeiro dia do projeto, evoluindo de forma regular até agosto de 2020.

A LGPD não é um monstro, mas sim uma oportunidade real de construção de uma cultura de segurança e privacidade responsável no ambiente corporativo.

Espero que tenha gostado do texto e que este possa ajudá-lo nesse importante momento para a construção de um ambiente de negócios mais saudável no Brasil!

Por enquanto é só! Até a próxima!

Waldemir.

Referências

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS (DUDH), DE 1948.

- https://www.direitocom.com/declaracao-universal-dos-direitos-humanos/artigo-12o

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

- https://www.cert.br/

GDPR – GENERAL DATA PROTECTION REGULATION

- https://gdpr-info.eu/

Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Lei de Defesa do Consumidor.

- http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados

- http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

LGPD BRASIL

- https://www.lgpdbrasil.com.br/

LGPD - Lei Geral De Proteção De Dados (Português) Capa Comum – 10 mai 2019 por Viviane Nóbrega Maldonado E Renato Opice Blum (Autor)

- https://www.amazon.com.br/Lgpd-Lei-Geral-Prote%C3%A7%C3%A3o-Dados/dp/8553213935

Use a nuvem inteligente da Microsoft para proteger os direitos individuais de privacidade em conformidade com o RGPD

- https://www.microsoft.com/pt-BR/microsoft-365/blog/2018/05/25/safeguard-individual-privacy-rights-under-gdpr-with-the-microsoft-intelligent-cloud/

Começando a sua jornada em torno da Lei Geral Brasileira de Proteção de Dados Pessoais (LGPD)

- https://www.microsoft.com/pt-br/lgpd

LGPD Na Prática: como implantar a Lei Geral de Proteção de Dados na sua empresa

- https://vanzolini.org.br/cursos/lgpd-na-pratica-como-implantar-lei-geral-de-protecao-de-dados-na-sua-empresa/