Centro Universitário Processus
PORTARIA Nº 282, DE 14 DE ABRIL DE 2022

CURSO DE DIREITO - 3º SEMESTRE

ALINE NUNES COELHO

GUILHERME CARVALHO TEIXEIRA

LUAN BARBOSA SOUZA

MARCOS ALEXANDRE ALVES RODRIGUES

MARIA FRANCISCA CRUZ DE SOUSA

RAYSSA REGINA PASSOS XAVIER

“A IMPORTÂNCIA DA PROTEÇÃO DE DADOS”

ATIVIDADE EXTENSIONISTA

DISCIPLINA: TEORIA GERAL DO DIREITO

ARTICULADORA : LOURIVÂNIA DE LACERDA CASTRO

BRASÍLIA

2023

OBJETIVO GERAL

O objetivo geral deste projeto é informar e esclarecer dúvidas relacionadas à proteção de dados pessoais, conforme estabelecido na Lei nº 13.709 (BRASIL, 2018), também conhecida como Lei Geral de Proteção de Dados (LGPD). O projeto visa promover a conscientização e o entendimento das disposições legais da LGPD, fornecendo informações relevantes e orientações práticas para indivíduos e organizações, a fim de promover o cumprimento efetivo dessa legislação e garantir a proteção adequada dos direitos de privacidade e segurança de dados.

OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste projeto consistem em primeiro lugar, alertar a população sobre os riscos iminentes associados ao vazamento de dados pessoais, enfatizando a ameaça do roubo de identidade, a exposição de informações sensíveis e os potenciais ataques cibernéticos, visando conscientizar as pessoas sobre a importância da segurança de dados. Em segundo lugar, busca-se fornecer orientações detalhadas e práticas para a adoção de medidas eficazes de proteção de dados, abrangendo a criação de senhas seguras, o uso da autenticação de dois fatores, a educação contra ameaças cibernéticas, a análise de políticas de privacidade, a configuração de configurações de privacidade em plataformas digitais, a realização de backups regulares e a manutenção de software atualizado.

METODOLOGIA

A metodologia para a realização do trabalho inclui duas etapas principais: a elaboração da cartilha e a sua entrega na Rodoviária do Plano Piloto em Brasília/DF.

Na primeira etapa, começaremos por realizar uma pesquisa aprofundada sobre as melhores práticas de proteção de dados pessoais e os riscos associados ao vazamento de informações. Essa pesquisa servirá como base para o conteúdo da cartilha, que será elaborado de forma sucinta e acessível, utilizando linguagem simples para garantir a compreensão por parte do público-alvo.

Na segunda etapa, a cartilha será impressa em uma gráfica local em quantidade suficiente para atender à demanda estimada na Rodoviária do Plano Piloto.

JUSTIFICATIVA

Com o aumento do número de usuários e a presença cada vez maior das empresas na internet, a segurança de dados se tornou imprescindível. Diante de ataques cibernéticos e uso indevido de informações de internautas, tornou-se necessário fiscalizar e garantir a navegação segura no ambiente online.

Por isso, a Lei Geral de Proteção de Dados Pessoais do Brasil (BRASIL, 2018) visa assegurar que as empresas e negócios tenham responsabilidade ao manusear e armazenar informações pessoais de terceiros, agindo com mais transparência com o público.

O regulamento precisa ser levado a sério, e muitas empresas se aperfeiçoam diariamente para seguir os requisitos da lei. É muito importante entender o que é a LGPD (BRASIL, 2018), quais requisitos ela propõe e como garantir que seu negócio esteja em conformidade com o código.

CRONOGRAMA

EVENTO	PERÍODO	OBSERVAÇÃO
Apresentação do plano de ensino	07/08/2023	
Definição do grupo de trabalho e tema	14/08/2023	
Elaboração do projeto e cartilha	21/08/2023	Discutido em sala de aula
Ajustes no projeto de acordo com as orientações da articuladora	28/08/2023	Discutido em sala de aula
Finalização da Cartilha e orçamento para confecção	04/09/2023	200 cartilhas
Ajustes finais do projeto	11/09/2023	Discutido em sala de aula
Entrega do projeto	18/09/2023	Encaminhado via e-mail

FUNDAMENTAÇÃO TEÓRICA

O QUE É LGPD

A Lei Geral de Proteção de Dados Pessoais do Brasil (BRASIL, 2018) é o regulamento brasileiro para garantir a segurança de informações pessoais, por meio de diversas normas sobre a coleta, armazenamento, manuseio e compartilhamento de dados, voltadas para empresas e negócios.

A lei foi aprovada em 2018, entrando em vigor em 2020. No início de 2022, foram acrescentadas ainda alguns pontos para pequenas empresas. Os requisitos devem ser seguidos tanto no ambiente online, quanto offline.

Além de dispor regras para o tratamento de dados no Brasil, a LGPD (BRASIL, 2018) também tem aplicação extraterritorial, ou seja, deve ser seguida independente da localização da sede da companhia ou da origem dos dados.

O QUE SÃO DADOS PESSOAIS

A LGPD (BRASIL, 2018) classifica os dados regulados em diversas categorias, incluindo dados pessoais, dados sensíveis, dados anonimizados e dados pseudonimizados. De acordo com o artigo 5º, os dados pessoais são definidos como informações relacionadas a uma pessoa natural identificada ou identificável, abrangendo elementos como nome, sobrenome, CPF, e-mail, endereço, data de nascimento, histórico de compras, dados de localização e identificadores eletrônicos.

Em essência, esses dados são aqueles que podem ser vinculados à identidade de uma pessoa viva, exigindo, portanto, uma proteção mais rigorosa durante seu tratamento, conforme estabelecido na LGPD (BRASIL, 2018).

Além disso, a LGPD (BRASIL, 2018) estipula uma categoria específica conhecida como "dados sensíveis". Esses dados abrangem informações delicadas, como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, bem como informações relacionadas à saúde, vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Essa classificação visa garantir uma

proteção adicional a dados que, se mal utilizados, poderiam resultar em discriminação ou violações graves dos direitos individuais.

Um elemento importante que é considerado dado pessoal, por exemplo, são os famosos cookies. Eles são arquivos pequenos que um site cria ao receber a visita de um usuário, e que permitem identificá-lo, possibilitando personalizar a página e acessar informações sobre o usuário.

QUAIS SÃO AS BASES LEGAIS DA LGPD

O artigo 7º da Lei Geral de Proteção de Dados (BRASIL, 2018) estabelece um arcabouço de princípios e situações em que o tratamento de dados pessoais é permitido, garantindo a proteção dos direitos dos titulares. Essas hipóteses abrangem uma variedade de contextos, desde o consentimento explícito do titular, que é a base fundamental, até situações como o cumprimento de obrigações legais, a realização de estudos por órgãos de pesquisa com a devida anonimização dos dados, e o tratamento necessário para a execução de contratos ou procedimentos preliminares relacionados a contratos nos quais o titular seja parte.

Além disso, o artigo prevê o uso de dados pessoais para garantir a proteção da vida e da integridade física dos titulares, bem como para a tutela da saúde, especialmente quando realizados por profissionais de saúde ou entidades sanitárias. Essas medidas visam assegurar a segurança e o bem-estar das pessoas.

CONSENTIMENTO

O consentimento é uma base legal que prevê que o usuário declare de forma inequívoca que concorda e permite o uso de seus dados pessoais pela empresa. Você deve se deparar com essa base legal frequentemente.

Suponha que você deseja receber um e-book de um determinado negócio, e preencheu um formulário com algumas informações, como e-mail e telefone. A empresa precisa perguntar se você aceita receber e-mails com promoções ou novidades, e se está de acordo com o fato de que ela terá acesso e poderá armazenar suas informações.

LEGÍTIMO INTERESSE

O legítimo interesse é uma base legal que permite o uso dos dados sem precisar do consentimento do usuário, contanto que as ações feitas com essas informações não violem os direitos e liberdades do internauta. O legítimo interesse pode ser usado em situações em que a prestação de serviços beneficiem o titular dos dados.

Para usar a base do legítimo interesse, a companhia precisa fazer um teste de proporcionalidade, que avalia a necessidade do uso dessa base legal, confirmando se a adoção dessa prática é capaz de atender os interesses da empresa e, concomitantemente, respeitar os direitos de seus titulares.

CONTRATO

A base legal de contratos prevê que os dados de uma pessoa podem ser processados para garantir o cumprimento de uma obrigação prevista em contrato, ou quando o uso das informações tem como objetivo validar ou registrar o início de vigência de um acordo.

Isso acontece, por exemplo, quando um colaborador assina um contrato com uma empresa para formalizar a contratação, e, para isso, precisa fornecer alguns dados. solicita que ele forneça uma série de informações pessoais necessárias para formalizar o contrato (dados do contratante, dados para faturamento, etc) que farão parte do futuro contrato de emprego do titular dos dados.

COMO ASSEGURAR O BOM FUNCIONAMENTO DE PRÁTICAS DE LGPD

Como você viu, a LGPD (BRASIL, 2018) é crucial não somente para a proteção de usuários, mas também para garantir a confiabilidade de um negócio, mostrando ao público que o negócio em questão é transparente e incentivando uma relação de confiança entre empresa e cliente.

Por isso, é essencial verificar se a sua empresa está agindo de acordo com os princípios previstos pela LGPD (BRASIL, 2018), sempre colocando em prática ações para assegurar que os procedimentos estão sendo seguidos.

Assim, é interessante ter dentro da companhia um setor ou colaboradores focados na LGPD (BRASIL, 2018), trabalhando para que a empresa fortaleça cada vez mais seus compromissos com a segurança dos usuários e esteja sempre em conformidade com ações que assegurem a transparência.

Profissionais voltados para dados podem mapear de todos os dados disponíveis na sua empresa, identificando riscos na segurança e estipulando ações para impedir ataques ou uso indevido de informações. Além de estar em conformidade com a lei, seu negócio fica muito mais organizado.

Por fim, não se esqueça que a LGPD (BRASIL, 2018) vai muito além de evitar multas ou penalidades: trata-se de trabalhar para garantir um ambiente seguro para todos.

DICAS DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

Uso seguro de credenciais de acesso

- Sempre que disponível, ative a autenticação em duas etapas. A senha é pessoal e intransferível, não a divulgue e nem compartilhe. A senha é sua e de mais ninguém!
- Não escreva sua senha em local público ou de fácil acesso como em papéis, em arquivos sem proteção no computador ou em outro tipo de mídia.
- Cuidado ao digitar a sua senha com alguém por perto, principalmente olhando para o seu teclado. Certifique-se sempre de não estar sendo observado ao digitar a sua senha.
- Feche sua sessão (*logout*) ao acessar sites que requeiram o uso de senhas, principalmente ao usar equipamentos compartilhados.
- Nunca use dados pessoais ou sequências de teclado como senha. Tente criar senhas fortes contendo letras (maiúsculas e minúsculas), números aleatórios e caracteres especiais, de pelo menos 10 (dez) dígitos.
- Evite usar a mesma senha para cadastro e acesso aos sistemas.
- Tente mudar suas senhas regularmente, principalmente se acessar sistemas em dispositivos que são utilizados por várias pessoas.
- Caso desconfie que sua senha tenha sido descoberta, vazada ou usada em um equipamento invadido ou infectado, altere-a imediatamente.
- Use conexões seguras (*https*) quando o acesso a um site, envolver o fornecimento de credenciais de acesso

Proteção do sistema operacional e aplicativos

- Mantenha sempre o sistema operacional e aplicativos instalados no seu equipamento com as atualizações mais recentes.
- Não saia clicando em *links* recebidos por meio de mensagens eletrônicas (SMS, e-mails, redes sociais, etc.). Desconfie sempre!
- Sempre que precisar instalar um novo aplicativo, procure obter de fontes confiáveis, como lojas oficiais ou do site do fabricante. Dê preferência àqueles que tenham sido bem avaliados e com grande quantidade de usuários.
- Use apenas sistemas operacionais e programas originais.

Proteção contra malware

- Configure seu antivírus para procurar por atualizações sempre que seu equipamento estiver conectado à Internet.
- Faça pelo menos uma varredura completa, por semana, em todo o sistema operacional.
- Use seu antivírus em todo arquivo baixado antes de executá-lo, assim como em toda mídia removível conectada.
- Desabilitar a reprodução automática de dispositivos removíveis no sistema operacional.

Cuidados com o uso do correio eletrônico

- Sempre verifique a procedência de e-mails em nome de bancos, provedores de serviços, lojas, órgãos públicos, etc. observando o cabeçalho e o conteúdo completo da mensagem. Nunca saia clicando de imediato em links e anexo da mensagem. Verifique se o remetente é mesmo quem diz ser. Sempre desconfie!
- Caso desconfie de alguma mensagem, consulte o Catálogo de Fraudes da Rede Nacional de Pesquisa (https://catalogodefraudes.rnp.br/) que tem como objetivo conscientizar a comunidade sobre os principais golpes que estão em circulação na internet, identificando e divulgando fraudes reportadas pela comunidade ou coletadas por seus sensores.

- Mesmo que tenha utilizado o antivírus, evite abrir arquivos enviados por fontes não confiáveis.
- Verifique a veracidade das informações e use sempre seu bom senso antes de repassar a mensagem.
- Antes de abrir um arquivo anexado à mensagem tenha certeza de que ele não apresenta riscos, verificando-o com ferramentas antivírus.
- Evite acessar seu webmail em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anônima.

Proteja seus dados pessoais

- Nunca forneça informações sensíveis em sites sem que você tenha solicitado o serviço que o exige, e o faça somente se confiar no site e se o mesmo estiver utilizando criptografia (procure pelo cadeado no navegador e um informativo de certificado digital).
- Evite fazer cadastros em sites de venda desconhecidos pela Internet, especialmente fornecendo seus dados pessoais, pois muitas pequenas e médias empresas possuem pouco ou nenhum tipo de segurança para armazenar e proteger seus dados.
- Cuidado ao disponibilizar informações muito pessoais em sites de relacionamento (telefones móveis, endereços residenciais etc).

Cópias de segurança (backup)

- Agende regularmente cópias de segurança de todos os seus dados importantes.
- Tenha sempre mais de uma cópia de segurança, mantendo-as, preferencialmente, em locais diferentes. Uma boa opção é ter uma cópia de segurança em serviços de armazenamento em nuvem (escolha serviços de nuvem confiáveis e habilite a verificação em duas etapas sempre que possível).
- Lembre-se: discos rígidos, pendrives, hd's externos e outras mídias dão defeito. Tenha sempre cópias redundantes.

- Para a proteção dos arquivos sensíveis, grave-os já criptografados, de forma que seja exigido uma senha para acessá-los.

  Mantenha sempre as mídias de backups em local protegido.
- Faça cópias de segurança sempre que houver indícios de risco iminente (Exemplo: mau funcionamento do equipamento, alerta de falhas, envio do equipamento a serviços de manutenção, etc.).
- Cuidado ao descartar as mídias. Se os arquivos não estiverem criptografados, alguém pode tentar acessá-los.

CONSIDERAÇÕES FINAIS

Os dados pessoais, conforme definidos pela Lei Geral de Proteção de Dados (LGPD), abrangem informações relacionadas a pessoas naturais identificadas ou identificáveis e englobam uma variedade de elementos, como nomes, CPFs, e-mails, endereços e históricos de compras. Esses dados, por sua natureza, exigem uma proteção mais rigorosa durante seu tratamento. Além disso, a legislação reconhece a categoria de "dados sensíveis," que engloba informações delicadas, como origem racial ou étnica, convicção religiosa, opinião política e saúde, entre outras, exigindo uma proteção adicional devido ao potencial risco de discriminação e violações dos direitos individuais.

A LGPD estabelece bases legais claras para o tratamento de dados pessoais, incluindo o consentimento do titular, o cumprimento de obrigações legais, o uso para fins de pesquisa, a execução de contratos e a proteção da vida, saúde e crédito, entre outros. Essas bases visam equilibrar a necessidade de proteger os direitos dos titulares de dados com as necessidades legítimas das organizações.

É crucial para as empresas compreenderem e adotarem essas bases legais de acordo com a LGPD, garantindo que o tratamento de dados seja realizado de forma ética e legal. Isso envolve a implementação de práticas de proteção de dados, como a obtenção adequada de consentimento, a consideração dos interesses legítimos e a conformidade com os requisitos contratuais. A LGPD não apenas visa evitar multas ou penalidades, mas também promove a confiabilidade dos negócios e estabelece relações de confiança com os clientes.

Além disso, para assegurar o bom funcionamento, é fundamental que as empresas tenham profissionais dedicados à proteção de dados, que possam mapear os dados disponíveis, identificar riscos na segurança e implementar

medidas para prevenir ataques ou uso indevido de informações. Isso não apenas mantém a conformidade legal, mas também organiza o negócio e fortalece sua reputação.

Finalmente, a segurança da informação e a proteção de dados pessoais são fundamentais no ambiente digital atual. É essencial que os usuários adotem medidas de segurança, como senhas fortes, autenticação em duas etapas e cuidado ao compartilhar informações sensíveis. A conscientização e a prática de hábitos seguros de navegação ajudam a proteger tanto os dados pessoais quanto a integridade online.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei nº 13.709,** de 4 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2023.

Dicas de Segurança da Informação e Proteção de Dados Pessoais. **Instituto Federal do Sudeste de Minas Gerais**. Disponível em: <https://www.ifsudestemg.edu.br/hotsites/processo-seletivo-2024-1/capa/index.html/acessoainformacao/protecao-de-dados-pessoais-no-if-sudeste-mg/dicas>. Acesso em: 11 de set. de 2023.

Ouvidoria ANPD. **Autoridade Nacional de Proteção De Dados** . Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/ouvidoria>. Acesso em: 08 de set. de 2023.