Como implementar a LGPD na prática em 2021: 20 passos essenciais para adequação de empresas e negócios

Implantar a LGPD não se resume em criar uma "Política de Privacidade"!

A Lei Geral de Proteção de Dados (Lei nº 13.709/18) já está em vigor desde setembro de 2020, trazendo direitos aos titulares de dados pessoais e deveres aos agentes de tratamento, sejam controladores ou operadores de dados pessoais.

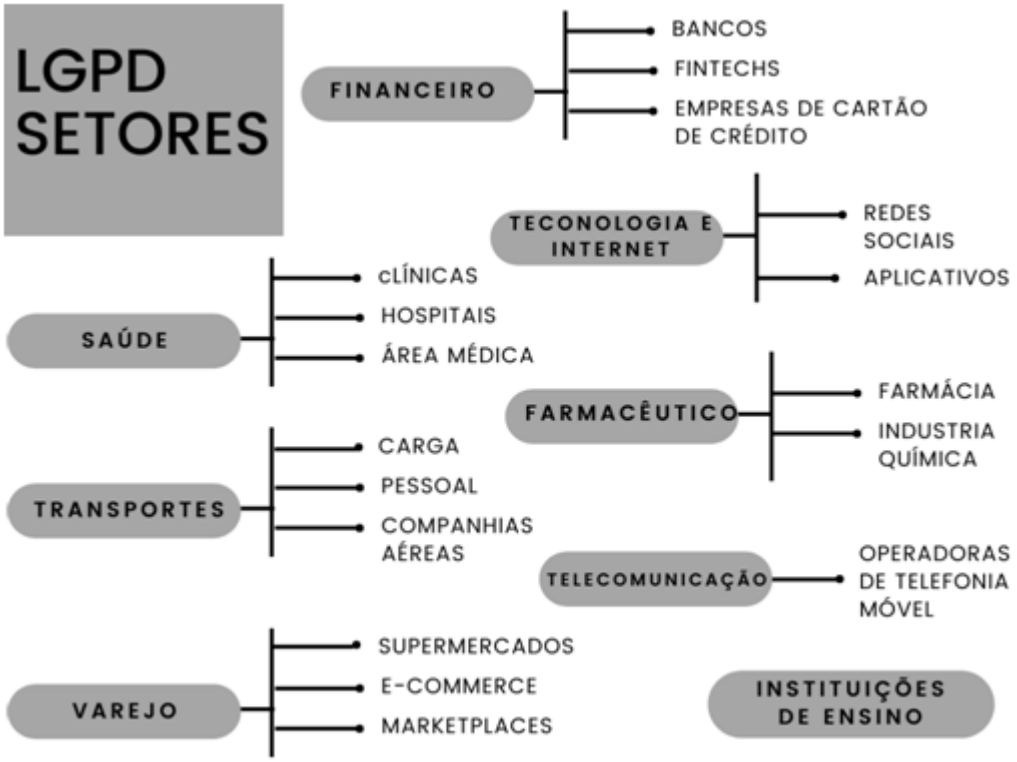
Como estamos discorrendo de uma norma pendente de diversas regulamentações e fixações de posicionamentos por parte da Autoridade Nacional de Proteção de Dados (ANPD), muitos subjetivismos são considerados quando o tema é afirmar que se está em conformidade com a Lei, bem como quais os meios para que isso aconteça.

Porém, ao contrário do que parece, adequar-se à LGPD é muito mais do que mudar a política de privacidade da empresa. Envolve o desenvolvimento da cultura da privacidade nos processos corporativos, um programa de governança que trate de um sistema de gestão da privacidade da informação, com revisões de posturas, ações e processos.

É notório que empresas dos mais variados setores devem comprovar adequação à norma, sobretudo porque o tratamento de

dados pessoais, hoje, é realidade nos negócios. Assim, preparamos 20 passos de adequação que auxiliarão empresas e negócios no processo de conformidade.

A adequação à LGPD deve ocorrer em diversos setores, incluindo, mas não se limitando a:



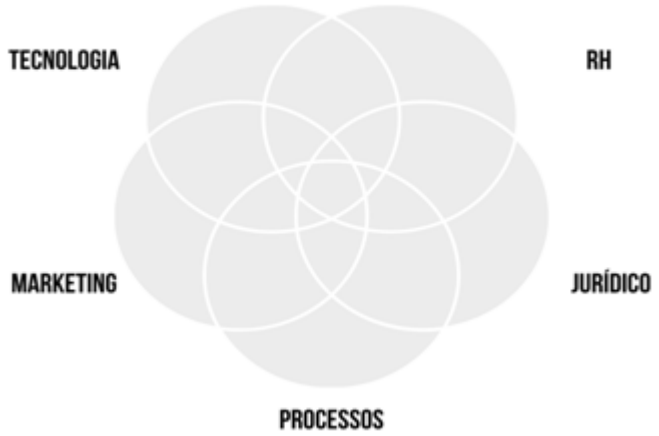
Conquanto alguns segmentos, naturalmente, em decorrência de suas atividades, acabam por tratar mais dados sensíveis e tenham processos mais críticos, nenhuma empresa deve ignorar a Lei, considerando ainda que as punições começam a ser aplicadas em agosto de 2021.

1. **Quais áreas envolver?**

Como visto, da mesma forma que a LGPD não é apenas uma

Política de Privacidade, também não é somente uma revisão de regras do *firewall*, criptografia da base de dados ou implantação de permissionamentos de acesso ou política de mesa limpa.

É preciso deixar claro que a adequação da LGPD envolve inúmeras competências, ligadas comumente às áreas de tecnologia, como segurança da informação, jurídico, compliance e time de processos ou projetos. Além disso, é o conjunto de ações, melhores práticas e processos que indicarão a maturidade do seu negócio em proteção de dados pessoais, e não apenas uma ação isolada de uma área específica da empresa.



Neste sentido, um processo de adequação deve considerar o apoio de todas as áreas e *keyusers,* que são definidos como peças-chave no projeto de adequação.

2. **Realize a reunião de *Kick-Off* e crie o Comitê de Proteção de Dados**

O início do projeto de adequação envolve a apresentação da

equipe que será responsável pelos esforços.

Neste momento, é importante a participação de todos que serão canalizadores do projeto junto aos setores e áreas do negócio e que atuarão no *Assessment* inicial, ou seja, a fase em que se avaliará a empresa ou a instituição no que diz respeito à sua maturidade de controles envolvendo proteção de dados.

Na reunião, é apresentado como funcionará o programa, cronogramas, as próximas etapas e uma estimativa de esforço inicial para que as equipes se planejem (esta estimativa pode modificar-se após a avaliação).

Assim, é formalizada a abertura do projeto. Uma exposição é feita com os colaboradores para a conscientização sobre o projeto que se inicia. Além disso, dos *keyusers* poderá sair os nomes das pessoas que integrarão o comitê de proteção de dados na empresa, que se recomenda seja constituído logo no início do projeto.

3. **Tenha em mente as macrofases do projeto**

As macrofases são: ***preparação, organização, implementação, governança, e avaliação e melhoria.***

Na preparação, a empresa é avaliada e a estrutura organizacional inicial é formada para a criação de um programa de proteção de dados.

Na organização, são estabelecidas as estruturas

organizacionais, planos de ação e os mecanismos necessários para suportar a privacidade e proteção de dados.

Na fase de implementação, os processos, medidas técnicas e organizativas entram em prática, aqui se inclui *privacyby design*, pseudonimização, anonimização, criptografia, controles de acesso, controles na contratação, segurança da cadeia de suprimentos, segurança física, novas políticas, novos aditivos, ativação de processos e capacitação/conscientização.

Na fase de governança, irá gerenciar aspectos do programa de proteção de dados, requerimentos dos titulares, gerenciará incidentes com dados, a avaliação, análise e gerenciamento de riscos, dentre outras ações.

E, por fim, na fase de avaliação e melhoria, a empresa revisará continuamente os controles e fiscalizará a manutenção do programa nas diversas áreas da empresa.

4. **Conduza o *Assessment* Inicial**

O *Assessment* Inicial é essencial e insumo para outras fases do processo de adequação, como o *mapping* dos dados e o registro das operações de processamento.

Nesta fase, os *keyusers*, tanto da consultoria LGPD como da empresa, irão avaliar *"in locu",* mediante respostas de áreas e acessos nos aplicativos e áreas virtuais, as questões envolvendo as políticas, ações e controles existentes.

O objetivo da avaliação é analisar os regulamentos aplicados à empresa, identificando o impacto da privacidade no negócio, bem como entender quais são os dados pessoais tratados e o ciclo de vida deles, isto é, a forma de coleta, armazenamento, classificação e descarte.

5. ***Mapping*** **e Inventário dos dados**

A partir do *Assessment*, fase intimamente ligada, ainda, na macrofase de preparação é realizado o mapeamento e o inventário de dados.

Data mapping ou mapeamento de dados é uma atividade de catalogação de todo o fluxo de dados pessoais que são objeto de qualquer operação de tratamento. O mapping pode ser mantido em sistemas eletrônicos, visto que facilita a tomada de decisões e a manutenção de registros.

Lembrando que o mapeamento de dados será um organismo vivo e deverá ser mantido sempre pela organização para cada novo ciclo de vida ou processo que faça o tratamento de dados pessoais.

Junto ao *data mapping*, é importante manter o inventário de dados que objetiva entender com detalhes a variedade dos dados tratados na empresa e categorizá-los, mensurar os riscos existentes e seus impactos, e servir como base para elaborar planos de ação mais direcionados e efetivos. É algo mais técnico, relacionado à granularidade de estruturas de campos.

Templates de Mapping podem ser encontrados

em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

6. ***Gap Analysis***

A minha experiência em adequação de grandes varejos e redes sociais tem demonstrado que o *mapping*, se a estimativa de esforço não for bem direcionada, é uma das etapas mais demoradas do processo de adequação. Isso se deve também ao fato de que diversos times, de outras inúmeras áreas de negócios, devem ser acionados para auxiliar o processo.

No entanto, quando adequadamente realizado, pode expor severas deficiências na empresa, como tratamentos irregulares, vulnerabilidades, bases legais equivocadas, ausência de definições claras quanto à retenção de dados, dentre outros riscos.

Neste momento, pós mapping, realizamos um relatório de *Gaps*, que são importantes insumos para os próximos passos, como o plano de ação e implementação.

7. **Programa de proteção de dados e plano de ação**

Na fase de preparação, também é importante a concepção do programa de proteção de dados.

Embora seja um conjunto de ações e práticas, recomendo sempre a documentação dele, constantemente revista, bem como a

criação de um plano de ação com metas de implementação e ajustes. A empresa precisará definir:

- Periodicidade do ***Status Report*** do projeto;
- Como será o processo e sistemas que suportarão o armazenamento da documentação relativa à conformidade;
- Um plano de conscientização que preveja recorrência, ações, comumente prevendo atividades durante o ano;
- Um planejamento de ações "vivas" que serão mantidas e deverão ser atualizadas pós-consultoria.

Documentamos estes itens, para que fiquem claros para os responsáveis pelo Comitê de Proteção de Dados e neste sentido eles terão um plano de ação definido.

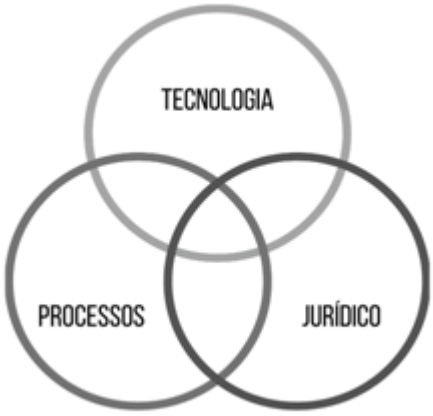
8. **Matriz de responsabilidades**

Já na fase de organização, é muito importante o estabelecimento da matriz de responsabilidades pela proteção de dados e privacidade. Nesta fase, também se define como manter os programas, as políticas e os controles de proteção de dados, além de definir e implementar como será mantido o envolvimento dos níveis táticos, operacionais e estratégicos da empresa.

9. **Estabeleça o *Data Protection Officer* (DPO)**

Na fase de organização é que estabeleceremos também o encarregado de proteção de dados, conhecido como Data Protection Officer (DPO), que desempenhará, dentre algumas atividades:

Mais uma vez, aqui, sobre as competências do DPO, entendo que este deva ter conhecimentos complementares, incluindo, mas não se limitando a conhecimento das áreas tecnologia, processos e jurídico:



10. **Estabelecimento dos processos**

É preciso criar, estabelecer e realizar a manutenção dos processos e procedimentos que garantam que as pessoas estão atuando nas melhores práticas de proteção de dados.

Assim, a elaboração de um plano de comunicação das ações, mudanças, novos ou atualização de processos existentes para considerar dados pessoais como “contratação de fornecedores”, “admissão”, “avaliação de riscos a privacidade”, planos de treinamentos, dentre outros, devem ser alinhados neste momento, não só com a criação de processos com fluxos claros, mas com o preparo dos profissionais que atuarão nas áreas e manterão estes “organismos vivos”. É importante integrar as ações de proteção de dados pessoais no dia a dia corporativo.

11. **Políticas de Privacidade, Proteção de Dados e Contratos**

Já na fase de implementação, um item atinente ao jurídico/compliance diz respeito à política de privacidade e proteção de dados pessoais.

A política de privacidade é um documento externo, destinado ao público em geral. O seu objetivo é regulamentar o comprometimento da empresa em relação à proteção de dados pessoais, e deixar claro como realiza o tratamento dos mesmos.

É de boa prática que a partir da política de privacidade, estabelecem-se também tabelas e matrizes sobre dados tratados, finalidade e base legal.

Além disso, é importante destacar o contato com o encarregado de proteção de dados, para que o titular possa enviar

requerimentos e sanar dúvidas em relação à proteção de dados.

Por sua vez, a política de proteção de dados é um documento interno, destinado à empresa, colaboradores, terceiros, e demais envolvidos no processo de tratamento de dados.

Trata-se de uma política que poderá ser regulamentada ou estratificada em outras normas e procedimentos. As normas estão relacionadas às regras básicas do que deve ser feito para observar determinado controle definido na política da organização. Já os procedimentos, detalham como deve ser implantado o controle.

Esta política prevê o que a empresa espera de profissionais e prestadores, inclusive prevendo sansões por descumprimento.

A política de privacidade e política de proteção de dados pessoais demonstram a transparência da empresa quando do tratamento de dados pessoais, observando o princípio da transparência, nos termos do art. 6º, VI, da LGPD.

Além disso, é importante a revisão jurídica dos contratos para que prevejam cláusulas que estabeleçam os deveres em relação ao tratamento de dados pessoais.

O esforço jurídico, neste momento, comumente se dá na elaboração de:

- Aditivos contratuais;
- *Data Processing Agreements;*
- Termos de comprometimento das empresas com a Política de Proteção de Dados.

12. **Processo para aprovação de tratamento de dados pessoais**

Qualquer nova operação, lançamento, *feature*, tela, sistema, ação, produto na empresa e que envolva o tratamento de dados pessoais deverá passar por um processo para análise e aprovação.

Comumente, este processo conduzirá os demandantes a necessidade de um Relatório de Impacto a Proteção de Dados (RIPD) ou não, de acordo com o que for identificado e critérios que devem ser transmitidos ao Comitê de Proteção de Dados.

Caso a empresa tenha decidido realizar o tratamento de dados, esta deverá seguir outro processo, o de privacidade por design. Pode ser necessário, neste aspecto, revisar bases legais ou revalidar consentimentos para tratamento de dados. Alguns itens e questionamentos revistos no conceito de privacidade por design de um novo serviço/processo/operação envolvem:

- É possível anonimizar os dados?
- É possível realizar o processo ou atingir as finalidades com menos dados pessoais?
- Quais técnicas de pseudonimização e criptografia disponíveis?
- O controle de acesso aos dados foi revisto?
- Revisão de interface para ativação de opções de privacidade por padrão;
- Como garantir os direitos dos titulares?

13. **Implementação de medidas técnicas e organizativas**

Na macrofase de implementação, inicia-se a adoção de medidas técnicas e organizativas para proteção de dados.

Como medidas organizativas, podemos citar, por exemplo, a classificação da informação, políticas e conscientização. Já as medidas técnicas envolvem controles, implementações e ações destinadas ao atendimento de diretrizes de segurança da informação aplicáveis aos dados, como criptografia, sistemas de proteção de dados, logging das atividades, dentre outros.

Recomenda-se, nesta fase, observar os requisitos e as diretrizes da norma ABNT ISO 27701 (Sistema de Gestão da

Privacidade da Informação), sobretudo, os requisitos e as diretrizes adicionais para controladores e processadores de dados.

A empresa não precisará implementar todos os controles, mas deverá selecionar adequadamente os necessários para proteção da sua atividade justificando a seleção. *Backups*, anonimização, registros de eventos, logs, revisões de minimização são executadas nesta fase.

14. **Execute o plano de treinamento**

A capacitação é uma boa prática e faz parte de um programa de proteção de dados. Ela envolve conteúdos direcionados às áreas específicas e insere elementos de conscientização para riscos envolvendo o tratamento de dados pessoais, levando em conta as atividades dos prestadores, colaboradores e terceiros. São ações comuns “ataques simulados”, treinamentos, cartazes, quizzes, questionários e outras formas de aumento da consciência sobre ameaças cibernéticas. Lembrando que “ações educativas” são previstas com boas práticas de governança no art. 50 da LGPD.

15. **Processo para recebimento de solicitações e resposta a titulares**

Esse é um dos passos prioritários de adequação. A empresa precisa disponibilizar para os titulares de dados um canal de contato para que possam realizar requerimentos e solicitações relativas a seus direitos previstos na norma.

Os direitos dos titulares de dados estão previstos no art. 18 da LGPD, que também assegura o direito de peticionar em face do controlador de dados pessoais, para exercitar os referidos direitos:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou

V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII – informação das entidades públicas e privadas com as

quais o controlador realizou uso compartilhado de dados;

VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

- 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
- 2º O titular pode opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
- 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

Importante destacar que este requerimento será exercido sem custo algum ao titular de dados pessoais, nos prazos e termos que serão previstos em regulamento. A boa prática recomenda, inclusive, que o titular sempre seja informado do prazo para atendimento a sua solicitação.

Conforme previsto na LGPD, a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular em formato simplificado, imediatamente; ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os

segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. A Legislação prevê, ainda, que os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

Neste contexto, é importante que a empresa entenda que não basta um formulário de contato ou um ajuste no SAC, mas efetivamente um processo interno que trate os requerimentos envolvendo dados pessoais, com papéis e responsabilidades definidas.

Nem sempre a empresa poderá atender os requerimentos dos titulares, mas é importante que esteja preparada, com uma boa fundamentação legal para explicar os motivos e que jamais deixe os requerimentos sem resposta.

É de suma importância manter os registros de todas as solicitações. A boa prática também vem prevista no controle A.7.3.9 da ISO 27701, destinado aos controladores, estabelecendo-se que *"A organização deve definir e documentar políticas e procedimentos para tratamento e respostas, a solicitações legítimas dos titulares de dados pessoais".*

16. **Plano de resposta a incidentes**

Do mesmo modo, é importante já na macrofase de governança, que o agente de tratamento de dados pessoais estabeleça um plano e processo de resposta a incidentes envolvendo dados pessoais.

Este poderá estar integrado ao processo já praticado pelo time

de resposta a incidentes de segurança da informação, caso o processo já exista.

Um processo claro de como saber o que fazer e como agir diante de incidentes que comprometam dados pessoais é fundamental, até mesmo porque a LGPD estabelece em seu art. 48 que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Neste aspecto, cumpre destacar a Diretriz 6.13 da norma ISO 27701 que dispõe, dentre outros pontos que:

1. a) Convém que a empresa estabeleça responsabilidades e procedimentos para identificação e registro de violações de dados pessoais;
2. b) Procedimentos relativos à notificação para as partes envolvidas e autoridades, considerando a legislação;
3. c) Realize uma análise crítica, como parte de um processo de gestão da segurança da informação, para avaliar se medidas foram tomadas adequadamente.

Assim, a comunicação aos envolvidos e à Autoridade Nacional de Proteção de Dados (ANPD) deverá se dar nos moldes do art. 48 da LGPD e prever:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;

- os motivos da demora, no caso de a comunicação não ter sido imediata; e
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Vale mencionar que cláusulas que cubram a notificação de violação de dados pessoais sejam previstas para operadores de dados pessoais, a fim de que estes deem ciência aos controladores tão logo constatem um incidente.

Em todos os casos, é importante observar o controle 6.13.1.7 da ISO 27701, com o estabelecimento de um processo para coleta de evidências em casos envolvendo incidentes com dados pessoais.

17. **Auditoria de risco e maturidade em proteção de dados**

Nesta fase, é relevante conduzir uma auditoria independente envolvendo a implantação dos processos e a maturidade do sistema. É preciso olhar para o mercado, verificar o que os concorrentes estão implantando, priorizando, como a Autoridade de Proteção de Dados está agindo, avaliar o *baseline* do início do projeto e verificar o que, de fato, está implementado e funcionando desde então.

Aqui, a auditoria tem a função de avaliar o estágio de adequação e os riscos residuais. Para condução dela, alguns *frameworks* podem ser utilizados, como o *Privacy Maturity Model.* : *https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf*

18. **Mantenha a documentação de privacidade organizada e atualize os termos**

Um dos princípios previstos na LGPD é o da responsabilização e prestação de contas, que prevê a demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Neste sentido, todas as ações aqui trazidas, que podem conduzir a empresa para a conformidade, precisam ser gravadas, registradas, testadas e sua documentação organizada.

Além disso, o sistema de gestão da proteção de dados é um organismo vivo, com constantes atualizações, o que demandarão a revisão e custódia constante de registros e documentos relativos. *Softwares* de gestão de documentos, consentimento, logging, gestão de versão de políticas, dentre outros, podem auxiliar nestas atividades. Também, algumas suítes de sistemas de gestão da proteção de dados já centralizam a gestão dos documentos, o que pode facilitar.

19. **Monitorar o sistema, Leis e relatar as desconformidades**

Como visto, um sistema de gestão da privacidade da informação é algo vivo, ativo, em constante atualização. Documentos, práticas e ações devem ser revistos constante e periodicamente.

O DPO, com apoio do Comitê Interno de Proteção de Dados, tem esta tarefa de coordenar as atualizações, monitorar o sistema,

acompanhar a evolução de entendimentos, legislativa e regulatória e zelar para que os processos internos estejam em conformidade, relatando desconformidades e adotando medidas para adequação, no âmbito de suas competências.

Análises críticas e técnicas de compliance são práticas previstas no controle 6.15.2.4 da ISO 27701 e envolvem, inclusive, monitoramentos contínuos e testes específicos de vulnerabilidade e invasão, como os *pentests*, ou testes de reversão de anonimização, técnicas que também são consideradas boas práticas para "se comprovar" a segurança de sistemas que tratam dados pessoais, tendo-se em mente que nos termos da LGPD, tratamento irregular não é só aquele que deixa de observar a legislação, mas que não fornece a segurança que o titular dele poderia esperar.

20. **Atue nas prioridades enquanto desenvolve as outras frentes!**

Alguns itens são considerados prioritários no processo de adequação. Significa dizer que enquanto a empresa avança nas fases-macro, pode ter um olhar especial para estes itens, considerados prioritários. Dentre as prioridades estão:

- constituição do comitê de proteção de dados;
- nomeação de um DPO;
- estabelecimento do plano de ação e programa de proteção e dados;
- criação do processo e área para requerimentos do titular;
- revisão das políticas de privacidade;
- avaliação inicial de segurança.

Outras atividades ainda podem ser listadas como prioritárias, de acordo com contexto e atividades de tratamento. Seja como for, é importante avançar nas ações de adequação,considerando que a Lei já está em vigor e as penalidades podem ser aplicadas a partir de agosto 2021.

Conclusões

Como visto, negligenciar a adequação do negócio à LGPD pode ser um erro e irá interferir nas negociações realizadas, visto que os produtos e serviços deverão ostentar um padrão de segurança e proteção de dados esperados. Além disso, com o avanço da tecnologia, amplificam-se os riscos e elevam-se as preocupações quanto a encontrar soluções de segurança adequadas.

Porém, seguindo as ações descritas neste guia, é possível avançar rumo à conformidade, realizando as ações necessárias e que atendem boa parte dos requisitos legais, com economia e eficiência.

O presente artigo elenca 20 passos que, se adotados, cobrem, significativamente, parte das ações ligadas ao processo de adequação.

Adequar-se é necessário. A adequação à LGPD não deve ser encarada somente como um rito obrigatório, mas como uma oportunidade de inovação e mudança de cultura, a fim de elevar o padrão da empresa, gerando valores sólidos voltados à proteção de dados pessoais.

Canvas compliance model

Elaboramos um mapa em formato Canvas, que traz um modelo mental de questões que a empresa deve fazer, e com isso, não negligenciar nenhuma ação necessária para que siga nas fases da adequação, descritas no mapa. O modelo auxilia empresas a seguirem uma sucessão ordenada de atos para a correta implementação. Para requerer o seu se inscreva no canal @josemilagre e conecte-se conosco. Acesse também nosso grupo de DPOs no Facebook https://www.facebook.com/groups/lgpdbrasil/

Como implementar a LGPD? CyberExperts Consultoria

A CyberExperts Consultoria é referência em projetos de adequação de negócios à LGPD, bem como na implementação de Sistemas de Gestão de Proteção de Dados, em conformidade com a ISSO 27701. Também oferecemos programas de conscientização e capacitação para empresas e órgãos públicos. O PrivacyOfficer é um programa de DPO *as a service*, para auxiliar negócios e agentes de tratamento nas questões envolvendo proteção de dados.

Solicite uma apresentação gratuita sobre a adequação LGPD aplicável ao seu negócio, ou conheça nossos treinamentos na área de proteção de dados: Acesse: www.cyberexperts.com.br

Sobre o autor: **José Antonio Milagre** (https://app.exeed.pro/holder/badge/55319) Data Protection Officer (DPO) EXIN. Pesquisador em direito e dados do Núcleo de Estudos em Web Semântica e Análise de Dados da USP (Universidade de São Paulo), Mestre e Doutorando em

Ciência da Informação pela UNESP, Pós Graduado em Gestão de Tecnologia da Informação, Advogado com atuação em Direito Digital, Perito Judicial em Informática e Proteção de Dados. Presidente da Comissão de Direito Digital da Regional da Vila Prudente da OAB/SP Autor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários a Lei 12.975/2014 e Manual de Crimes Informáticos).

Algumas participações na imprensa:

https://www1.folha.uol.com.br/cotidiano/2018/07/comissao-da-camara-aprova-juizado-especial-para-crime-cibernetico.shtml

https://oglobo.globo.com/economia/tecnologia/como-voce-era-ha-10-anos-brincadeira-no-facebook-pode-trazer-riscos-sua-privacidade-23377262

https://cio.com.br/quando-os-algoritmos-falham-e-o-combate-as-fakenews-causa-outros-danos/

Colaboradora: **Laura Secfém Rodrigues**. Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law.Graduada em Direito pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE).

Home Office causa aumento de crimes digitais no Brasil

Com a pandemia muitas empresas migraram de seus ambientes corporativos para os chamados Home Office, ou Teletrabalho, no entanto, esta nova realidade trás vulnerabilidade aos dados empresariais que ficam a mercê dos criminosos.

Saiba os detalhes para proteger sua empresa acessando: https://www.gazetasp.com.br/brasil/2020/12/1080963-brasil-sofreu-mais-de-34-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2020.html

---

Vendas pela internet podem facilitar fraudes na Black Friday; veja como evitar

Você costuma fazer compras pela internet? Sabe como conferir a autenticidade dos sites? Como se proteger para não cair em golpes? O Especialista em Direito Digital e Crimes cibernéticos, José Antonio Milagre, fala sobre os cuidados que devem ser adotados durante as compras e o cenário atrativo para os criminosos durante o período de grandes descontos, como a Black Fryday.

Saiba mais em: https://jovempan.com.br/noticias/brasil/vendas-pela-internet-podem-facilitar-fraudes-na-black-friday-veja-como-evitar.html

---

O novo sistema de transferência bancária está dando o que falar! Já cadastrou a sua chave Pix? O Especialista, José Milagre da dicas para faze-lo com tranquilidade

O Especialista em Crimes Digitais e Perito em Informática falou ao Gazeta do Povo sobre o novo sistema de transferência bancário, o Pix, você já está por dentro desta nova tecnologia? O Especialista fala sobre a segurança da ferramenta e como se proteger dos golpes que podem surgir.

Para saber mais detalhes acesse: https://www.gazetadopovo.com.br/economia/chave-pix-armadilhas-no-uso-de-dados/

Como os “hackers” agiram no ataque ao Superior Tribunal de Justiça do Brasil?

Investigação, lições e como se proteger do ransomware

*José Antonio Milagre**

Um dos maiores ataques cibernéticos do país indisponibilizou serviços do Superior Tribunal de Justiça Brasileiro (STJ). Estima-se que o Ministério da Saúde também tenha sido atingido. Após ter dados críticos criptografados, os técnicos da corte encontraram um pedido de resgate.

Ao que identificado, o STJ foi vitimado por uma ameaça conhecidíssima, nada de “alta tecnologia”, mas um ataque de ransomware, “sequestro de dados”, códigos automatizados que ao infectarem máquinas, criptografam arquivos com diversas extensões, ou mesmo cifram o disco todo, exigindo o pagamento em bitcoins.

No caso do STJ, o ataque criptografou os arquivos, renomeando as extensões, aparentemente, para *. Sth888. Como prova de que podem reverter o conteúdo, pedem que a vítima envie qualquer arquivo menor que 900 KB e devolverão descriptografados.

Assim, bases de dados críticas, sistemas, servidores web e softwares são paralisados, causando indisponibilidade de serviços e grandes transtornos. No caso, até audiências foram paralisadas. Trata-se de uma ameaça onde o que não se falta são medidas "preventivas" para evitar que criminosos tenham sucesso com o golpe digital. (Já tratei inclusive deste tema no meu canal em: *Ransomware: Como evitar, remover, descriptografar e descobrir como foi infectado? 2020 José Milagre* https://www.youtube.com/watch?v=EPJwP1rRsq8).

Muitos poderiam pensar que um Tribunal estruturado e com um grande orçamento, jamais seria vítima de uma ameaça tão conhecida, para qual existem recursos preventivos diversos. Porém, a invasão ao STJ e a outros órgãos públicos nos faz refletir sobre alguns pontos:

a) Não importa o quão a empresa invista em infra-estrutura em seu ambiente, na nova forma de trabalho, home office, a vulnerabilidade pode estar no elo mais fraco da corrente, ou seja, as máquinas vulneráveis dos trabalhadores, que acessam a VPN ou rede da empresa;

b) Até mesmo ameaças conhecidas, se não tratadas com medidas técnicas e organizativas, podem impactar grandemente em dados e na disponibilidade de sistemas; Um exemplo de boa prática é a adoção de backups e o estabelecimento de um *disaster recovery plan*.

c) Uma estrutura de resposta a incidentes jamais será eficaz se não estiver formalmente constituída e preparada com antecedência, com processos claros para compreensão do incidente, se evolve dados pessoais ou se há a necessidade da perícia em informática, para que se possa identificar e apurar

o modus operandi e a possível autoria.

Os criminosos podem responder, de acordo com a situação, dentre outros delitos, por invasão de dispositivo informático e também pelo delito de interrupção ou perturbação de serviço informático, ou de informação de utilidade pública, crimes previstos no Código Penal Brasileiro e Lei 12.737/2012 (Carolina Dieckman).

No entanto, no caso do ataque de ransomware, tão dificultoso quanto descriptografar os dados sem a chave de reversão (o que demandaria muito poder de processamento, diante da complexidade dos algoritmos), é a apuração da autoria ou dos responsáveis. A perícia digital e em informática lidará com origem incerta, além da dificuldade de apurar a conta de destino do resgate, considerando que os criminosos recebem em criptomoedas e as transações na Blockchain podem não indicar muito sobre o recebedor.

Importante destacar, igualmente, que de acordo com a Lei Geral de Proteção de Dados, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, ou ilícito.

Mais que isso, deverão comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, em prazo razoável, indicando a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para

a proteção dos dados, observados os segredos comercial e industrial, os riscos relacionados ao incidente e as medidas que foram ou que serão adotadas para reverter, ou mitigar os efeitos do prejuízo.

Logo, é dever do órgão apurar se existiu ofensa a dados pessoais e ser transparente a respeito, nos termos da legislação nacional de proteção de dados.

Ferramentas e kits que permitem que qualquer pessoa aplique o ransomware e se torne um criminoso, com alguns cliques, são facilmente encontradas na rede. Pacotes efetivos e "atualizados" são vendidos na deep web, inclusive com disparos de e-mails "*pishing*" e outras formas mais sofisticadas de infecção, como o carregamento do código a partir do navegador, com o acesso a um site infectado. Em sentido oposto, as técnicas de perícia em informática para rastreio da Blockchain em busca do destino do dinheiro produto de crime engatinham e as transações em criptomoedas para fins ilícitos constituem um grande desafio para peritos de informática e investigadores digitais.

Deste modo, o ransomware, conquanto ameaça conhecida, continua em alta e muito efetiva, lesando de pequenos empresários e grandes cortes, sobretudo diante dos descuidos com proteção de dados e cópias de segurança, e como visto, a prevenção continua sendo a melhor forma de proteção contra este problema.

Prof. MSc. José Antonio Milagre, é perito em informática, advogado especialista em crimes cibernéticos e direito digital, Mestre e Doutorando em Ciência da Informação pela UNESP, Pesquisador do Nucleo de Estudos em Web Semântica e

Análise de dados – NEWSDA-BR da Universidade de São Paulo (USP), Diretor do Instituto de Defesa do Cidadão na Internet – IDCI. Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros e "Marco Civil da Internet: Comentários à Lei 12.965/2014" e "Manual de Crimes Informáticos". É colunista da Rádio Justiça/STF.

consultor@josemilare.com.br

Como hackers tiveram acesso a conversas privadas de Sergio Moro?

O Especialista e Perito Digital, José Milagre, esclareceu ao Uol algumas dúvidas sobre o acesso às conversas do Ex Juíz e falou sobre a criptografia de ponta a ponta que protege o Chat Secreto do Telegram.

Para saber mais acesse: https://www.uol.com.br/tilt/noticias/redacao/2019/06/10/como-hackers-tiveram-acesso-a-conversas-privadas-de-sergio-moro.htm

---

Lições para aprender rápido com o vazamento de senhas envolvendo sistemas do Ministério da Saúde

16 milhões de pessoas teriam sido comprometidas. Cidadãos podem requerer informações e mais transparência sobre o incidente envolvendo dados pessoais.

José Antonio Milagre

Repercutiu no país o vazamento de senhas de sistemas eletrônicos do Ministério de Saúde e que teria permitido o acesso a dados pessoais de pelo menos 16 milhões de pessoas, sendo considerado o maior vazamento de dados sensíveis do Brasil. O problema ocorreu a partir da publicação das credenciais em uma plataforma aberta na internet, comumente utilizada para compartilhamento de códigos.

Os dados publicados poderiam ser usados para acessar dados como CPF, endereço, telefone e dados pessoais sensíveis como doenças pré-existentes. Dados sensíveis são aqueles cuja exposição podem causar danos a direitos e liberdades dos indivíduos, ou que possam ensejar discriminação do titular e incluem as informações e dados referentes à saúde.

As senhas foram disponibilizadas em uma planilha, sem proteção, que por sua vez fora disponibilizada no site GITHUB, comumente usado por programadores para compartilhamento de

códigos. A questão se traduz em uma nítida falha humana, de colaborador que, sem observar requisitos e diretrizes de segurança da informação, bem como inconsciente de princípios fundacionais de privacidade por design, publicou o conteúdo crítico em uma área pública, com intenção temporária, como se fosse uma “área de transferência”, mas esqueceu de apagar. O colaborador foi demitido.

Importante destacar que os controladores de dados pessoais são considerados pela Lei como pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Neste sentido, o fato apenas expõe a previsão da Lei Geral de Proteção de Dados, sobretudo, a responsabilidade de controladores em relação a atos de seus colaboradores e prestadores de serviços.

O fato de publicar uma nota de que “não houve publicação de dados” pelo colaborador não afasta o risco, pois, a partir das credenciais, pessoas mal intencionadas poderiam acessar os referidos dados, por meio de acesso a sistemas do Governo Federal.

A denúncia de quem encontrou a vulnerabilidade foi a um Jornal, o que pode ser um indício de que os agentes de tratamento tomaram conhecimento a partir da notícia publicada. Seja como for, o fato escancara a necessidade de empresas estabelecerem procedimentos claros e de desenvolverem processos para tratar incidentes com dados, que possam ocorrer, atendendo a LGPD. Canais acessíveis para se receber comunicados sobre supostas violações são fundamentais.

A norma informa em seu artigo 42 que o controlador ou o

operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a reparar. Do mesmo modo, informa que estes agentes de tratamento serão responsáveis pelos danos decorrentes da violação da segurança dos dados, quando não adotarem as medidas de segurança previstas no art. 46, e assim, dando causa aos danos.

O art. 46 da norma prevê a necessidade de agentes de tratamentos adotarem medidas técnicas e organizativas para protegerem os dados pessoais, sobretudo de acessos não autorizados. Em complemento, a ISO/IEC 27701 estabelece controles, requisitos e diretrizes que podem ser adotados por agentes de tratamento de dados, de modo a comprovar ou atender parte das necessidades regulatórias.

Em caso de incidentes como o ocorrido, no entanto, deve a empresa comunicar à Autoridade Nacional e ao titular sobre a ocorrência, que possa lhe acarretar risco ou dano. Embora a Autoridade Nacional de Proteção de Dados ainda deva definir detalhes sobre esta comunicação, a Lei já traz o que uma comunicação de violação de dados pessoais deverá conter:

A descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial, os riscos relacionados ao incidente, os motivos da demora, no caso de a comunicação não ter sido imediata, as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Neste sentido, o fato de lançar mão de “notas públicas” genéricas, em nossa visão, não pode ser considerado o mais efetivo e transparente de cientificar pessoas possivelmente afetadas, inclusive em seus dados sensíveis. Deste modo, não é demais dizer que os cidadãos e titulares de dados podem requerer aos agentes envolvidos informações sobre o ocorrido, em detalhes, até para que possam se proteger, caso seus dados constem do possível vazamento.

Como visto, um Sistema de Gestão da Proteção de Dados, considerando um Time de Resposta a Incidentes devidamente constituído, preparado e com processos claros para responder a notificações de violação de dados é fundamental, sobretudo porque no juízo de gravidade do incidente, a comprovação de medidas técnicas adequadas, não só reativas, mas preventivas, serão consideradas, como, por exemplo, medidas para tornar os dados ininteligíveis.

O caso em tela nos exemplifica situações corriqueiras que muitos hoje ainda praticam e que podem causar danos terríveis aos titulares. A falta de treinamentos e conscientização corporativa pode custar muito caro. Mais grave que isso, pesquisas e strings repassados aos buscadores podem revelar repositórios de dados pessoais, mantidos por empresas a órgãos públicos, expostos e esquecidos em diretórios não protegidos e indexados pelos buscadores, onde sequer senha é necessária para acesso. Muito ainda será exposto. A negligência ainda persiste, mesmo com o advento da LGPD e, francamente, não há previsão de que este cenário de consciência de privacidade mude em um curto lapso temporal, sobretudo, enquanto as penas à altura dos danos praticados não comecem a ser aplicadas.

José Antonio Milagre é advogado especialista em segurança da informação e crimes cibernéticos, Mestre e Doutorando em

Ciência da Informação pela UNESP, Data Protection Officer (EXIN), e Diretor-Presidente do Instituto de Defesa do Cidadão na Internet (IDCI-Brasil). consultor@josemilagre.com.br

---

Black Friday 2020: Especialista em crimes digitais, José Antonio Milagre, orienta como evitar golpes virtuais e como agir caso tenha sido vítima.

Mais uma BlackFriday se aproxima e com ela o oportunismo de criminosos cibernéticos, que usam de técnicas variadas para aplicação de golpes, explorando muitas vulnerabilidades dos consumidores virtuais, que desatentos, acabam fornecendo dados pessoais ou comprando em páginas falsas, que são criadas apenas pelo período necessário para tirar o dinheiro do consumidor. Esta edição, porém, promete ser maior por conta do isolamento social diante da COVID-19. Segundo a Ebit Nielsen, as vendas devem crescer 27% em comparação com a edição de 2019.

Os criminosos digitais têm criado "lojas iscas", normalmente hospedadas em servidores no exterior. Do mesmo modo, ocultam os dados do registrante, por meio de registros *"domain by proxy"*, tudo para dificultar a investigação de quem está por

trás do e-commerce “simulado”.

Rapidamente investem em anúncios nos buscadores e outros métodos de impulsionamento, incluindo redes sociais e rapidamente ficam bem ranqueados na rede. A vítima então se depara com o anúncio, normalmente com preço fora do comum. Se não se atentar para elementos visuais da página ou dados de contato da loja, acaba acreditando que está fazendo um bom negócio, e nunca mais verá seu dinheiro.

As lojas falsas, normalmente se valem de depósito bancário ou boletos, que dificultam o cancelamento das compras ou o rastreio do dinheiro. Assim, todo o cuidado é pouco no período de promoções, já que o crime digital brasileiro explora momentos de grande mobilização digital para auferir lucro, lesando pessoas.

O advogado e perito especialista em crimes cibernéticos, José Antonio Milagre, CEO da CyberExperts e Diretor do Instituto de Defesa do Cidadão na Internet (IDCI) apresenta estratégias para se proteger de golpes digitais e dá dicas sobre como agir, caso tenha sido vítima de fraudes e crimes cibernéticos na BlackFriday.

Dez estratégias para que não que seja vítima de golpes digitais na BlackFriday:

1) Cuidado com descontos absurdos. Embora seja Blackfriday, 90% de desconto é algo estranho de se ver. Cuidado, confira a média de preço dos produtos. O criminoso vai usar este gatilho para chamar sua atenção;

2) Avalie a reputação da Loja. Em um universo de aproximadamente 1 milhão de lojas virtuais, muitas delas podem ser “lojas iscas”, criadas para ficar no ar por pouco tempo, fazer centenas de vítimas e desaparecer. Portanto, pesquise se a loja tem “histórico”, comentários, outras compras, etc. O Google está aí para isso;

3) Avalie as formas de pagamento. Desconfie de lojas que só oferecem depósito bancário, boleto ou criptomoedas. Estas modalidades podem dificultar o cancelamento da compra ou a investigação dos destinatários. Opte sempre por meios de pagamento seguros, onde o dinheiro é liberado quando o consumidor declara que recebeu a mercadoria;

4) Busque contatos da loja. Faça contatos prévios com a loja, mas não só por e-mail, busque um contato telefônico, verifique onde está a sede e desconfie de lojas onde o único contato é um telefone celular;

5) Cuidado com ofertas em comunicadores, e-mails e redes sociais. Jamais clique ou acesse lojas virtuais a partir de links, ou ofertas que receber em comunicadores, WhatsApp e redes sociais;

6) Não acesse lojas pelo buscador. Acesse diretamente o site da loja evitando também pesquisar pela loja no buscador. Cuidado com pequenas mudanças no nome do site e avalie se possui certificado digital expedido para o próprio site. Os criminosos digitais podem falsear um link direcionando a vítima para o site errado. Ataque de pishing são muito comuns, com a falsificação de marcas e identidade visual de sites com ofertas de descontos, dentre outras chamadas para pescar consumidores desatentos;

7) Cuidado com códigos enviados para o celular para supostos descontos. Imagine que você recebe uma mensagem que conseguiu um cupom especial para o BlackFriday, mas para que você receba, você precisará informar um código que chegará pelo celular via SMS. Neste exato momento a vítima não ganhou o desconto, mas pode ter permitido a clonagem do WhatsApp ou até mesmo ter o reset de senhas de app's financeiros realizados com sucesso, dando acesso ao criminoso. Não confie jamais nesta abordagem. Não informe a ninguém códigos que receber pelo celular;

8) Golpes com PIX. Muitos criminosos também poderão explorar este momento envolvendo a novidade, falsear identidade visual de lojas e oferecer produtos com "desconto" para compras com o pix, oferecendo códigos errados ou chaves que direcionarão o pagamento para o fraudador. Muita cautela no uso da nova tecnologia;

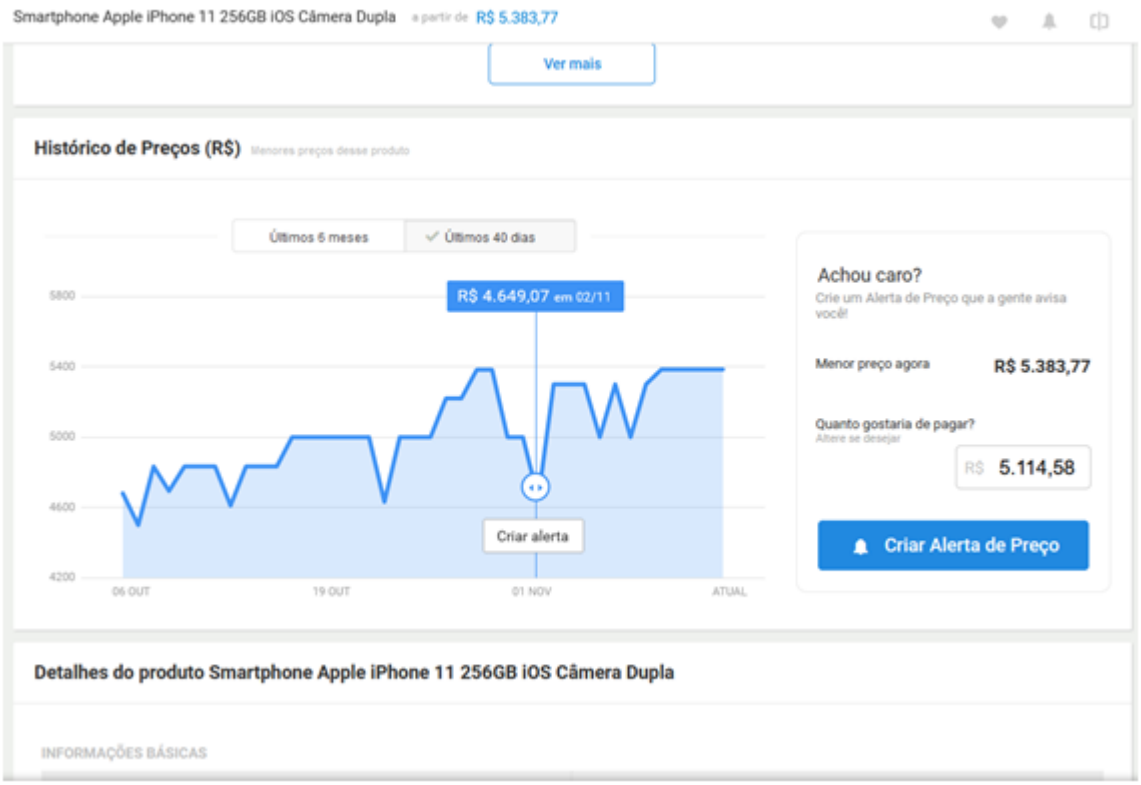
9) Desconfie de dados excessivos. Cheque a política de privacidade do site, se conecte a partir de uma conexão segura, avaliando se o site também tem SSL (https) assegurando proteção contra interceptação de dados e jamais forneça dados mais que necessários para a compra, como "senha do cartão" e outros dados. Mantenha sempre seu sistema operacional atualizado, com firewall e anti-malware ativados;

10) Faça provas de tudo. Guarde provas de toda a compra, salve os códigos, registre prints, e-mails recebidos, se necessário registre em vídeo do processo de compra. Todos estes dados podem ser uteis diante de uma fraude ou golpe, onde a perícia digital poderá identificar a autoria dos criminosos.

Avaliar aspectos de legalidade de um site nem sempre é uma

tarefa fácil para o consumidor. Embora a Lei Geral de Proteção de Dados já esteja em vigor (LGPD), já esteja em vigor, muitas lojas ainda não estão em conformidade e não são totalmente transparentes em seus processos.

Outra proteção importante, mas não realizada a golpes digitais, é avaliar as chamadas “fraudes” de lojas que sobem o preço para depois baixarem. Para isso sites como buscapé, zoom e baixou agora podem auxiliar, pois, apresentam um histórico do preço.



Buscapé mostra preço do Iphone 11 em 02/11 e 14/11 de R$ 4649,07 por R$ 5383,00

Caso tenha sido vítima de um golpe digital, o especialista, José Antonio Milagre, recomenda: “Imediatamente *resgate todos os dados da compra, registre um boletim de ocorrência online e procure um especialista em direito digital e crimes cibernéticos para que se incie um processo de apuração da*

autoria e responsabilização dos criminosos. Em casos de clonagem do chip, pode-se buscar a reparação em face da operadora de telefonia móvel.”

Do mesmo modo é muito importante contactar o banco com informações sobre a fraude e notificar a loja que eventualmente teve a marca usada para a fraude, para se buscar uma resolução amigável. As lojas podem ser responsáveis, se não adotavam medidas de segurança da informação ou não monitoravam o uso indevido de suas marcas, permitindo que fossem usadas para fraudes e golpes.

Porém, é importante advertir, se a loja comprovar que não deu causa ou que a despeito de todas as ostensivas demonstrações de segurança, a culpa foi exclusiva do consumidor, esta pode não se obrigada a reparar. Cada caso é um caso, e muitos deles serão apreciados pela Justiça. Por isso, prevenção é a melhor opção, sempre.

O IDCI (Instituto de Defesa do Cidadão e Consumidor na Internet) presta atendimento e apoio a vítimas de golpes e crimes cibernéticos, por seus canais, Siga @idcibrasil no Facebook e Instagram.

Prof. MSc. **José Antonio Milagre**, é Advogado e perito especializado em Direito Digital e Crimes Cibernéticos, Mestre e Doutorando Ciência da Informação pela UNESP, Presidente da Comissão de Direito Digital da OAB/SP Regional da Vila Prudente, Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros “Marco Civil da Internet: Comentários à Lei 12.965/2014” e “Manual de Crimes Informáticos”. Fundador do Instituto de Defesa do Cidadão na Internet – IDCI.

Canais:

http://www.instragram.com/drjosemilagre

http://www.facebook.com/drjosemilagre

http://www.youtube.com/josemilagre

Criminosos fraudam dados para sacar FGTS. Saiba como se proteger com as dicas do Especialista José Milagre

O Especialista em Direito Digital, José Milagre, participou do Fala Brasil da Record TV, apresentado por Celso Zucatelli, para para falar sobre a nova modalidade de crime cibernético. Os criminosos estão fraudando dados em aplicativo do governo para sacar FGTS de beneficiários. Quais os cuidados e como se proteger. A matéria já está no Portal do R7.

Saiba mais em:https://recordtv.r7.com/fala-brasil/videos/criminosos-fraudam-dados-em-aplicativo-do-governo-para-sacar-fgts-de-beneficiarios-22102020

35 milhões de chaves “PIX” registradas. Você sabe como se proteger dos criminosos?

Segurança da informação e dados pessoais no uso do PIX! Matéria realizada pela Rede Globo – TV TEM, com a participação do perito e especialista em Crimes Digitais, José Milagre, para falar sobre os riscos e os cuidados que os usuários e correntistas devem ter para não sofrerem golpes digitais. Já são mais de 35 milhões de chaves geradas e todo o cuidado é pouco!

Assista
em http://g1.globo.com/…/transferencias-bancarias…/8958459/