

Workshop LGPD

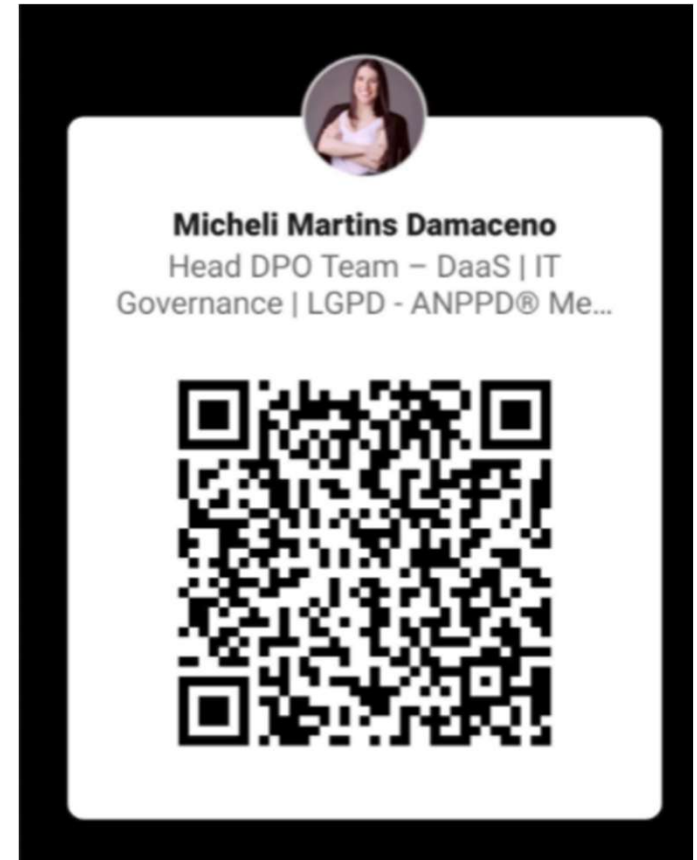
Projeto de Adequação



Apresentação

Micheli Martins Damaceno – Head DPO Team - Daas

Graduada em Ciência da Computação com Especialização em Gestão Estratégica em TI. Certificações em ITIL, COBIT, IT Governance, PDPE (Privacy and Data Protection Essentials), ISFS (Information Security Foundation), PDPF (Privacy and Data Protection Foundation) e Lean IT. Membro do Comitê de Segurança ANPPD - Associação Nacional dos Profissionais de Privacidade de Dados. Líder de apoio Womcy Girls & Geek e Mentora Cloud Girls.



Sumario

- Sobre a Lei 13.709
- Principais Conceitos da Lei
- Titular de Dados
- Os Impactos da Lei
- Penalidades
- Etapas de Adequação
- Conscientização e Boas Práticas em Segurança da Informação
- Dúvidas?

Sobre a Lei 13.709

LEI 13.709, DE 14 AGOSTO DE 2018, conhecida como Lei Geral de Proteção de Dados Pessoais, foi sancionada com o intuito de aumentar a responsabilidade das empresas sobre a forma como lidam com informações pessoais, evitando vazamento, abusos, perda ou uso dos dados para fins não autorizados. É importante ressaltar que os dados pessoais não são apenas de clientes, aplicando se também aos dados de funcionários, prestadores de serviço, entre outros.

- Ela traz uma nova realidade ao cotidiano de todas as empresas, não importa o segmento ou porte, atinge todas sem qualquer distinção.
- Pelos escândalos de vazamentos de informações, envolvendo empresas gigantes como Facebook, Google expondo dados pessoais de milhões de pessoas, motivaram governos de vários países a tratarem o tema com legislação específica.



Principais Conceitos da Lei

CONTROLADOR pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais	OPERADOR pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador	AGENTES DE TRATAMENTO o controlador e o operador	ENCARREGADO ("DPO") pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional
TRATAMENTO toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração	CONSENTIMENTO manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada	MAPEAMENTO DE DADOS é o processo de identificar elementos de dados entre dois modelos de dados distintos, ou mediação de dados entre uma fonte de dados e um destino (passos)	FLUXO DE DADOS é a representação do mapeamento de dados normalmente reproduzido por processo ou subprocesso, incluindo transferências de dados.

Fonte: KPMG – Microsoft Summit Proteção de Dados – Trilha TI e Segurança

Titular de Dados

Dado pessoal é o que identifica uma pessoa!

Dado sensível: origem racial, ou étnica, convicção religiosa, opinião política, entre outros.



Acesso e retificação

Anonimização, bloqueio ou eliminação:
dados excessivos

Portabilidade

Informação sobre o compartilhamento
de dados

Negativa de consentimento:
informações e consequências

Revogação do consentimento

Os Impactos da Lei

- Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários;
- Mudança de paradigma;
- Cultura empresarial;
- Visão de marketing corporativo;
- Empresas passam a ter dados mais qualitativos;
- Segurança jurídica para as pessoas.



Sobre a Lei 13.709

PENALIDADES:

A legislação estabelece ainda as penalidades aplicáveis no caso de descumprimento das regras nela estabelecidas, que variam desde advertência até multas (que podem ser diárias) de até 2%(dois por cento) do faturamento da pessoa jurídica até o limite R\$ 50.000,000,00 (cinquenta milhões de reais) por infração.

Contudo, as penalidades levarão em conta diversos critérios objetivos.

Etapas da Adequação



Conscientização e Boas Práticas de Segurança da Informação

Formatos da Informação

		
FÍSICO	VOLÁTIL	DIGITAL
Documentos Impressos Anotações em Papel Mídias (Pendrives, HD's)	Conversas Telefônicas Reuniões Conversas Informais	Internet, Redes Sociais E-mails, Banco Dados Arquivos, Sistemas, Mobile App
		
<p>A informação é um ativo valioso e deve ser tratado de forma adequada visando garantir Confidencialidade, Integridade e Disponibilidade para posterior avaliação e divulgação</p>		
		

Conscientização e Boas Práticas de Segurança da Informação

Riscos

Segurança da Informação

PESSOAS

- Conscientização e Capacitação
- Descaso com informações da empresa
- Definição de Responsabilidades
- Engenharia Social

CONSEQUÊNCIAS

- Ações judiciais e perdas de clientes
- Impacto negativo na imagem da empresa
- Acesso indevido à informações confidenciais
- Redução do valor da marca
- Indisponibilidade de serviços



TECNOLOGIA

- Indisponibilidade Infraestrutura
- Falhas em sistemas e bancos de dados
- Perda de Notebooks e dispositivos Móveis
- Invasão a rede da empresa

PROCESSOS

- Vulnerabilidades em processos/sistemas
- Ausência de controle de acesso

Prevenção contra Ransomware

Protegendo a Integridade dos Dados da sua Empresa.



[View this email in your browser](#)

Ransomware é um malware / tipo de ataque cibernético, que criptografa e bloqueia os dados das vítimas, provocando a restrição do acesso aos dados da **Empresa** que sofreu o ataque.

Depois do sucesso no ataque, as empresas são exigidas a pagar um resgate, pela troca de um método para descriptografar ou desbloquear os arquivos.

COMO O RANSOMWARE TRABALHA



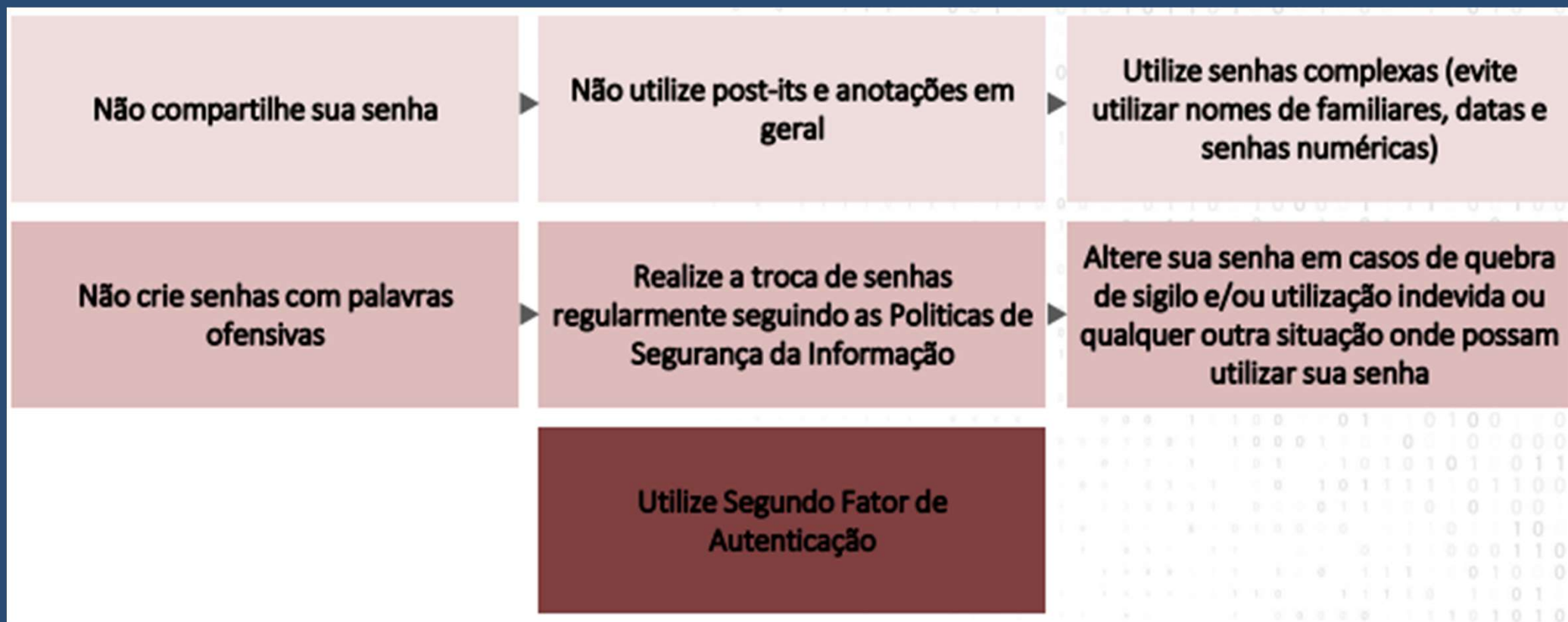
Site da Renner sai do ar após ataque hacker – entenda o caso

Uma das empresas de TI que atende a varejista disse que seus sistemas não foram afetados. A suspeita é que o ataque se concentra em servidores de Porto Alegre

Leonardo Guimarães,
do CNN Brasil Business, em São Paulo*

Conscientização e Boas Práticas de Segurança da Informação

Controles de Senhas



Conscientização e Boas Práticas de Segurança da Informação

E-mail Corporativo

Não utilize o e-mail corporativo para questões pessoais. Siga a Política de Segurança da Informação

EXCLUA e-mails não solicitados

Verifique se os endereços dos destinatários estão corretos. Evite o envio indevido de informações

Utilize Criptografia sempre que disponível

Não encaminhe e-mails que comprometam a privacidade, pedidos de ajuda e obscenos

Conscientização e Boas Práticas de Segurança da Informação

Internet e Redes Sociais

Não acesse páginas da internet que contenham conteúdo pornográfico, difamatório, ofensivo, discriminatórios ou afins

Não realizar publicações em redes sociais de conteúdo corporativo que não seja autorizado pelas áreas de comunicação

Não utilize ferramentas de navegação (browser) não homologadas pela Área de Tecnologia da Informação

Não faça download de aplicativos, sistemas ou afins sem o consentimento de TI

Não utilize os recursos da empresa para participar de jogos pela Internet ou download de qualquer natureza que não seja de interesse corporativo

Conscientização e Boas Práticas de Segurança da Informação

Organização



Mesa Limpa e Armários
trancados



Ctrl + Alt + Del para
bloquear o computador



Retire os documentos da
impressora



Apague informações de
quadros e flicharts



Não armazene informações
em computadores
compartilhados



Recolha anotações após
reuniões internas

Conscientização e Boas Práticas de Segurança da Informação

Privacidade e Sigilo

Somente compartilhar informações confidenciais com colaboradores que necessitem dessas informações para realizar os seus trabalhos

Utilize as informações da empresa de maneira segura e não permita sua circulação de forma descontrolada

Evitar conversas sobre quaisquer informações da empresa em locais abertos.

Se as **informações forem confidenciais, o cuidado deve ser redobrado**, mesmo nas instalações da Companhia (recepção, corredores, copa etc.)

DÚVIDAS?

micheli.martins@clm.com.br

11 989934109