GUIA DA LEI GERAL DA PROTEÇÃO DE DADOS

VERSÃO 3.0

O CAMINHO DAS PEDRAS PARA SUA EMPRESA ENTRAR EM COMPLIANCE COM A LEI

BluePex®

Introdução

LEI GERAL DA PROTEÇÃO DE DADOS

Muito em breve, entrará em vigor a Lei Geral de Proteção dos Dados Pessoais (Lei nº. 13.709/2018) que regulamenta a coleta, o uso e o tratamento de dados por parte de órgãos privados e públicos.

Ela impactará empresas de todos os segmentos, que precisarão se adequar às mudanças.

Com a data de vigor da lei cada vez mais próxima, ainda existem muitas dúvidas com relação ao assunto.

Por esse motivo, nós da BluePex® resolvemos escrever este eBook com as informações mais importantes. Espero que a sua leitura seja proveitosa!

SUMÁRIO

O que é LGPD.....4

Segurança da informação x Segurança na TI.....4

Por que devo me preparar?.....4

O que a Lei Tutela.....5

Tipos de Dados.....5

O Alcance da Lei.....6

Os papéis.....6

A quem pertencem os dados?.....6

Direitos do titular dos dados.....7

Consentimento.....7

Coleta Mínima.....7

Penalidades.....8

Exceções da Lei.....8

Princípios da LGPD.....9

Roadmap: Por onde começar a implementar a LGPD.....10

Entendendo os Riscos.....11

Boas práticas na segurança da tecnologia.....12

Boas práticas nos processos.....13

Boas práticas no jurídico.....14

Como a BluePex® pode te ajudar.....15

O QUE É LGPD?

A Lei Geral da Proteção de Dados é uma lei que surgiu da demanda pela proteção da privacidade do indivíduo, assunto cuja complexidade só aumenta a cada dia, atrelada diretamente à evolução dos meio digitais.

A LGPD faz um paralelo com a lei do com a lei do consumidor CF 1988 Art. 5º, X:

> *"São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação."*

Dito isto, podemos considerar a LGPD como um sistema legislativo criado para assegurar os direitos do indivíduo, estabelecidos pelo artigo 5º.

> *A LGPD foi inspirada na legislação GDPR da União Europeia, que foi criada em 2016 e entrou em vigor em 2018. Para as empresas nacionais estabelecerem relações com empresas da União Europeia, é necessário que elas estejam em compliance com a LGPD, que está correlacionada com a GDPR.*

SEGURANÇA DA INFORMAÇÃO X SEGURANÇA NA TI

É importante observar que a LGPD não diz respeito somente aos dados digitais. Um dado físico também pode passar por um vazamento, passível de punições previstas na lei. Uma nota escrita a mão, a pasta do funcionário no RH ou um contrato impresso contendo os dados de um cliente precisam ser protegidos tanto quanto os dados no computador, no servidor ou na nuvem. Portanto é importante enxergar a forma que a empresa manuseia os dados como um todo.

Dito isto, ao contrário do pensamento comum, a LGPD não abrange apenas o setor de TI (tecnologia da informação), mas também o financeiro, os recursos humanos, o departamento comercial, o marketing etc.

Não confunda a segurança da informação com segurança na TI!

POR QUE DEVO ME PREPARAR?

Atualmente já existem legislações que visam garantir a segurança dos dados, como o Marco Civil da Internet, por exemplo. Porém não existe uma grande preocupação

por parte das empresas em estar em compliance com estas leis, afinal é muito raro a aplicação de multas no caso de descumprimentos.

Mas então por que com a LGPD será diferente?

Vamos fazer um breve comparativo: Por que a lei do consumidor funciona, e é atendida por todas as empresas no Brasil?

Porque existe o PROCON.

Quando o consumidor (pessoa física) se sente lesado por um produto ou serviço, ele se dirige ao PROCON e efetua uma reclamação, que caso apurada, geram multas para a empresa, que pode ter a infração exposta na mídia, o que mancha a imagem corporativa.

A LGPD segue um sistema parecido com o da lei do consumidor.

Uma pessoa que se sentir lesada por um mau uso ou vazamento dos seus dados poderá se dirigir à **ANPD (autoridade nacional da proteção de dados)**, efetuar sua reclamação, que ao ser apurada pode gerar diversos problemas para a empresa, como penalidades, multas, e exposição na mídia, o que pode manchar profundamente sua imagem junto ao público.

> *Enquanto a LGPD não entra em vigor outros órgãos ficam responsáveis pela fiscalização, como a* ***Comissão de Proteção de Dados Pessoais do Ministério Público do Distrito Federal e Territórios.***

O QUE A LEI TUTELA?

- Os direitos fundamentais de liberdade e de privacidade do **INDIVÍDUO**;
- O livre desenvolvimento da personalidade da **PESSOA NATURAL**.

Ou seja, a LGPD tutela o manuseio dos dados da pessoa física (nome, CPF, RG etc.).

Dados relacionados a empresas (CNPJ, razão social etc.) não se enquadram na lei.

TIPOS DE DADOS

Os tipos de dados pessoais são divididos em quatro categorias:

Dado identificado: são dados nos quais é possível identificar diretamente o indivíduo.

Exemplos: Nome completo, RG, CPF.

Dado identificável: são dados que não identificam diretamente o indivíduo, mas que juntamente a outros dados pode ajudar a identificá-lo.

Exemplos: Número do cartão de crédito, empresa em que trabalha, Endereço, IP do computador.

Dado sensível: Dados relacionados à vida privada, honra e imagem das pessoas, que podem gerar algum tipo de discriminação.

Exemplos: Convicção religiosa, opção sexual, opinião política, informações sobre saúde.

Dado anonimizado: Aquele em que não é possível identificar a pessoa.

Exemplo: Pesquisa do IBGE.

O ALCANCE DA LEI

- A LGPD abrange qualquer operação de tratamento de dados realizada por pessoa física ou jurídica, de direito público ou privado.
- A lei é válida para qualquer dado que seja tratado no Brasil, sendo o titular do dado brasileiro ou estrangeiro.
- Se o dado estiver hospedado fora do Brasil (em um servidor da Amazon, por exemplo) mas é tratado no Brasil, ainda assim se enquadra na LGPD.

OS PAPÉIS

- **Titular:** a pessoa natural a quem pertencem os dados pessoais;
- **Controlador:** responsável pelo tratamento (uso) dos dados pessoais;

Exemplo: Loja de Roupa que coleta os seus dados para fazer um cadastro.

- **Operador:** Pessoa ou empresa terceira que realiza o tratamento dos Dados

Exemplo: O escritório contábil que administra a carteira da empresa.

- **Encarregado:** pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador e o titular (ou com A ANPD caso já efetuada alguma denúncia). O encarregado atua como uma espécie de relações públicas.
- **Autoridade Nacional de Proteção de Dados:** Órgão nacional responsável por fiscalizar e aplicar a lei. Funciona como se fosse um “PROCON” da LGPD.

> ***DPO***
> *É necessário ter em mente que o DPO é uma função atribuída na **GDPR,** a versão européia da LGPD, e que muitas vezes é utilizada como comparativo à lei brasileira. A função de DPO não necessariamente existe na LGPD, o mais próximo disso seria o **encarregado**.*

A QUEM PERTENCE OS DADOS?

Os dados pertencem unicamente ao **TITULAR**. O controlador e o operador apenas manuseiam estes dados com o **CONSENTIMENTO** do titular. Portanto é estritamente proibido utilizar estes dados para fins que não foram apresentados de forma clara ao titular, e consentidos por ele.

Exemplo prático

Uma farmácia coleta o CPF do cliente e informa que o dado será usado unicamente para fornecer um desconto. O dado não pertence à farmácia, ela é apenas um controlador, quem trata o dado. Este dado será usado para fazer vendas e promoções para o titular, conforme informado.
Posteriormente a farmácia repassa este dado para um laboratório. A farmácia está cometendo uma infração à LGPD, pois não houve consentimento do titular para que o seu dado pessoal fosse repassado a uma empresa terceira.

DIREITOS DO TITULAR DOS DADOS

Acesso aos dados

- Atualização, correção e eliminação dos dados;
- Portabilidade;

Proteção dos dados

- Uso dos dados dentro dos parâmetros legais (consentimento);
- Remoção dos dados e esquecimento;
- Informação clara e precisa sobre o uso dos dados.

*No caso de ocorrer algum problema ou vazamento, o titular dos dados **DEVE** ser avisado, **SEMPRE** tente reverter a situação junto a ele. No caso de uma eventual reclamação à ANPD, caso comprovado que houve algum tipo de negociação ou uma tentativa de reverter a situação por parte do controlador dos dados, a justiça tende a aplicar penalidades menores.*

CONSENTIMENTO

Art. 7º - O Tratamento de dados pessoais somente poderá ser realizado:

I - Mediante o fornecimento de consentimento pelo titular.

Art. 11 - O Tratamento de dados pessoais sensíveis somente poderá ocorrer:

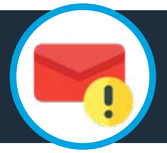
I - Se o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

COLETA MÍNIMA

Durante o planejamento do tratamento a ser realizado, estipule quais dados do cliente serão necessários para alcançar o objetivo desejado. **SEMPRE** colete o minímo de dados possíveis, apenas o necessário. Coletar dados desnecessários pode ser perigoso para a sua empresa, pois dificulta o controle, e no caso de um vazamento pode acarretar penalidades muito mais severas.

PENALIDADES

As empresas que não seguirem a lei poderão ser penalizadas severamente. Dentre as penalidades, temos:



Advertência
As empresas poderão receber avisos caso não estejam cumprindo com a lei.

Divulgação da infração
Infrações ou vazamento de dados poderão ser divulgados na mídia, causando danos à credibilidade e reputação da empresa.

Multas
De até 2% no faturamento anual ou até R$ 50 milhões para cada infração. Poderão ser aplicadas penalidades diárias de acordo com a gravidade.

EXCEÇÕES DA LEI

Existem algumas excessões à regra quanto ao tratamento de dados pessoais. São elas:

Tratamento de Dados Pessoais (Art. 7)

II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - Administração pública - T. e uso compartilhado de dados necessários à execução de políticas públicas (...);

IV - Estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - Necessário para a execução de contrato (...) do qual seja parte o titular, a pedido do titular dos dados;

VI - Exercício regular de direitos em processo jud., admin. ou arbitral;

VII - Proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - Tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - Atender aos interesses legítimos do controlador ou de terceiro exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dp;

X - Proteção do crédito, inclusive quanto ao disposto na legislação pertinente;

Tratamento de Dados Pessoais Sensíveis (Art. 11)

II Sem consentimento do titular quando for indispensável para:

a) Cumprimento de obrigação legal ou regulatória pelo controlador

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas;

c) Estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (incapaz de revelar a identidade de uma pessoa);

d) Exercício regular de direitos (execução de política pública, obrigação legal do controlador etc);

e) Proteção da vida ou da incolumidade física do titular ou de terceiro;

f) Tutela da saúde;

g) Garantia da prevenção à fraude e à segurança do titular nos processos de identificação

e) Autenticação de cadastro em sistemas eletrônicos (biometria, por ex.).

PRINCÍPIOS DA LGPD

Visto o conteúdo abordado anteriormente, todas as empresas que realizam atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação as finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

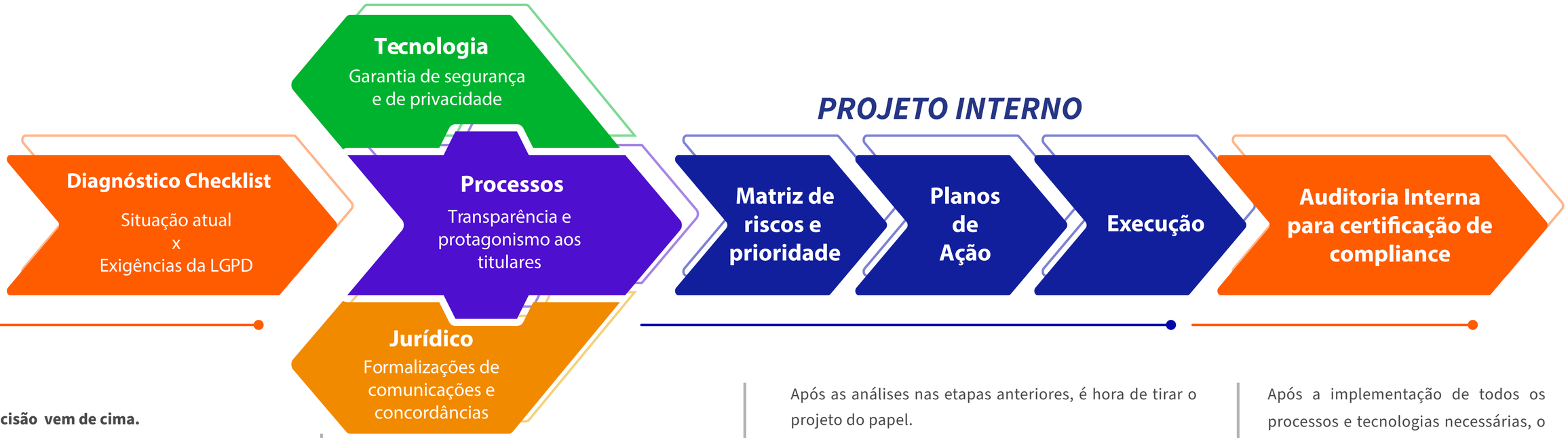
VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - Responsabilização e prestação de contas: demonstração, pelo agente, 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.

ROADMAP: POR ONDE COMEÇAR A IMPLEMENTAR A LGPD



A decisão vem de cima.

O primeiro passo é convencer a alta direção da importância da LGPD, seguida da criação de um comitê multidisciplinar, que ficará responsável pela implementação da LGPD na empresa.

Após a criação do comitê, deverá ser analisada a forma como os dados são atualmente tratados em cada setor da empresa, para depois comparar com as exigências da LGPD.

Deverão ser atendidos estes três pilares da segurança da informação. Pense nesta etapa como um tripé: **Se tirar um pé, todo o esquema cai.**

Tecnologia: Diz respeito à todo o aparato tecnológico utilizado para o tratamento e para proteger os dados.

Processos: Todo o processo relacionado aos dados, desde a coleta, tratamento e interação com o titular.

Jurídico: Contratos e formalizações.

Após as análises nas etapas anteriores, é hora de tirar o projeto do papel.

Matriz de riscos e prioridade: Aqui são definidos quais problemas serão resolvidos primeiros, através de uma análise de probabilidade x impacto.

Planos de Ação: Planejamento de quais ações serão tomadas na empresa como um todo para eliminar todos os riscos. **É importante definir datas e prazos.**

Execução: Fase de execução do planejamento realizado no passo anterior.

Após a implementação de todos os processos e tecnologias necessárias, o comitê deverá se reunir para verificar se a compliance está funcionando nos conformes.

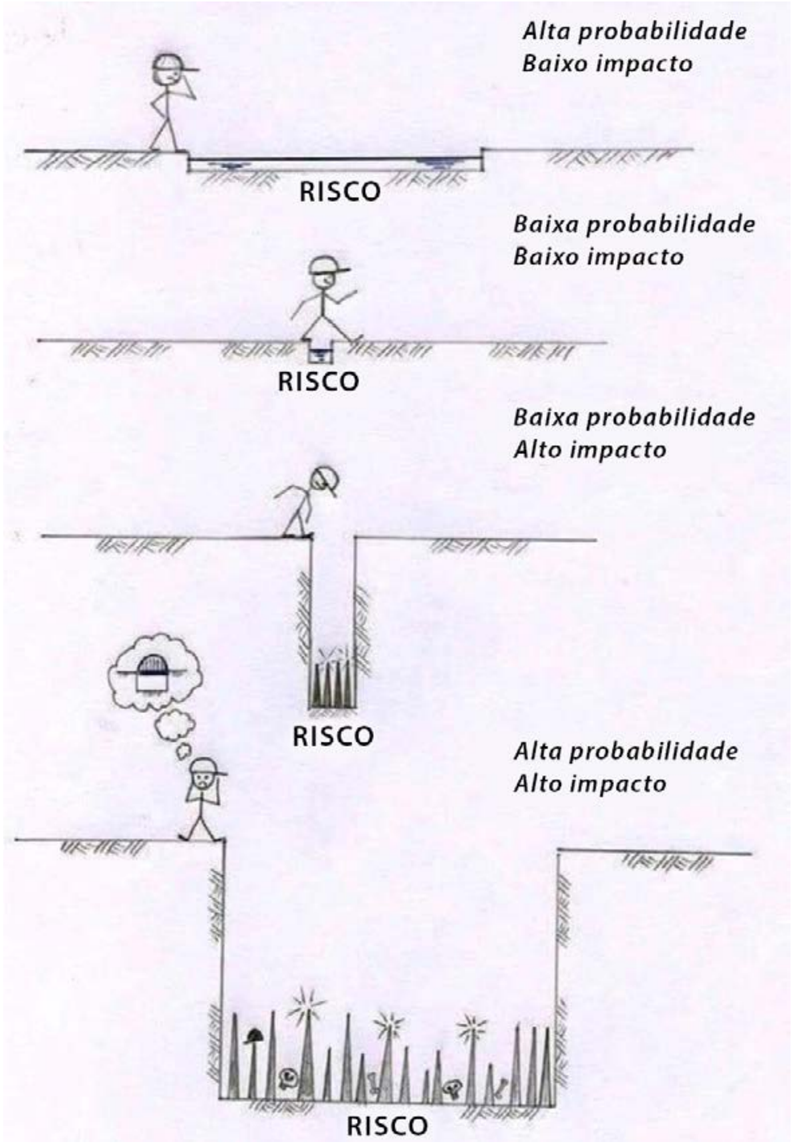
Caso seja identificado qualquer furo, deverão voltar à primeira etapa do roadmap até corrigir o problema.

ENTENDENDO OS RISCOS

O primeiro passo do projeto interno para a implantação da segurança de dados na sua empresa (logo após as análises) é o mapeamento de riscos.

O comitê interno deve mapear todos os pontos da empresa que estão passíveis de um vazamento de dados, identificar a probabilidade de vazamento, e no caso de uma eventualidade, qual seria o impacto causado por este vazamento.

Após esta análise, o próximo passo é tomar ações para reduzir o risco dos pontos mais críticos onde um vazamento possa ocorrer.



Fonte da imagem

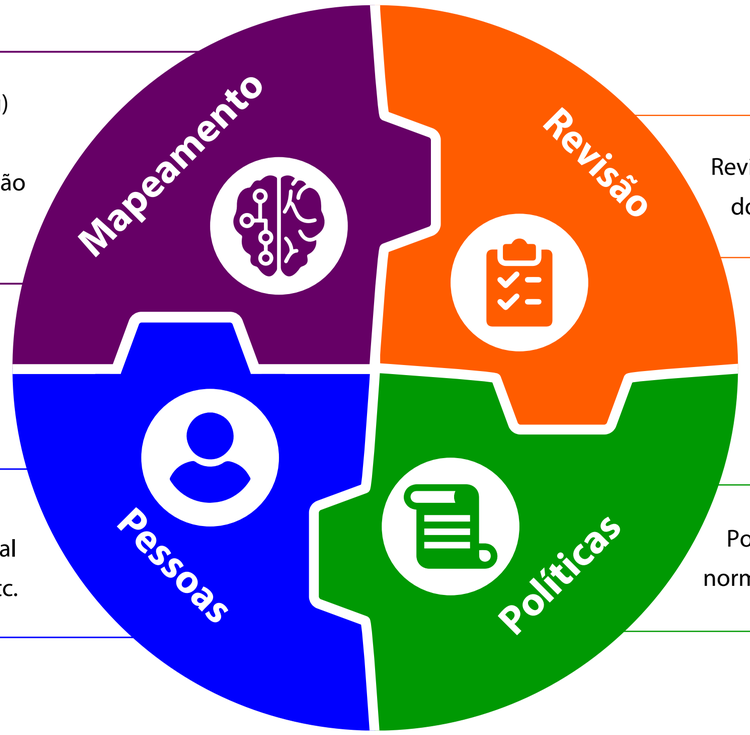
The Cyber Security Hub™

https://www.linkedin.com/company/the-cyber-security-hub/

BOAS PRÁTICAS DE SEGURANÇA NA TECNOLOGIA

BOAS PRÁTICAS DE SEGURANÇA NOS PROCESSOS

Mapear os dados pessoais (data mapping) tratados na empresa é o passo inicial que permitirá diagnosticar a situação em relação a legislação e planejar a adequação.



Revisão de processos, incluindo revisão dos procedimentos de segurança física.

Processos relacionados às pessoas: Conscientização, treinamentos (presencial ou EAD), termos de confidencialidade, etc.

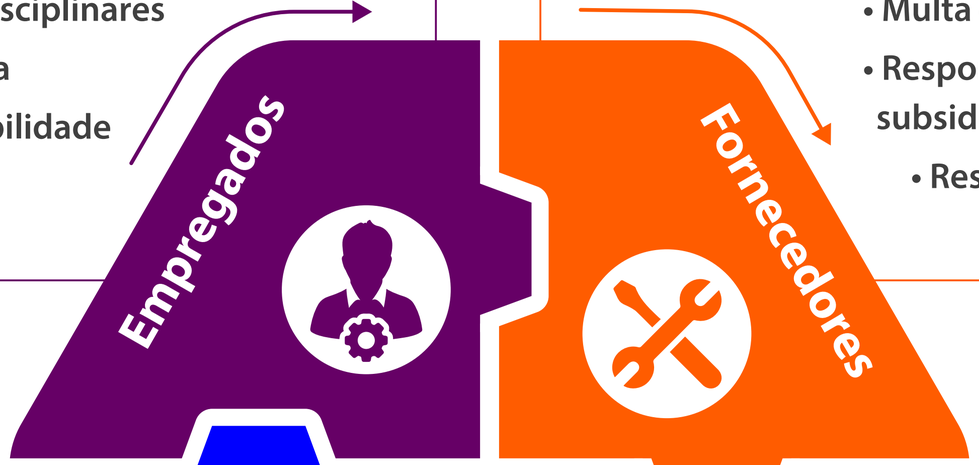
Políticas de segurança e privacidade, normas e procedimentos operacionais.

Referências de Apoio

- Business Process Management (BPM)
- Business Process Improvement (BPI)
- Normas da série ISO 9000 (ABNT NBR ISO 9000:2005, ABNT NBR ISO 9001:2008, ABNT NBR ISO 9004:2010

BOAS PRÁTICAS DE SEGURANÇA NO JURÍDICO

Deverão prever observância e sanções pelo descumprimento da LGPD



- Sanções disciplinares
- Justa causa
- Responsabilidade subsidiária

- Multa contratual
- Responsabilidade subsidiária
- Rescisão

- Multa
- Quebra da parceria
- Responsabilidade solidária
- Obrigação de adesão

- Incluir todas as autorizações possíveis para o uso de seus dados
- Coleta mínima

COMO A BLUEPEX® PODE TE AJUDAR

A BluePex® é uma desenvolvedora de soluções para segurança na TI, portanto podemos te fornecer várias soluções para auxiliar sua empresa na compliance com a LGPD no pilar da tecnologia. Conheça algumas de nossas soluções:

BluePex® Advanced Mail Security

Segurança avançada para e-mails

• Monitore o seu serviço de e-mail em uma dashboard de interface amigável. Conta também com a exportação de relatórios;

• Numa interface simples e fácil de acessar, o próprio usuário pode verificar os e-mails barrados, definir suas listas brancas e negras, ter acesso a quarentena e poder resgatar e-mail retidos. O Antispam arquiva os e-mails duvidosos a espera que o usuário possa fazer a aprovação ou rejeição.

• Monitoramento em tempo real de mais de 200 das principais blacklists, listas de antivírus e sites de busca. Caso seu e-mail caia na lista negra, nosso suporte orientará de como retirar;

• Crie as regras de e-mail rapidamente, filtro por remetentes, domínios, redes, países, regras em lote, tipos MIME, extensões de arquivo, regras personalizadas, regras RBL, SPF, DKIM, configurações Bayes, lista negra para destinatário, destinatários válidos e muito mais;

• Controle interno de conteúdo enviado nos e-mails, evitando vazamentos internos;

• Proteção contra vazamento de dados DPL;

• Proteção de armazenamento em nuvem (criptografado).

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: § 2º As informações e os dados poderão ser fornecidos, a critério do titular:
I - por meio eletrônico, seguro e idôneo para esse fim;

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS | Seção I | Do Controlador e do Operador
Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

BluePex® Firewall UTM NGFW

Segurança e controle para a borda da rede

• O novo formato do firewall por aplicação, além de identificar comportamentos padrões não somente nos cabeçalhos, mas também na área de dados dos pacotes e determinar que tipo de aplicação está associada, é um recurso extremamente relevante, pois permite não somente a visibilidade, mas também a operação de controle de acesso baseado no tipo de aplicação que está sendo acessada.

• Mapeie o nível de riscos da sua rede de forma inteligente, através de um painel de controle customizado para o gerenciamento de vulnerabilidades.

• Controle e bloqueie redes sociais e pornografia com o Webfilter+: controle o tráfego de internet de maneira a proteger a rede corporativa, limitando o usuário a navegar apenas em páginas de interesse da corporação. Alguns sites consomem banda excessiva de internet podendo prejudicar a disponibilidade do link. Já outros desperdiçam o tempo da sua equipe.

• A linha Firewall UTM NGFW da BluePex® possui a função IPS (Intrusion Prevention System), responsável por detectar arquivos intrusos na rede. Os malwares e outros tipos de artefatos maliciosos tentam invadir a rede sozinhos ou por intermédio de usuários involuntários. Neste caso, a função IPS monitora os acessos e detecta a tentativa de invasão. Os malwares são bloqueados automaticamente e os usuários infectados são sanitizados antes de entrar na rede.

• A proteção de navegação bloqueia o acesso a sites sinalizados por espalhar trojans, spyware ou qualquer outro tipo de software malicioso, impedindo a conexão e a infecção, assim bloqueando sites perigosos e fraudulentos para evitar phishing, downloads acidentais de malwares e outros tipos de artefatos maliciosos.

• A proteção de arquivos adiciona uma camada de proteção que verifica todos os arquivos baixados.

• O bloqueio por comportamento detecta novas ameaças que não são conhecidas pelo identificador de comportamento comum dos ataques.

• O Anti-Ransomware conta com monitoramento comportamental personalizado que impede o ransomware antes que ele possa criptografar qualquer dado.

• A proteção antimalware protege a borda da rede utilizando um banco de dados exclusivo de ameaças nacionais e internacionais, além da prevenção contra novos malwares e ataques sofisticados através de vulnerabilidades como o dia zero, utilizando inteligência

artificial heurística, bloqueando um comportamento duvidoso e emitindo um alerta.

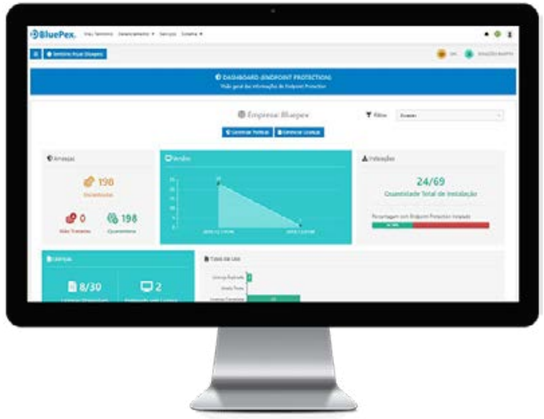
BluePex® Endpoint Protection & Control

Segurança e controle para endpoints e servidores

• A proteção de endpoints é responsável por proteger as estações de trabalho e servidores da sua rede. Para este fim, conta com recursos como proteção antivírus, antimalware, antiphishing e diversos outros artefatos maliciosos, proteção realtime do dispositivo e proteção da navegação, visualização de quarentena por usuário e diversos outros recursos. **Gerencie a proteção da sua rede:** Caso um usuário desative a proteção realtime da sua estação de trabalho, o gestor de TI recebe uma notificação.

• Visualize e gerencie os dispositivos conectados a rede: com a nossa solução, o gerente de TI terá uma melhor visibilidade do seu parque tecnológico, visualizando os dispositivos conectados à rede e identificando a necessidade de cada usuário de forma simples e remota.

• Com a informação nas suas mãos, será mais fácil prever diversos problemas que podem surgir de atualizações de software, falta de armazenamento, e etc, aumentando a vida útil dos equipamentos, reduzindo custos e aumentando a produtividade. Com esta ferramenta em mãos também é possível fazer inventários de software e hardware em poucos cliques.



CAPÍTULO VII | DA SEGURANÇA E DAS BOAS PRÁTICAS | Seção I |Da Segurança e do Sigilo de Dados
Art. 46. 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.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

CAPÍTULO VI | DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS | Seção I | Do Controlador e do Operador
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A BLUEPEX®

A BluePex® nasceu para suprir as maiores necessidades do mercado de TI: facilitar a Segurança, Controle, Disponibilidade e Compliance para o setor. Desenvolvemos tecnologia de última geração para a gestão de segurança na TI. O profissional de TI pode monitorar, proteger e antecipar problemas de sua rede, de onde quer que esteja.

Somos uma das maiores startups do país na área de gestão de segurança e infraestrutura de TI, e conhecemos como ninguém as peculiaridades do mercado nacional.

Nossas soluções são de desenvolvimento próprio, inovadoras, completas, intuitivas e de fácil integração para que a empresa tenha tranquilidade e segurança no seu dia-a-dia.

Possuímos expertise para atender o seu negócio. Contamos com um suporte consultivo em português, 24 horas por dia e 7 dias por semana, sem limites de chamado, com o objetivo de auxiliar nossos clientes em qualquer situação. Não paramos, pois sua empresa também não pode parar!

Conheça nosso portfólio de produtos! Acesse www.bluepex.com

CONTATO

0800 520 6505

business@bluepex.com

Agende uma apresentação com um de nossos especialistas em rede para saber mais sobre os nossos produtos.

São Paulo/SP - R. Professor Tamandaré Tolêdo, 69 | 15º Andar – Itaim Bibi
CEP 04532-020 | Telefone: (11) 4200-1404

Portugal - R. Engº Frederico Ulrich. 2650 | Porto - Moreira da Maia
CEP: 4470-605 | Telefone: 351 220301520

USA - 1230 Peregrine Way | Miami - Weston FL
Zip Code: 33327 | Telefone: +13055605940

Unidade Fabril: Limeira – SP | Regionais: Rio de Janeiro – RJ | Curitiba – PR | Recife – PE | Fortaleza – CE | Goiânia – GO

www.bluepex.com