Associação Nacional dos Profissionais de Privacidade de Dados

ARTIGO TÉCNICO

Segurança da Informação: Princípios essenciais para conformidade à LGPD

Resumo:
A segurança da informação vem ganhando protagonismo nas empresas que levam a sério a LGPD, principalmente pelo fato de que não é possível implementar a LGPD sem um mínimo de segurança da informação e assim garantir minimamente que, está de acordo com as recomendações de mercado e assim protegendo os dados.

1. Introdução

Com a data de início das sansões pela ANPD – Autoridade Nacional de Proteção de Dados já estabelecida para Agosto de 2021, as empresas que vem buscando se adequar a LGPD, estão identificando cada vez mais que se tiverem implementada mesmo que minimamente SGSI, facilita a adequação e implementação da LGPD.

Todas as empresas vão ter que se adequar a LGPD, protegendo os direitos dos titulares de dados, sejam eles clientes, funcionários, contratados ou fornecedores. O mercado terá seus olhos voltados para os vazamentos e multas aplicadas nas empresas que não se adequarem e permitirem vazamentos de dados.

Investidores estão sendo cada dia mais criteriosos no que tange a segurança da informação e LGPD, eles estão exigindo que empresas tenham boas práticas relativo a segurança da informação ISO27001, referência a Norma 27701 e recomendação para seguir na implementação da LGPD para que o investimento possa ser liberado sob um risco controlado.

Com o trabalho de conscientização de segurança da informação e LGPD que realizamos diariamente na ANPPD por meio de diversas mídias como redes sociais, artigos, lives, webinares e workshops, criamos no site da ANPPD um Portal de Violações - O "Violações LGPD" é um serviço de consulta pública gratuita que reúne as autuações relacionadas com privacidade de dados (sob a ótica da LGPD - Lei Geral de Proteção de Dados, e outras normas relacionadas ao tema) impostas por diversos órgãos brasileiros uma vez já tornadas públicas e publicadas nos sites das autoridades. Nem todas as tramitações tornam-se públicas, portanto, podem existir autuações não listadas. https://anppd.org/violacoes

A LGPD cita segurança em vários artigos na lei, em que precisamos reforçar as melhores práticas relacionadas à segurança da informação e LGPD:

Art. 6º As atividades de tratamento de dados pessoais deverão observar boa-fé e os seguintes princípios:
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;

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
g) garantia da prevenção à fraude e à **segurança** do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
IV - a adoção de **medidas de segurança** previstas em regulamento;

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;

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
Parágrafo único. Responde pelos danos decorrentes da **violação da segurança dos dados** o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano;

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;

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a **garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais**, mesmo após o seu término;

Art. 48. 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.
III - a **indicação das medidas técnicas e de segurança** utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

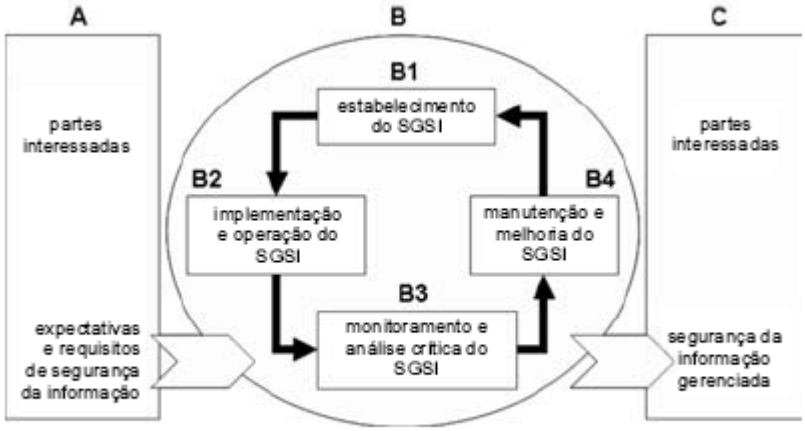
Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos **requisitos de segurança**, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares; e

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)
VI - **Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança**; (Incluído pela Lei nº 13.853, de 2019).

2. Adoção das melhores práticas de segurança da informação.

Dentro das melhores práticas relacionado a ISO 27001 podemos citar genericamente algumas práticas que vão facilitar a implementação da LGPD garantindo a segurança aos dados utilizados, coletados ou processados.

1. Comunicar imediatamente incidentes de segurança em vez de resolvê-los para garantir que a Evidencia Critica não seja destruída;
2. A relação entre ameaça e risco é que RISCO é baseado na probabilidade da ocorrência de uma ameaça;
3. A organização deve cumprir a legislação e regulamentos nacionais e locais é a primeira dentro da política;
4. Uma medida de segurança não é medida de nível organizacional é a Implementação de controle de acesso baseado em funções por exemplo;
5. Existem possibilidade de 2 tipos de danos que devem ser evitados e mitigados e são eles, indireto: ou
6. indireto: Perda de negócio devido a um ataque de DDOS;
7. Mitigação de ameaças como a divulgação das informações do sistema da empresa para um hacker;
8. Adoção de medidas físicas para detecção de segurança como Extintor de Incêndio;
9. Adoção Preventiva de contramedidas devem ser escolhidas para reduzir a possibilidade de ocorrência de um incidente;
10. Contramedidas de Prevenção como backup periódico realizado e arquivado em local seguro e resiliente;
11. Adoção de BYOD que permite apenas acessem a rede da empresa, somente dispositivos conformes com a política;



12. A Criptografia de disco é uma medida de segurança técnica que protege as informações contra divulgação indesejada no caso de perda de um notebook por exemplo;
13. Vulnerabilidade é como se chama a causa potencial de um indecente indesejado;
14. Ameaças humanas não intencionais são, por exemplo a ameaça de um usuário deletar acidentalmente um documento;
15. Neutralizar o risco é a principal estratégia de risco com uma combinação de medidas de segurança preventivas, detectivas e repressivas;
16. É necessário testar um PCN Plano de Continuidade de Negócios com regularidade para certificar que as mudanças no negócio sejam refletidas no plano empresa;
17. Controle de acesso lógico é um exemplo de medida de segurança técnica;
18. Aplicação de patches imediatamente após sua disponibilização seria uma boa medida para evitar riscos;
19. É nos controles de segurança que são tomadas medidas para proteger um sistema de informação contra-ataques hackers;
20. Um alarme de fumaça é um tipo de medida de segurança Detectiva; e
21. Um sistema de chave codificada é um tipo de medida de segurança Preventiva;

3. Facilidade de implementar LGPD para empresas que já possuem um SGSI implementado ou em andamento

Empresas que seguem as melhores práticas de segurança da informação tem a possibilidade de realizar a adequação de forma menos traumática, uma vez que entendemos que o básico já está implementado e garantindo que os dados da empresa estão guardados e protegidos por meio de antivírus atualizados, firewall instalados, softwares atualizados com os paths de segurança, além de em alguns casos criptografia, que garante que somente as partes interessadas tenham acesso aos dados.

4. Prevenção

1. Elaborar sempre uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos;
2. Jamais utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários;
3. Utilizar uma senha diferente para cada serviço;
4. Alterar a senha com frequência;

5. Criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador; e
6. Utilizar o usuário Administrator (ou root) somente quando for estritamente necessário.

5. Conclusão

Nos últimos anos, por força de uma sociedade globalizada, as empresas, tem passado por transformações, cujo objetivo é torná-la aptas, comprometidas, eficaz e transparente no que tange as informações do consumidor. Neste ponto importante sinalizar que não só no ambiente privado, mas no público também se observa esta mudança positiva no tratamento de dados e informações.

Um passo importante é a otimização do processo de gestão no setor tecnológico, lembrando que o que inibe o processo de transformação é um fator bem comum como o atingimento de resultados.

É de fato que o tema Segurança da informação é uma desinformação de ordem aguda por parte da gestão, por causa do "tecniquez" bastante utilizado pelos profissionais de tecnologia.

E muito importante fazer cópias de segurança dos dados de um computador antes que ele apresente algum problema e seja necessário enviá-lo para manutenção. Uma cópia de Segurança dos dados antes de enviá-lo para a manutenção. Portanto, e muito importante que a empresa tenha disponível copias de segurança recentes de seus dados. Não se pode descartar a possibilidade no seu servidor, ter a infeliz surpresa que todos os seus dados foram apagados durante o processo algum processo e ou regra de negócio se existirem dados sensíveis armazenados em seu servidor, como declaração de campanhas, serviços, documentos e outras informações sigilosas, certificados digitais, entre outros.

6. REFERÊNCIAS

Livro; Praticando a Segurança da Informação, Edilson Fontes, CISM, CISA

Livro: A Segurança da Informação nas Empresas, Ampliando Horizontes além da Tecnologia, Geuorge Dawel

Livro: Safernet Dicas

Lei Geral de Proteção de Dados em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

CLASSIFICAÇÃO DESTE DOCUMENTO - PÚBLICO

Elaborador por:

Daniel Carnaúba
Coordenador Nacional do Comitê de Segurança da ANPPD
José Lopes Ramos
Coordenador Nacional do Comitê de Segurança da ANPPD
Luciano Piccolo
Vice-Diretor do Comitê de Segurança da ANPPD

Bruno Claus
Diretor do Comitê de Segurança

Davis Alves, Ph.D
Presidente da ANPPD

Revisado por:

Luciene Rosa
Coord. Comitê de Conteúdo da ANPPD

Anielle E Martinelli
Diretora do Comitê de Conteúdo da ANPPD

Data de publicação:
Junho de 2021