Segurança da Informação para Internet das Coisas (IoT)

> *Uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)*

Alunos

- Bruno Silveira de Moraes - 1461797
- Ericson Rogério Moreira - 1538663
- Matheus Ferreira Gomes - 1284983
- Pedro Paulo Rocha de Andrade - 1500076
- Raimundo Angeliano Gonçalves de Sousa - 1476646

Abstract - Resumo

O artigo abordar a segurança da informação sob os aspectos da lei brasileira que trata da proteção de dados dos usuários, ***Lei Geral de Proteção de Dados (LGPD)****, aplicada a* ***IoT****. Aspectos como coleta, transmissão e armazenamento de dados pessoais e sigilosos descritos da lei são desafios quando falamos de dispositivos restritos. Foram abordados os principais conceitos requeridos pela LGPD assim como a discussão sobre a aplicabilidade dos conceitos de segurança nestes dispositivos visando estar em conformidade com a LGPD.*

🔥 Introdução

- A internet tem realizado uma verdadeira revolução no cotidiano das pessoas
- Existem hoje cerca de 1,26 telefones celulares para cada habitante (IBGE 2017)
- Neste contexto apareceram tecnologias voltas para IoT
- Junto a esta gama de novas possibilidades e alternativas criadas pela IoT, surgiram também novos desafios.
- Lei Geral de Proteção de Dados - LGPD

🔥 Introdução

> *De acordo com a LGPD todo usuário tem direito a privacidade e a proteção dos dados pessoais diante de **empresas público/privadas** juridicamente constituídas, no entanto este texto desafia a IoT em nichos como por exemplo a automação residencial, onde dispositivos estariam coletando uma gama de informações pessoais, aplicando algoritmos de inteligência artificial e ainda cruzando estas informações através de Machine Learning (ML) afim de gerar estatísticas para detectar padrões e comportamentos.*

👊 Empresas Públicas Vs. Empresas Privadas

- Diferenças básicas

Privada	Público
Lucro	Impacto social
Pode tudo, menos o que é proibido por lei	Só pode fazer o que está na lei

- LIMPE da Adm pública

> art 37. CF/88: A administração pública **direta**, **indireta** ou **fundacional**, de qualquer dos Poderes da **União**, dos **Estados**, do **Distrito Federal** e dos **Municípios** obedecerá aos princípios de **Legalidade, Impessoalidade, Moralidade, Publicidade e Eficiência**...

📋 Organização do artigo

1. Apresentada a fundamentação teórica
2. Maiores detalhes da LGPD
3. Análise entre LGPD e o universo de IoT utilizando aspectos da SI
4. Conclusão

📌 Fundamentação teórica

- Segurança da Informação - **SI**
- Internet das coisas - **IoT**
- Lei Geral de Proteção de Dados Pessoais - **LGPD**

📌 Fundamentação teórica - Segurança da Informação (SI)

- **Confidencialidade:** garantir que somente quem deve acessar a informação de fato acesse a mesma.
- **Integridade:** garantir que a informação acessada realmente está correta, integra, não foi modificada ou alvo de fraude/falsificação.
- **Disponibilidade:** garantir que a informação possa ser obtida sempre que for necessário, assim, estando sempre disponível para quem necessite fazer uso da mesma.

📌 Fundamentação teórica - IoT

- **Dispositivos restritos:** grandes barreiras no contexto de recursos computacionais, como memória, processador, armazenamento, energia e a transmissão de dados.
- **Grande desafio:** além da funcionalidade do dispositivo, adicionar novos recursos para segurança normalmente é visto como oneroso ao projeto.
- **Legislação:** LGPD através de seu viés regulatório tem meios para exigir estes recursos ao projeto devido ao seu peso de lei, embora isto nada mude o fato de ainda ser um desafio no desenvolvimento de uma solução IoT.

🇧🇷 Lei Geral de Proteção de Dados Pessoais

Partes mais impotantes:

- Uso da Informação
- Acesso a Informação
- Titularidade e Responsabilidade
- Tratamento das Informações
- Divulgação de Incidentes

🇧🇷 Lei Geral de Proteção de Dados Pessoais

Uso da Informação

> Especificar para o usuário qual a finalidade da coleta de seus dados, além de ser transparente em relação ao tratamento dessas informações e adotar medidas que garantam sua segurança

🇧🇷 Lei Geral de Proteção de Dados Pessoais

Acesso a Informação

> O usuário deve ter acesso fácil às informações que estão sendo utilizadas sempre que desejar, podendo revogar seu consentimento de compartilhamento de dados posteriormente, sem maiores dificuldades

🇧🇷 Lei Geral de Proteção de Dados Pessoais

Titularidade e Responsabilidade

> O ”titular” dos dados é a pessoa a qual as informações se referem. No entanto, quando o titular concorda com o uso de suas informações, a empresa torna-se a responsável pela sua segurança e seu tratamento;

🇧🇷 Lei Geral de Proteção de Dados Pessoais

Tratamento das Informações

> O tratamento de dados deve ser finalizado quando o objetivo especificado anteriormente for alcançado (salvo casos específicos), quando as informações deixarem de ser necessárias ou quando o órgão regulador solicitar

🇧🇷 Lei Geral de Proteção de Dados Pessoais

Divulgação de Incidentes

> Qualquer vazamento ou falha de segurança que comprometa os dados de algum usuário devem ser relatados imediatamente às autoridades competentes, para que o problema seja resolvido.

👮 Segurança da Informação, LGPD e IoT

> *Objetivo de manter a privacidade dos dados de usuários através do texto trazido pela LGPD, verificam-se os desafio direcionados a aplicação dos mecanismos e tecnologias afim de atingir estes objetivos em dispositivos que por padrão possuem limitações físicas.*

Requisitos de segurança dos dados

- Coleta
- Transmissão
- Armazenamento

👮 SI, LGPD e IoT - Coleta

A LGPD especifica que:

> Qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos.

👮 SI, LGPD e IoT - Coleta

Regras de boas práticas e de governança que estabeleçam as condições de organização.

Estas práticas podem ter como referências a:

- **ISO 27000:** Sistema de Gestão de Segurança da Informação
- **ISO 27002:** Aborda os controles que podem ser aplicados afim de obter-se estas práticas.

👮 SI, LGPD e IoT - Coleta

Desta forma

Verifica-se a necessidade de:

- Mecanismos que indiquem ao usuário a finalidade da coleta de suas informações e ainda se
- O usuário autoriza a coleta destes dados.

💣 **Não sendo isto transparente, os dados ali coletados não poderão ser utilizados, pois isto contrariaria a LGPD.**

👮 SI, LGPD e IoT - Transmissão

Maior desafio

O maior desafio ocorre por conta dos dispositivos que apenas coletam algo e enviam utilizando tecnologia sem fio de baixo
consumo de energia.

Tais equipamentos **não** possuem recursos para executarem, por exemplo, a pilha **TCP/IP** e protocolos adaptados para internet das coisas na camada de aplicação.

👮 SI, LGPD e IoT - Transmissão

- Dispositivos restritos podem estar operando com **6lo** na camada de rede.
- Entretanto, na camada inferior, onde a comunicação sem fio pode ser utilizada de modo aberto traz um ambiente exposto a ataques, capturas de pacotes e a exploração de vulnerabilidades.

Nestes casos diversos ataques podem ser realizados contra as informações que trafegam entre as camadas **OSI**.

> **6Lo:** protocolo IPv6 modificado para uso em dispositivos de hardware restrito

👮 SI, LGPD e IoT - Transmissão

🪱 Tipos de Ataques a Transmissão

- **Injeção de mensagens:** Este tipo de ataque possui características iguais a famigerada exploração do **homem do meio**, imputando pacotes no protocolo da camada inferior.
- **Fragmentação de pacotes:** Dividir uma carga de dados em diversas partes menores. A remontagem de pacotes em dispositivos restritos pode gerar problemas como processamento extra e consequentemente um consumo maior de energia desligando este equipamento, além de também esquentar o dispositivo.

👮 SI, LGPD e IoT - Armazenamento

Desafio

Como os dados deverão ser protegidos, uma vez que não existe muitas possibilidades para alterações físicas destes dispositivos afim de empregar os requisitos vistos na LGPD?

Solução (?)

- Os dados armazenados podem ser passiveis de criptografia afim de aumentar a segurança dos usuários.
- **No entanto técnicas criptográficas poderiam consumir recursos altos para execução desta tarefa.**

👮 SI, LGPD e IoT - Armazenamento

Portanto

> É **indispensável** promover a proteção dos dados pessoais e sigilosos armazenado em IoT, **contudo** tratando-se de ambientes onde os recursos do hardware são **limitados**, **inviabilizasse** a utilização de **criptografias tradicionais**, onde a execução de algoritmos criptográficos teria um **alto custo**, degradando o desempenho computacional e o alto consumo de energia.

👮 Segurança no Armazenamento por meio da Criptografia

O que poderia ser feito?

Separar as informações importantes dos demais dados: classificação dos dados de acordo com o seu grau de valor ou significado que o conjunto de dados possui, onde estas informações consideradas sensíveis devem receber uma proteção criptográfica.

👮 Segurança no Armazenamento por meio da Criptografia

Entretanto

A **LGPD** relaciona **dados pessoais** e **dados sigilosos** como classificações que **necessitam de proteção**.

Alternativa

Deste modo podem ser utilizadas como alternativas para a **criptografia destes dados cifras de blocos leves**.

👮 Segurança no Armazenamento por meio da Criptografia

Cifras de blocos leves

> Cifras de blocos leves baseiam-se em funções de rede de Feistel e Substituição de Permuta. Este tipo de cifra, funciona com a execução de uma função de mapeamento de blocos possuindo n-bits de texto não cifrado para blocos de n-bits de texto cifrado, onde “n”é comprimento do bloco. Par metrizada por k-bits, a função da chave “K”contém o mesmo tamanho do bloco, impossibilitando a expansão dos dados.

👮 Segurança no Armazenamento por meio da Criptografia

Com o uso de cifras de blocos leves temos

- Redução de poder da criptografia
- Menor níveis de segurança em relação a algoritmos mais robustos como o Advanced Encryption Standard (AES)

Porem, atualmente, a maioria das informações são armazenadas em texto claro e a aplicação de uma criptografia de cifras de blocos leves já traria um ganho significativo a segurança

🏁 Conclusão

> *... são grandes os desafios do tema proposto devido a complexabilidade de aplicar requisitos de segurança a objetos com processamento, memoria, largura de banda e energia restritos. Ainda assim, independentemente do cenário de IoT que este estará compreendido, a aplicabilidade destes mecanismos e tecnologias descritas neste trabalho deverão empregar uma maior proteção aos usuários quanto a seus dados. Diminuindo assim as lacunas presentes entre a LGPD e a SI para dispositivos restritos.*

👍 Obrigado