

### **Exercícios- Segurança em IoT e Aspectos Legais**

- 1) Relativo as técnicas de proteção das informações, defina e apresente um exemplo de cada um destes conceitos aplicados em IoT. Lembre-se que estamos falando sobre IoT, dados, etc. em suas buscas.**

**a) Uso do protocolo TLS em dispositivos IoT**

**b) Uso de chips para criptografia**

**c) Tokenização**

É o procedimento no qual é feita a substituição de dados confidenciais por caracteres de identificação exclusivos que possuem todas as informações principais sobre os dados, assim, promovendo a maior segurança e confidencialidade.

**d) Anonimização**

Anonimização é o procedimento de descaracterizar a informação, fazendo que através da informação uma pessoa não possa ser identificada.

Uma forma de praticar a anonimização é a criptografia.

**e) Mascaramento**

Técnica faz o uso de ferramentas para substituir os dados reais por dados fictícios. Desta forma, os dados são de certa forma protegidos.

**f) Erasure Code (Reed-Solomon e Cauchy erasure code)**

- 2) Quais os seus aspectos legais e implicações no uso de IoT. Como a LGPD influencia no uso de IoT no Brasil**

Com a LGPD as empresas envolvidas direta ou indiretamente com IoT precisam se reenquadrar nas novas normas das leis. São diversas exigências que essas empresas devem atender, a maioria são requisitos para aumentar a transparência entre cidadãos e seus dados. Portanto, as empresas brasileiras precisam possibilitar a autorização de coleta de dados, entrega das informações completas mediante solicitação, direito de ser esquecido, criptografia das informações armazenadas e portabilidade dos dados de uma empresa à outra.

Os termos de prestação de serviços devem ser mais simples e específicos informando quais dados serão obtidos, o objetivo e o motivo da coleta de forma clara e de fácil entendimento.

- 3) Quais os problemas existentes ou futuros em relação a propriedade dos dados.**

Com a grande quantidade de dispositivos inteligentes ao nosso redor, será cada vez mais complexo limitar ou proibir a coleta e armazenamento de determinados dados. Outro problema atual é proibir o desvio de propósito, uma vez que, muitas empresas compartilham informações capturadas com outras empresas.

#### **4) Quais são os problemas relativos a privacidade e segurança?**

Quanto a privacidade, trata-se de um enorme desafio, pois segundo um levantamento da Cisco, em 2020 já teremos a marca de 50 bilhões de dispositivos conectados. Esses dispositivos estão em todos os lugares e até mesmo em nosso corpo. Garantir que cidadãos que não autorizam a coleta de seus dados realmente sejam atendidos, pode ser uma atividade muito complexa em cidades inteligentes. Quando uma pessoa pede para não ser identificada, a empresa responsável pela rede de câmeras e todas as outras organizações envolvidas no processo precisam ser capazes de excluir a trilha de dados referentes a ela e não a capturar mais. Isso não só é difícil de ser feito na prática, mas também tem implicações para manutenção da cidade – objetivo do projeto de IoT.

Referente à segurança de dados, muitos desenvolvedores ainda não possuem um consenso e conhecimento total do que é realmente necessário em termos de segurança. Portanto, deve-se apostar em testes de vulnerabilidade e conscientizar os usuários a sempre manterem seus dispositivos atualizados. Devido o grande volume de dados capturados, é necessária toda atenção na gestão de armazenamento, servidores e data centers. Todos devem ser capazes de acompanhar a complexidade e suportar o volume de dados, garantindo a segurança dos mesmos.