KORE

Guia Completo para Implementação de IoT

Sumário

66% das empresas alegaram que a execução de um projeto de IoT provou ser muito mais difícil do que o esperado[1].

Não é mais novidade que a Internet das Coisas (IoT) evoluiu para muito mais do que um termo tecnológico, afinal, de acordo com a GSMA, organização que representa as principais companhias de celular em todo o mundo, há previsão de que, até 2025[8], as receitas oriundas de oportunidades geradas em IoT cheguem ao patamar de $1,1 tri. Novas tecnologias relacionadas ao universo da IoT estão surgindo, transformando os modelos de negócios e possibilitando a criação de novos produtos e serviços em praticamente todos os setores. Ainda que muitas empresas de todos os segmentos e tamanhos já entendam a importância que a Internet das Coisas tem dentro de seus negócios, só 15% dos executivos estão satisfeitos com o projeto de IoT de sua empresa[1]. Para piorar ainda mais esse cenário, 66% das empresas alegaram que a execução de um projeto de IoT provou ser muito mais difícil do que o esperado[1]. Isso porque muitas delas têm dificuldades de avaliar e entender, com precisão, o que essas tecnologias IoT precisam, em termos de recursos, para executar suas implantações. Com o intuito de ajudar as empresas a se prepararem para um projeto de IoT de sucesso e superar desafios comuns do segmento, este eBook irá explorar sete etapas que devem ser levadas em conta para otimizar todo o processo – desde a implementação até a execução - e otimizar os resultados com o maior ROI possível.

Avaliação de Disponibilidade de IoT

Antes de iniciar o planejamento estratégico de um projeto de IoT, a primeira etapa que deve ser seguida é **avaliar a "disponibilidade para IoT"** da empresa. Isso pode ser feito a partir de uma avaliação da maturidade em relação à IoT com base em dois principais critérios - Capacidades Técnicas e Visão de IoT (conforme gráfico ao lado). Ao ter essas informações mapeadas, planejar, implementar e executar se tornam processos mais realistas e descomplicados.

A "Visão de IoT" mede o conhecimento de tecnologias de IoT e como, onde e quando aplicá-las a seus processos.

As principais áreas a serem consideradas ao avaliar este aspecto incluem:

- clareza no Retorno sobre o Investimento (ROI) para a implementação de acordo com as especificações necessárias
- conhecimento da aplicação aos negócios e das tecnologias envolvidas
- nível de adesão dos executivos para apoiar um projeto de IoT
- compreensão e/ou esclarecimento dos objetivos que a empresa busca alcançar com a IoT
- nível de agilidade para gerenciamento de mudança dentro da empresa

Conforme o gráfico de avaliação de disponibilidade de IoT abaixo, uma empresa típica iniciando sua jornada em IoT pode ser avaliada como "Básica" no eixo Visão de IoT, enquanto uma empresa que já implantou uma Prova de Conceito (PoC) pode ser avaliada como "Intermediária".

No outro eixo, a "Capacidades Técnicas" é uma avaliação do conhecimento técnico e recursos dentro da empresa para executar e implantar uma solução de IoT. Embora os cases de maior sucesso relacionados à IoT sejam focados nos modelos e resultados de negócios, sua natureza é totalmente tecnológica e, por isso, exige experiência ao ser implantada.

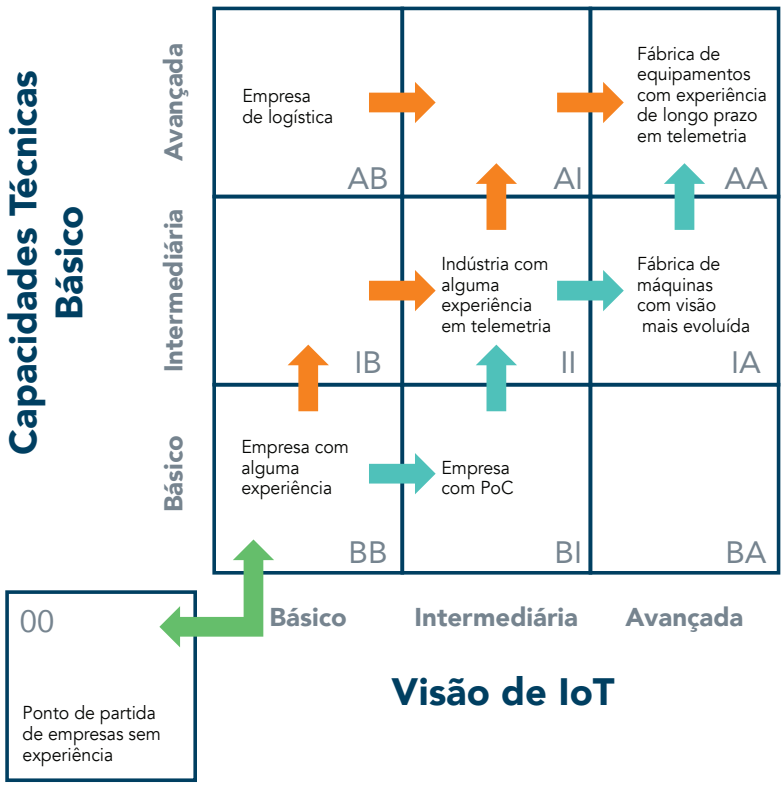
As principais áreas a serem consideradas ao avaliar este aspecto incluem:

- nível de experiência interna ou conjuntos de habilidades
- nível de tecnologia tradicional/recursos de TI
- parceiros de tecnologia

Conforme o gráfico, uma empresa iniciando com alguma experiência técnica pode ser avaliada como "Básica" nas Capacidades Técnicas, enquanto uma empresa com anos de tecnologia de logística pode ser avaliada como "Avançada".

Ao se realizar uma auditoria de disponibilidade de IoT, é importante levar em consideração todos os departamentos da empresa para ter uma visão holística e garantir resultados mais precisos.

Definindo metas, identificando obstáculos e compreendendo todo o potencial da IoT desde o início, sua empresa vai encurtar o caminho para a implementação de uma solução de IoT bem-sucedida.



Source: Gartner

Desenvolvimento de Estratégia para IoT

Ter uma estratégia de IoT é fundamental para definir, com precisão, como e quando as metas de negócios serão alcançadas ao longo da implementação da solução. Aproveitando os resultados da avaliação de disponibilidade de IoT como pano de fundo, a estratégia vai ser a responsável por trazer à tona todos os componentes necessários e cronogramas, **fornecendo a estrutura** ideal para direcionar os esforços dentro de seu modelo de negócios. Para aumentar as chances de sucesso, a estratégia de IoT deve ser completa, cobrindo todos os aspectos de processos de negócios, arquitetura, tecnologia, organização, design e governança - de ponta a ponta.

Cada estratégia de IoT deve começar com a identificação dos processos de negócios nos quais a solução de IoT pode ser aplicada para permitir a transformação e eficiência do seu funcionamento. Esta informação permite que as organizações entendam melhor onde esses processos ocorrem, quais sistemas são integrados aos processos e quão seguros esses processos devem ser, etc., orientando, assim, muitas das decisões estratégicas, tais como:

- Arquitetura de rede IoT
- Requisitos do dispositivo IoT
- Estratégia de aquisição e sourcing
- Escolha de parceiro IoT
- Solução(ões) piloto(s)
- Cronograma de implantação da solução
- Controle de IoT

Conforme os detalhes estratégicos de IoT começam a se encaixar, é fundamental estabelecer uma solução e controle para garantir que as etapas corretas progridam conforme o planejado e, em última análise, para atingir os objetivos que se espera de uma solução de IoT.

Cada estratégia de IoT deve começar com a identificação dos processos de negócios nos quais a solução de IoT pode ser aplicada para permitir a transformação e eficiência do seu funcionamento

Avaliação de Segurança em IoT

De acordo com um estudo da HP Security, até 90% dos dispositivos de IoT coleta algum tipo de informação pessoal. Soma-se a isso o fato de o número de violações de dados nos EUA ter aumentado 29% em 2017[3]. O fato é que **a segurança em IoT é fundamental para o sucesso** de qualquer projeto e o nível de medidas necessárias é diretamente proporcional à importância e sensibilidade dos dados e sistemas que a solução de IoT irá ter acesso. A segurança em IoT pode ser dividida em três principais "Camadas", e **as melhores práticas devem ser aplicadas em todas elas** para minimizar o risco:

I. Camada do Dispositivo

A camada do dispositivo na segurança em IoT está relacionada ao endpoint do dispositivo que se conecta e permite a coleta e transmissão de dados do elemento físico em uma solução de IoT. A fim de proteger adequadamente a solução IoT nesta camada, as empresas devem ter certeza de que tanto as propriedades físicas (invólucros de metal para prevenir roubo de chips, por exemplo), bem como propriedades de software (firmware, sistemas operacionais, aplicativos em execução, por exemplo) estão protegidos. Possíveis problemas de segurança devem ser considerados em relação às propriedades de software, visando garantir que o firmware seja atualizado de forma protegida contra acessos indesejados e mudanças de configuração. Do ponto de vista do software, inclusive, há uma série de medidas que as empresas podem tomar para ajudar a bloquear seus dispositivos. Alguns exemplos incluem:

- Uso de inicialização segura para garantir que apenas softwares verificados operem no dispositivo
- Autenticação e autorização do usuário para garantir controle de acesso
- Firmware seguro do dispositivo atualizado regularmente para bloquear redes não permitidas ou uso de aplicativos

É importante notar que alguns dispositivos IoT são pequenos em tamanho com memória e processamento limitados para oferecer suporte a recursos de segurança avançados.

Nesses casos, deve-se considerar a adoção de soluções de segurança em IoT baseadas em nuvem.

II. Camada de Comunicação

A camada de comunicação na segurança em IoT está relacionada à tecnologia de conectividade de rede que permite ao dispositivo enviar e receber dados. Para proteger adequadamente a camada de comunicações de uma solução IoT, as empresas devem considerar implementação de soluções focadas em infraestrutura e dados.

A segurança da infraestrutura de rede é normalmente verificada junto à conectividade de rede de provedor(es). Algumas questões críticas que as empresas devem levar aos provedores de conectividade durante o processo de escolha de parceiros incluem:

- Quais métodos de criptografia e firewall são usados pelo provedor de rede?
- Existe um Sistema de Prevenção de Intrusão (IPS)?
- Todos os servidores e componentes de rede estão atualizados com as versões mais recentes? Existe um processo em vigor para aplicar novos patches e atualizações de forma rápida?

Em relação às medidas de segurança dos dados em IoT, as melhores práticas recomendadas giram em torno de criptografia. É ela que protege os dados durante os acessos em redes diferentes, incluindo a Internet pública.

As soluções de Rede Privada Virtual (VPN), bem como soluções de acesso seguro de dados são alguns exemplos que garantem autenticidade e integridade dos dados transmitidos.

III. Camada de Aplicação

A camada de aplicativo na segurança da IoT está relacionada à proteção do aplicativo e dos bancos de dados que fazem parte da solução. Tal como acontece com as outras camadas, a segurança do aplicativo deve ser levada em conta em todo o processo de desenvolvimento para proteger componentes da web, móveis e nuvem. As melhores práticas para proteger este nível da solução IoT incluem:

- ferramentas de análise de código para inspecionar automaticamente código-fonte e identificar potenciais falhas de segurança
- atualizações de aplicativos automatizadas de forma eficiente para proteger contra novos ataques e outros riscos
- soluções de troca de chaves que permitam atualização das chaves de segurança do aplicativo IoT, mesmo em redes públicas
- soluções de registros de certificado que forneçam identificador único para cada dispositivo e realizem a verificação antes de habilitar acesso para sistemas/redes

Além disso, as empresas devem sempre ter à disposição estrutura para gerenciamento de ameaças, a fim de garantir a disponibilidade e integridade de suas soluções. Como o mundo da tecnologia está em constante evolução e os hackers estão constantemente melhorando seus ataques, é preciso garantir o entendimento e os padrões de comportamento de suas soluções de IoT para que possam rapidamente detectar e responder a possíveis anomalias. A melhor maneira de conseguir isso é implementando sistemas de monitoramento de ponta a ponta que notifiquem as equipes de segurança quando uma mudança no dispositivo ou no comportamento do aplicativo é detectada.

Escolha de Conectividade de Rede

Todas as soluções de IoT requerem conectividade de rede para funcionar. E, em se tratando de IoT, existe uma ampla gama de tecnologias de rede que facilitam a transferência de dados entre dispositivos e sistemas. Ao desenvolver uma nova solução IoT, é preciso escolher a opção que melhor funcione com as necessidades específicas de seu negócio. As tecnologias de rede podem ser categorizadas em três principais áreas - Rede de Área Pessoal (PAN - NFC e Bluetooth, por exemplo), Redes Locais (LAN - WiFi, ZigBee, por exemplo) e Rede de Longa Distância (WAN - celular e satélite, por exemplo) - todas elas variam muito em recursos relacionados à largura de banda, suporte à mobilidade, duração da bateria e rendimento, dentre outras características. Entre as tecnologias WAN, que representam a maior parte do mercado B2B de soluções IoT, a conectividade celular é a mais amplamente utilizada, com uma estimativa de 450 milhões de conexões ativas em 2017[4].

Como a última "evolução" da rede celular, o 4G LTE, está rapidamente se tornando a tecnologia preferida para implementações de IoT e a GSMA prevê que ela será responsável por 53% de conexões globais totais até 2025, contra apenas 29% em 2017[5].

Por outro lado, é preciso entender que o **4G LTE não é uma tecnologia única**, mas uma gama de tecnologias englobadas. Diferentes "categorias" de LTE foram projetadas para fins específicos, com níveis específicos de desempenho e requisitos de arquitetura de dispositivo também específicos. O aumento da adoção da 4G LTE para IoT se deve ao lançamento de **tecnologias novas e com baixo consumo de energia (LPWAN)**, criadas especificamente para apoiar o rápido crescimento da IoT em todo o mundo.

Projetadas para substituir redes celulares 2G e 3G para IoT, essas tecnologias LPWAN, como NB-IoT e LTE-M, são variantes do 4G LTE de menor potência e menor largura de banda que fornecem a longevidade das categorias LTE tradicionais (ou seja, Categoria 1 ou Cat-1, Categoria 4 ou Cat-4), a um custo muito mais baixo, com vida útil da bateria muito mais longa e consumo de energia muito menor. Dentre os benefícios das soluções IoT implantadas em redes LPWAN LTE, vale elencar:

- consumo de energia muito baixo com alguns aplicativos ostentando vida útil de bateria de 10 ou mais anos
- baixo custo do módulo de celular
- cobertura interna e externa em localizações até então inacessível
- tecnologia escalável com capacidade de suportar um grande número de dispositivos em uma ampla área geográfica
- conectividade segura de ponta a ponta e com suporte para autenticação apropriada para o aplicativo IoT
- solução de tecnologia de rede de longo prazo

Além das tecnologias 4G LTE de baixo consumo de energia, também há uma série de LPWAN proprietários de rede que operam de **forma não licenciada**, como Sigfox e LoRa. Ao usar o espectro licenciado, as operadoras devem se registrar e obter uma licença da ANATEL para possuir e operar com uma conectividade de 99,999% livre de interferências. O espectro não licenciado não requer nenhuma permissão ou licença especial para operar, mas se houver vários provedores operando na mesma área, conexões não licenciadas podem ficar sujeitas a interferência[6].

Antes do surgimento de NB-IoT e Cat-M1, as redes não licenciadas eram a única solução LPWAN para novas soluções de IoT que exigiam menor potência, maior alcance e maior vida útil da bateria. Embora o mercado esteja mudando para tecnologias de rede licenciadas, ainda existem determinadas regiões e casos de uso em que a conectividade não licenciada é uma solução adequada. A escolha para a rede depende dos requisitos exclusivos de cada empresa. Ao se escolher uma tecnologia de rede, os elementos-chave e especificações a serem consideradas são as seguintes:

	LTE Cat 6	LTE Cat 4	LTE Cat 1	LTE Cat-M1	NB-IoT	Sigfox	LoRa
Largura da Banda	40 MHz	20 MHz	20 MHz	1.4 MHz	200 kHz	100 Hz	125 kHz
Vida Útil da Bateria	Dias	Dias	5 anos	5-10 anos	10+ anos	10+ anos	10+ anos
Taxa de Transferência	DL: 300 Mbps UL: 50 Mbps	DL: 150 Mbps UL: 50 Mbps	DL: 10 Mbps UL: 5 Mbps	1 Mbps	250 kbps	100 bps	290bps - 50kbps
Taxa de Dados Bidirecional	Full Duplex	Full Duplex	Full Duplex	Full ou Half Duplex	Half Duplex	Não	Dependente de Classe
Segurança	3GPP (128-256bit)	3GPP (128-256bit)	3GPP (128-256bit)	3GPP (128-256bit)	3GPP (128-256bit)	16 bit	32 bit
Escalabilidade	Alta	Alta	Alta	Alta	Alta	Baixa	Média
Suporte de Mobilidade	Total	Total	Total	Conectado e Modo Ocioso	Modo Ocioso	Não	Sim
Suporte de Localização (LBS)	Sim	Sim	Sim	Necessita GPS	Necessita GPS	Não	Sim
Suporte de Voz	Sim	Sim	Sim	Sim	Não	Não	Não
Custo de Módulo	$50+	$40	$20-25	$10-20	$5-10	$2	$12
Uso de Caso Comuns	Aplicativos Médicos Virtuais	WAN Primário e WAN de backup para clínicas médica	Aplicativos para gerenciamento de diabetes	Sistema de Resposta de Emergência Pessoal (PERS)	Aplicativos para terceira idade		
Disponibilidade	**Disponível**	**Disponível**	**Disponível**	**Disponível**	**Disponível**	**Disponível**	**Disponível**

Escolha de Dispositivo IoT

O dispositivo IoT está diretamente relacionado à tecnologia envolvida por trás de qualquer solução IoT. Para escolher o dispositivo ideal para o seu negócio, é muito importante considerar, do ponto de visto da tecnologia, o suporte de rede, os aplicativos, os requisitos de segurança etc. Um passo fundamental para garantir esta combinação entre dispositivo e tecnologia é determinar o padrão de dispositivo, pois existem vários protocolos disponíveis no mercado que são projetados para suportar diferentes funcionalidades. Os padrões do dispositivo, por exemplo, podem variar do MQTT - que é um protocolo de mensagens simples projetado para dispositivos restritos com requisitos de baixa largura de banda em redes de alta latência-, para Lightweight M2M (LWM2M), que é um protocolo de gerenciamento de dispositivo projetado para controle remoto de gestão de redes de sensores, dispositivos M2M e habilitação de serviços. A escolha correta do padrão de dispositivo selecionado é extremamente importante para correlacionar com sua capacidade de suportar as aplicações e outras tecnologias desejadas.

Uma vez que os padrões de dispositivo são compreendidos e selecionados, **as empresas têm essencialmente duas opções:** comprar um dispositivo pronto para uso que atenda aos requisitos de sua solução de IoT ou construir um dispositivo proprietário do zero. Embora cada opção tenha vantagens distintas, é preciso entender que a decisão de construir um dispositivo personalizado consumirá mais tempo. Os recursos precisarão ser dedicados para abordar um número de itens que vão desde a avaliação e seleção do módulo, ao design industrial, à engenharia mecânica, à **certificação do dispositivo**, apenas para citar alguns.

Algumas considerações importantes ao tomar a decisão entre desenvolver ou adquirir de terceiros incluem:

- tamanho e escala da implantação da solução IoT
- aporte financeiro para despesas iniciais
- importância de ser uma propriedade intelectual
- importância de fortalecimento da marca
- requisitos para entrar no mercado
- disponibilidade de recursos técnicos para suporte
- necessidades potenciais de certificação de dispositivos

Normalmente, o desenvolvimento faz mais sentido para empresas que estão indo para o mercado como "empresas de IoT" e têm um núcleo de competência em tecnologia IoT. Esses tipos de negócios têm a expertise necessária para executar o desenvolvimento e, o peso de ter uma solução própria é mais importante que possíveis atrasos no lançamento ou impactos financeiros.

Por outro lado, comprar soluções já prontas faz mais sentido para empresas que estão usando soluções de IoT como produto de "consumo", que não estão sendo oferecidos aos usuários finais, mas sendo implementados para melhorar as operações internas ou processos. Esses tipos de empresas geralmente não têm recursos internos necessários para projetar e construir um dispositivo IoT do zero e, portanto, o investimento inicial em dispositivos prontos para uso vale mais a pena.

Independentemente da decisão, o mais importante para o dispositivo escolhido é suportar o aplicativo que irá alimentar a solução IoT da empresa, bem como fornecer níveis adequados de segurança com base nos resultados da avaliação de segurança IoT.

Gerenciamento do Ciclo de Vida da Solução IoT

Uma vez feita toda a avaliação e seleção da tecnologia, projeção, desenvolvimento e testes da solução IoT, é importante entender que o projeto ainda não está concluído, já que para o seu bom funcionamento é necessária uma implantação contínua, além de gestão operacional e esforços de sustentação e suporte para maximizar o ROI. Há uma série de processos que devem ser definidos para garantir que todo o ciclo de vida da solução IoT seja devidamente levado em consideração. Este momento pode ser dividido em três subáreas: implantação (também conhecida como logística direta), gestão operacional e sustentação e suporte (também conhecido como logística reversa). Para colocar a solução IoT no mercado de forma eficiente e completa, além de manter sua integridade e adaptá-la adequadamente a quaisquer problemas ou atualizações relacionadas à solução, as empresas devem se planejar para esses processos contínuos.

Implantação de solução IoT (Logística Direta)

Para evitar atrasos de lançamento no mercado ou dificuldades imprevistas na transição de uma solução IoT da Prova de Conceito (PoC) para a produção, as empresas devem considerar as seguintes características:

Gerenciamento operacional da solução IoT

Depois que uma solução de IoT é implementada, muitas empresas, especialmente aquelas novas no universo da IoT, podem não entender totalmente o nível de recursos necessários para oferecer suporte à implantação conforme a escala aumenta. Para evitar problemas de gerenciamento e escalabilidade, as empresas devem considerar as seguintes características:

Sustentação e suporte da solução IoT (Logística Reversa)

Até mesmo os projetos de IoT mais bem-sucedidos estão sujeitos a problemas que podem estar além do controle da empresa (desligamento da rede 2G, por exemplo) e requerem adaptação contínua e suporte para manter seu funcionamento. Para minimizar esses impactos, é preciso considerar as seguintes características:

A decisão entre optar por gerenciar esses processos internamente ou encontrar um parceiro que vá fornecer serviços de gerenciamento de ciclo de vida de endpoint, dependerá do nível de experiência em IoT da sua empresa, data limite para lançamento de produto e disponibilidade de recursos, conforme endereçado na fase da estratégia de IoT .

Otimização da Solução de IoT

Assim que uma solução de IoT for implementada, é necessário monitorar continuamente a sua eficácia para gerar maior valor e de forma mais rápida para os seus clientes. É graças a este monitoramento contínuo e às análises de rede, de dispositivo e de aplicativos de desempenho que são extraídas as informações básicas para preparar e priorizar atualizações de soluções IoT. Por exemplo - se um dispositivo IoT específico está apresentando baixo desempenho de rede, o monitoramento das redes será o responsável por apontar melhor se o problema é resultado de interrupção da operadora ou da cobertura, ou se o problema está no próprio dispositivo.

As empresas também podem aumentar a eficácia de sua solução IoT e criar valor agregado ao alavancar os dados coletados por meio de seus dispositivos. Um estudo recente estima que a quantidade de dados atualmente sendo processados no universo digital poderia ser representada por 254.276 km de iPads Air de 128 GB empilhados - ou seja, aproximadamente dois terços do caminho da Terra para a lua7. Os dados coletados via soluções de IoT são indiscutivelmente o maior diferencial da Internet das Coisas, fornecendo grandes quantidades de informações, que até então eram indisponíveis.

Levando a análise de dados além da funcionalidade da solução IoT, as empresas podem aproveitar os dados coletados para extrair inteligência de negócios, **melhorar a eficiência operacional** ou até mesmo **introduzir novos serviços** que são relevantes ou paralelos às ofertas atuais. Por exemplo, um fabricante de dispositivos médicos de aparelhos de ressonância magnética que implementou uma solução IoT para monitorar e rastrear o uso desses dispositivos durante os exames, agora pode estender a solução para o mercado, permitindo que hospitais paguem pelas máquinas em um modelo OpEx "por imagem", sem a necessidade de um grande investimento. Este modelo "As-A-Service" focado em dados de negócios de IoT, permite que o fabricante penetre em novos mercados, atendendo a fornecedores com orçamentos menores. Outro exemplo pode ser uma empresa que implementou um aplicativo de rastreamento de frota habilitado para IoT para simplesmente rastrear a localização de um veículo, mas aproveitou a análise de dados para monitorar o comportamento do motorista, aumentar a eficiência do combustível e implementar práticas de manutenção preventiva.

Conclusão e Próximos Passos

O ecossistema da IoT é altamente complexo, e cada jornada para a implementação de solução IoT será exclusiva para os processos de negócios e metas relacionadas à IoT de cada empresa. Dito isto, é importante ter em mente que as empresas, mesmo as mais experientes, não devem tentar "andar sozinhas" nesta jornada. De acordo como uma pesquisa da Cisco, descobriu-se que as companhias mais bem-sucedidas na implementação de soluções IoT envolvem seus parceiros de ecossistemas em cada estágio de planejamento, desenvolvimento, implantação da solução e gestão. O parceiro de IoT ideal deve ser um consultor confiável, com profunda experiência em IoT e agnóstico em relação à priorização de tecnologia. Ao selecionar o parceiro que fornece soluções e serviços abrangendo todo o processo de implementação de IoT (ou seja, serviços consultivos, dispositivos IoT e / ou serviços de certificação de dispositivos, conectividade de rede, ciclo de vida de endpoint, serviços de gestão, etc.), as empresas conseguem reduzir riscos e evitar desafios desnecessários, além de se beneficiarem a partir de uma solução de IoT otimizada e simplificada.

Sobre a KORE

A KORE é líder pioneira e consultora de confiança que ajuda a entregar negócios transformadores de soluções IoT. Nós ajudamos empresas de todos os tamanhos a navegarem nas complexidades de IoT e melhorar a sua execução para que possam se concentrar em resultados operacionais e de negócios. Nossa experiência em IoT, de alcance global, aliada à independência e agilidade de implantação, aceleram e melhoram o retorno de nossos clientes sobre cada centavo investido em IoT.

Saiba como a KORE pode simplificar a complexidade da IoT para garantir uma implementação bem-sucedida.

Fontes

1. https://newsroom.cisco.com/press-release-content?articleId=1847422
2. https://www.gartner.com/imagesrv/research/iot/pdf/iot-275309.pdf
3. https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881
4. https://www.statista.com/statistics/671216/global-m2m-and-nb-iot-connections-forecast/
5. https://www.gsma.com/mobileeconomy/#techmigration
6. https://blog.oneringnetworks.com/the-difference-between-licensed-v-unlicensed-spectrum-for-fixed-wireless
7. https://www.versatek.com/blog/how-much-data-will-the-internet-of-things-iot-generate-by-2020/
8. http://www.itpro.co.uk/internet-of-things-iot/31218/iot-revenue-opportunity-to-exceed-1-trillion-by-2025