**Segurança de internet 5G: Como preparar a segurança que enfrentará a onda de modernização do IoT.**

**Resumo**

A Internet 5G é uma tecnologia de comunicação móvel de nova geração que está sendo estudada pelas diversas países principais como EUA, Japão, China e Coreia do Sul com objetivo de inicializar a utilização em 2020, Ao enfrentar que daqui a 10 anos, os transmissões de dados que as pessoas irão utilizar serão 10 vezes ou até 1000 vezes maior do que atualmente com a evolução de IoT (Internet of Things). Para que haja uma capacidade de manter esta explosão de transmissões e processar com velocidade eficaz, o mercado necessita de um sistema que possibilita armazenar os dados muito maior e uma segurança mais robusta para controlar os riscos que serão causados na sociedade. Então o objetivo deste trabalho é demonstrar a evolução da tecnologia 5G, e como se proteger com o aumento de tráfegos de conexões que ocorrerá com IoT.

**Referencial Teórico**

Uma das características principais da internet 5G é a Computação Nuvem, as transações de dados será realizado via Nuvens e

No artigo “**Segurança em Cloud Computing (2015)**”, as autoras apontam as características de gestão de riscos e governança da segurança de informação, ou seja, descreve as formas de como proteger o ambiente nuvem, já que a internet 5G propôs a utilizadação de cloud computing para realizar as tranmissões de dados dos diversos dispositivos IoT (Internet of Things). Dentro do contexto, há modelos de implantação para computação em nuvem, detallhando os princípios de segurança de Segurança para ambiente nuvem e seus modelos de serviços como SaaS (Software as a Service ), IaaS (Infrastructure as a Service ) e PaaS (Platform as a Service).

A tabela abaixo mostra seus principais pilares para segurança de informação e seus respectivos características :

| Princípios da Segurança | Característica |
| --- | --- |
| Integridade | Garantir o padrão da informação estabelecida pelo proprietário da informação. |
| Confidencialidade | Garantir a limitação de acessos à informação aos usuários indevidos. |
| Disponibilidade | Garantir a informação que sempre seja disponível para usuários legalizados. |
| Autenticidade | Garantir a autenticação à acessos as informações. |
| Não-repúdio | Garantir que o usuário não consiga negar a transação feita anteriormente. |
| Conformidade | Garantir que os sistemas estão sob leis, normas e regulamentos. |

Conceitos de segurança.

Fonte: : http://www.ciencianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf”

Para que possa implementar a nuvem, segundo a **Castro e Sousa** "Nuvem é preciso estabelecer requisitos contratuais adequados e adotar tecnologias capazes de coletar os dados necessários para informar as decisões de informação de risco (por exemplo, o uso da informação, acesso, controles de segurança, localização, etc.)..”, isso significa que, os dispositivos que possuem os sistemas, ou seja, a IoT que terá seus diversos sistemas diferentes precisará padronizar o seu modelo, para que não necessite instalar softwares de segurança para cada dispositivos de internet das coisas.

**Referências Bibliográficas**

Castro, R. & Sousa, V. P. (2015)”Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança”, Disponível em < <http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud.pdf> >, acesso em 16/05/2016.

# Euobserver (2015) “Security and privacy challenges for next generation 5G technologies “ Disponível em < <https://euobserver.com/stakeholders/131843> >, acesso em 15/05/2016.

Huawei (2015) “5G Security: Forward Thinking Huawei White Paper”, Disponível em < [http://www.huawei.com/minisite/5g/img/5G\_Security\_Whitepaper\_en.pdf](http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf%20) >, acesso em 15/05/2016.

Mendes, Jose R. (2014) ”5G: A QUINTA GERAÇÃO”, Disponível em < <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3866/1/CT_TELEINFO_2013_1_06.pdf> >, acesso em 15/05/2016.