**FAETERJ – RIO**

ARTHUR LOURENÇO MACHADO

JOÃO PEDRO DE FERREIRA OLIVEIRA FERREIRA

RODRIGO RODRIGUES FERREIRA MAGGESSI CASTRO

**TRABALHO FINAL**

RELATÓRIO TÉCNICO

RIO DE JANEIRO

2022

ARTHUR LOURENÇO MACHADO - 1920478300009

JOÃO PEDRO DE FERREIRA OLIVEIRA FERREIRA - 2010478300069

RODRIGO RODRIGUES FERREIRA MAGGESSI CASTRO - 1910478300034

**TRABALHO FINAL**

RELATÓRIO TÉCNICO

Trabalho de Segurança da Informação para a composição de nota da AV2 apresentado à FAETERJ-RIO.

Professora: Maria Cláudia Roenick.

**RIO DE JANEIRO**

**2022**

SUMÁRIO

[1. INTRODUÇÃO 4](#_Toc101884152)

[2. CRIPTOGRAFIA DIFFIE-HELLMAN 5](#_Toc101884153)

[3. FUNCIONAMENTO 6](#_Toc101884154)

[4. OPERAÇÃO COM MAIS DE DUAS PARTES 8](#_Toc101884155)

[5. AUTENTICAÇÃO E A TROCA DE CHAVES DIFFIE-HELLMAN 8](#_Toc101884156)

[6. VARIAÇÕES DA TROCA DE CHAVES E SUAS APLICAÇÕES 9](#_Toc101884157)

[Elliptic-curve Diffie-Hellman 9](#_Toc101884158)

[TLS 10](#_Toc101884159)

[ElGamal 10](#_Toc101884160)

[STS 11](#_Toc101884161)

[7. VANTAGENS E DESVANTAGENS DO ALGORITMO DIFFIE-HELLMAN 11](#_Toc101884162)

[8. CONCLUSÃO 12](#_Toc101884163)

[9. REFERÊNCIAS 13](#_Toc101884164)

1. INTRODUÇÃO

**Título:** Criptografia Diffie-Hellman

**Objetivo Geral:** A troca de chaves Diffie-Hellman é um método de troca segura de chaves criptográficas em um canal público e foi um dos primeiros protocolos de chave pública concebidos por Ralph Merkle e nomeados em homenagem a Whitfield Diffie e Martin Hellman. Será apresentado nesse trabalho toda a complexidade desse método, seu funcionamento, suas variações, vantagens e desvantagens.

2. FRAMEWORK

Levando em consideração a missão que um centro hospitalar possui, o framework escolhido pelo grupo foi o ITIL (Information Technology Infrastructure Library). Por se focar tanto em gestão de tecnologia como em infraestrutura, acreditamos que irá nos permitir lidar com quaisquer variáveis na implementação do projeto.

O ITIL possui 2 objetivos principais:

• Foco interno, preza pela gestão de processos de forma eficaz;

• Foco externo, preza pela qualidade da experiência dos clientes.

Além disso, o ITIL é um dos frameworks mais populares, também é aplicado em empresas de diversos portes em todo o mundo. Isso facilita tanto o acesso a material quanto a análise de cases. Dentre os principais motivos que levou nossa equipe a tal escolha, destaca-se a flexibilidade que o framework preconiza, pois não é um método rígido - e sim, em linhas gerais, um apanhado de orientações e melhores práticas. Nossa empresa pode implementar apenas parte das práticas delineadas na documentação e ainda assim alcançar os objetivos esperados a médio e longo prazo.

Alguns outros pontos que podem ser explorados através da orientação do framework para aumento de eficiência e resultados que também valem ser citados, são:

• Uma melhora significativa no desempenho dos funcionários: Ao adotar o ITIL, os processos e atividades dos profissionais que trabalharão com esse modelo são mais organizados e há definições mais claras sobre os papéis e a atuação de toda a equipe.

• Redução de gastos: Com boas práticas é possível detectar falhas e erros com antecedência e minimizar os prejuízos em curto, médio e longo prazo. Assim, não é preciso adotar medidas urgentes (que geralmente são caras) para consertar problemas dessa ordem.

• Maior satisfação do cliente: Essa metodologia reduz riscos e erros, e gera menos incidentes (como a paralisação de serviços). Portanto, otimiza a experiência do cliente, visto que este recebe um serviço mais estável e seguro. Promovendo a confiança do consumidor em relação à empresa e, assim, o relacionamento do cliente-companhia é fortalecido, o que, por sua vez, contribui para o processo de fidelização.

**3. OBJETIVOS**

Um dos nossos primeiros objetivos é a formação contínua dos profissionais do centro hospitalar. Afinal, a formação de um profissional não pode se restringir somente ao momento em que ele chega na empresa, é importante capacitá-lo ao longo de todo período em que este faz parte do quadro. Além dos objetivos óbvios que se podem obter com esta prática, a formação contínua serve também para que a empresa possa estar constantemente reafirmando seus valores, atualizando conhecimento, investindo em seus membros e lembrando a estes profissionais que há um benefício mútuo nessa iniciativa.

Para este centro hospitalar, planeja-se a instauração de um processo de formação contínua através da construção de um setor responsável única e exclusivamente pela parte educacional da empresa. Para suportar este setor, será criada uma plataforma de educação, onde haverá formações para diferentes fins, desde as mais abrangentes até as mais específicas. Nesta plataforma, cada gestor poderá acompanhar o progresso e desempenho de sua equipe, definir trilhas de aprendizagem além de agendar e acompanhar o resultado de avaliações.

O quadro deve estar com os conhecimentos regulatórios sempre atualizados e dentro do que se espera para o segmento. Além disso haverá o controle do crescimento e engajamento com a plataforma de cada equipe através de um banco que armazena as horas investidas em paralelo com os cursos concluídos e certificados emitidos.

Sempre que se fala em educação, se fala em longo prazo. Muito além do desempenho dos alunos — que serão metrificados através de relatórios periódicos — espera-se que a cultura do centro hospitalar mude. O objetivo é ter profissionais mais motivados e capacitados, sempre dispostos a passar conhecimento adiante com uma postura colaborativa.

Nosso segundo objetivo é especificamente focado na segurança da informação e na investigação e desenvolvimento científico nas áreas das ciências da saúde.

Técnicas e conceitos estão em constante movimento de reciclagem e aprimoramento. Por conta disso, não tirar proveito dos dados gerados a partir do tratamento de uma quantidade considerável de pacientes por ano (dado o porte do centro hospitalar) poderia se chamar de desperdício. Principalmente quando a proposta de gerar conhecimento em torno desta área não só é valorizada economicamente como também traz benefícios em nível humanitário.

Como passo inicial é necessário desenvolver uma forma coletar todos os dados de pacientes, tratamentos, procedimentos, entre diversas outras coisas, e em seguida, injetá-los em um data lake onde eles futuramente seriam tratados por profissionais especializados para que se iniciasse o processo de análise e pesquisa. Também vale ressaltar que estes dados são extremamente sensíveis por envolver terceiros que buscam o tratamento no hospital. Portanto é necessário que haja responsabilidade e segurança. Tanto através de normas e boas práticas no tratamento e interação com os mesmos como também um plano de segurança para minimizar os riscos de vazamentos.

O progresso da iniciativa seria medido através de resultados obtidos no futuro com os dados fornecidos ou até mesmo com o fato dessas informações poderem colaborar com iniciativas alheias ao hospital (após uma minuciosa análise sobre a segurança e permissão dessa troca de informações). Um exemplo de esforços conjuntos para sustentar esse caso seria o compartilhamento de dados de pacientes de Covid-19 com a finalidade de buscar um tratamento mais adequado/eficiente.

O resultado concreto esperado é a produção de conhecimento e um banco de dados seguro caso seja necessário referenciar casos anteriores para o tratamento de pacientes futuros. O resultado ideal seria contribuir para, ou por conta própria, o aprimoramento ou desenvolvimento do tratamento de alguma(s) enfermidade(s).

8. CONCLUSÃO

Devido às suas vantagens, Diffie-Hellman provou ser um sistema útil de troca de chaves. Embora, seja realmente difícil de ser quebrado e um intruso espionar a rede, descriptografar os dados e obter as chaves, isso ainda é possível se os números gerados não forem inteiramente aleatórios e grandes o suficiente para impossibilitar a quebra por força bruta. Quando aliadas a outras técnicas de criptografia e segurança, Diffie-Hellman, se mostra bastante eficiente complementando um esquema de segurança de alta confiança.

9. REFERÊNCIAS

**- “Troca de chaves de Diffie–Hellman”. Wikipédia. Disponível em: <https://pt.wikipedia.org/wiki/Troca\_de\_chaves\_de\_Diffie%E2%80%93Hellman>. Acesso em: 21, abril de 2022.**

**- “Troca de chave Diffie-Hellman”. Stringfixer. Disponível em: <https://stringfixer.com/pt/Diffie-Hellman>. Acesso em: 21, abril de 2022.**

**- Ferreira, Thiago. “Algoritmo Diffie-Hellman”. iMasters, 2007. Disponível em: <** **https://imasters.com.br/back-end/algoritmo-diffie-hellman>. Acesso em: 20, abril de 2022.**

**- Marques, Thiago. “Criptografia: Abordagem histórica, protocolo Diffie-Hellman e aplicação em sala de aula”. Repositório UFPB, 2013. Disponível em: <** **https://repositorio.ufpb.br/jspui/bitstream/tede/7545/5/arquivototal.pdf >. Acesso em: 23, abril de 2022.**

**- “Algoritmo de Troca de Chaves de Diffie Hellman”. Education-wiki. Disponível em: <** **https://pt.education-wiki.com/4355142-diffie-hellman-key-exchange-algorithm>. Acesso em: 23, abril de 2022.**