FACULDADE ANHANGUERA

TECNÓLOGO CIBERSEGURANÇA

NOME:TASSIANA MILKA FONTANA SOARES

ROTERIO DE AULA PRÁTICA

CAMPINAS-SP

2025

NOME:TASSIANA MILKA FONTANA SOARES

ROTERIO DE AULA PRÁTICA

Relatório da aula prática de realizar exercícios proposto sobre Função Hash e os Processos e Políticas de segurança.

CAMPINAS-SP

2025

SUMÁRIO

Função Hash

1.Introdução

Função de Hash foi criado na finalidade de descrever pela mensagem do correio eletrônico, uma senha, chave criptográfica e arquivo pela sequência de bits que retorna informações pelos identificadores únicos para os valores.

Para realizar a entrada e saída da exibição do resultado possuí alguns sites que auxilia no desenvolvimento um deles é SHA-256 Online Hash Generator Online que o usuário pode informar e concluir com retorno.

2.Objetivos

Explicar sobre Função Hash de como é importante e juntamente na realização do exemplo descritivo.

3.Métodos

- Descrever os requisitos proposto de Hash sobre a finalidade até criação de exemplos para entender.

3.1. Introdução aos Conceitos

- A seguir possuí sobre as principais partes que define a Função Hash.

3.1.1. Função de Hash

Função de Hash é definido como um algortimo para comprimento de dados variável fixo com nomes de retorno dos códigos hash, somas hash (hash sums), checksums ou simplesmente hashes.

Na finalidade de resumir dados, verificar a integridade de arquivos para segurança de senhas e informações armazenadas estabelecendo a autenticação dos dados de maneira criptográfica para garantir a comunicação pela examinação dos has criados antes e depois da transmissão de dados dos dois Hash idênticos na transmissão.

Pelas suas propriedades a Função Hash contém em divisão de grupos para compreender cada uma delas:

- Resistência à pré-imagem: Produzir um valor z para encontrar uma entrada x que contenha o Hash do valor z para proteger;

- Resistência à segunda pré-imagem: Protege contra o ataque que contenha o valor de entrada e o substitui uma entrada com mensagem válida;

- Resistência à colisão: Contém um valor fixo de saída na resistência à segunda pre-imagem.

3.1.2. Tipos de Ataques às Funções Hash

- Ataque de Colisão: Conhecido como SHA-1 que interrompe a Função Hash pelas entradas personalizadas;

- Ataque de Pré-Imagem: Acontece quando invasor tenta encontrar uma mensagem do valor de Hash;

- Ataque de Pós-Imagem: O momento em que o atacante tenta encontrar uma mensagem diferente para produzir o mesmo valor de Hash da mensagem original.

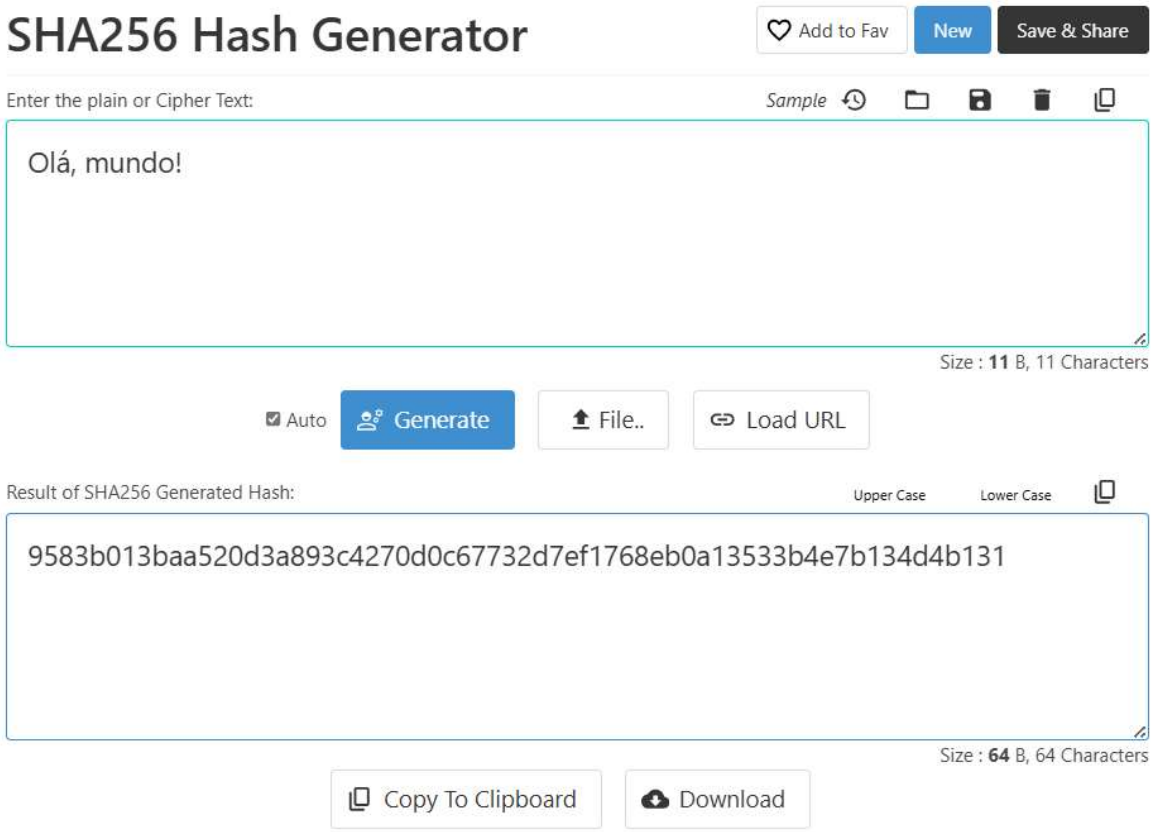
3.1.3. Estrutura de um Código Hash

- A seguir vai demonstrar a estrutura do código em linha contendo números e letras.

3.1.3.1. Exemplos

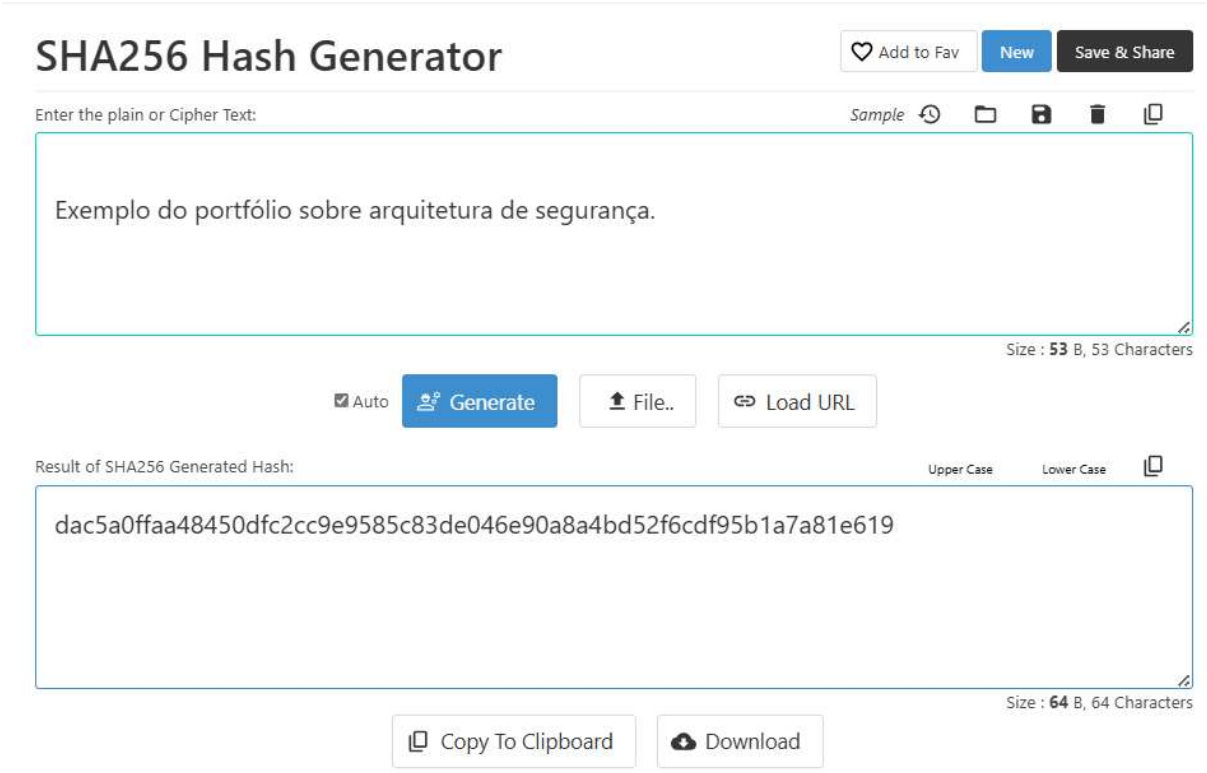
- Os dois exemplos NA FIGURA 1 e 2 são pequenas frases descrita e demonstrando a conversão para código de Hash.

FIGURA 1:Primeira mensagem



Fonte: autoria própria

FIGURA 2:Segunda mensagem



Fonte: autoria própria

3.1.4. Funções Hash Aprimoram a Segurança

A Função Hash contém a facilidade de proteger segurança dos dados na utilização de assinaturas digitais para verificar a autenticidade e a integridade de documentos digitais pela criptografia usando a chave privada.

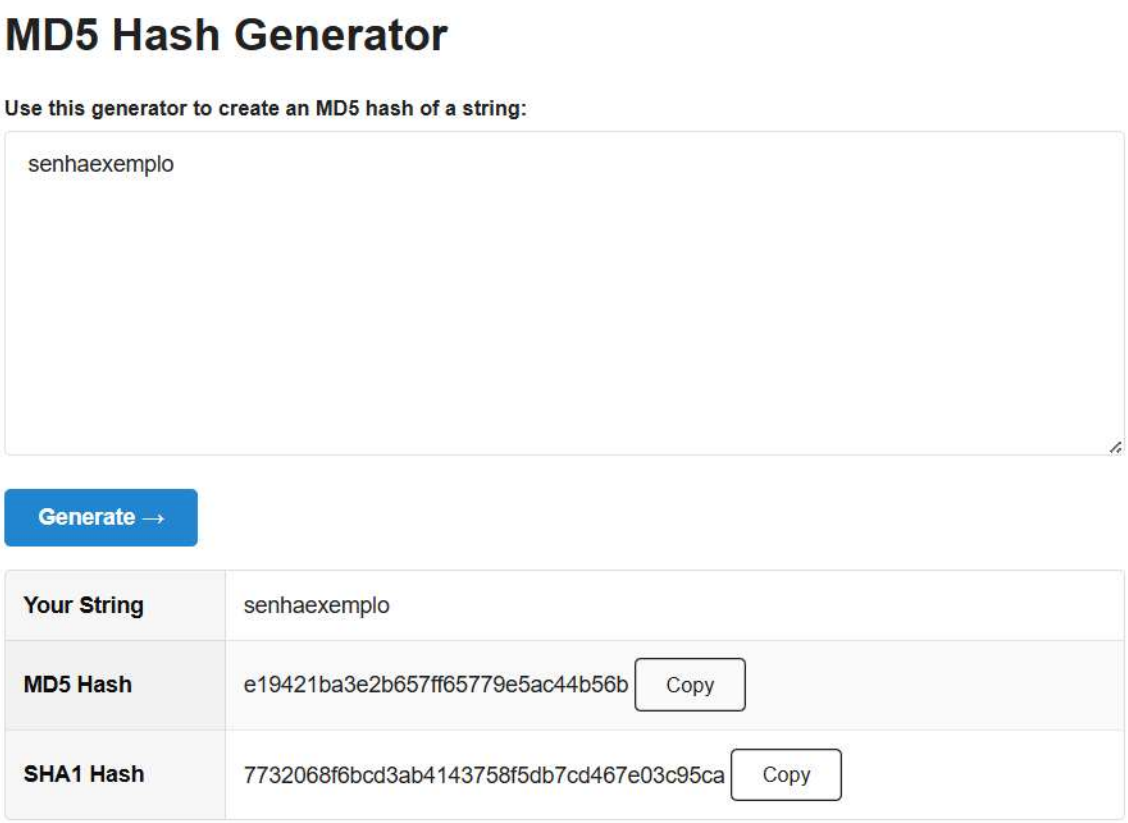
Possuí protocolos para armazenamento seguro de senhas e certificados digitais que armazena as senhas reais dos seus valores de Hash que o usuário insira a senha

durante a autenticação, o valor é resultante do valor de Hash armazenado e o valor ser iguais é considerado válido sem expor a senha real para impedir um invasor acessar as senhas originais.

3.1.4.1. Exemplo de senha

- Um exemplo na FIGURA 3 de senha criada como “senhaexemplo” na finalidade de converter para MD5 Hash e SHA1 Hash.

FIGURA 3:Senha



Fonte: autoria própria

4.Resultado

Durante a realização obteve o entendimento da importância sobre Função Hash na tecnologia quando referimos a segurança de dados dos arquivos ou senhas e foi utilizado um gerador online de uma conversão para código de Hash conforme os exemplos descritos.

5.Conclusão

A Função Hash é algo muito utilizado para segurança desde das propriedades, integração para proteger dos ataques que um invasor pode realizar pelos arquivos ou senhas de usuário.

Uma funcionalidade positiva para descrever e obter o resultado confidencial da mensagem em letras e números pelos geradores de códigos Hash da sequência de bits pelos identificadores dos valores.

Para isso, possuí alguns sites que auxilia na criação e exibe conforme descrito pelo usuário ou selecionar arquivo em formato txt.

6. Referências Bibliográficas

WIKIPEDIA. Função hash. Disponível em:https://pt.wikipedia.org/wiki/Fun%C3%A7%C3%A3o_hash . Acesso em:15/03/2025.

KASPERSKY.Brian Donohue.Hash:o que são e como funcionam. Disponível em:https://www.kaspersky.com.br/blog/hash-o-que-sao-e-como-funcionam/2773/ . Acesso em:15/03/2025.

MEDIUM.Fernado Souza. Função hash ou hashing.Disponível em:https://medium.com/prognosys/fun%C3%A7%C3%B5es-hash-ou-hashing-b2c90ac5c398 . Acesso em:15/03/2025.

SEGINFO. Ataques de colisão SHA-1 agora são realmente práticos e criptografia se torna um perigo iminente. Disponível em: https://seginfo.com.br/2019/05/20/ataques-de-colisao-sha-1-agora-sao-realmente-praticos-e-criptografia-se-torna-um-perigo-iminente/ . Acesso em:15/03/2025.

BRUNORIBAS.FUNÇÃO HASH CRIPTOGRAFADA (MD5, E A FAMÍLIA SHA. Muriel Mazzetto. Disponível em: https://www.brunoribas.com.br/sc/2016-1/cripto/muriel-hash.pdf?form=MG0AV3 . Acesso em:15/03/2025.

EITCA.Como uma função de hash garante a integridade e a segurança dos dados? -Academia EITCA.Disponível em:https://pt.eitca.org/c%C3%ADber-seguran%C3%A7a/eitc-%C3%A9-acc-criptografia-cl%C3%A1ssica-avan%C3%A7ada/fun%C3%A7%C3%B5es-de-hash/introdu%C3%A7%C3%A3o-%C3%A0s-fun%C3%A7%C3%B5es-hash/revis%C3%A3o-de-exame-introdu%C3%A7%C3%A3o-%C3%A0s-fun%C3%A7%C3%B5es-de-hash/como-uma-fun%C3%A7%C3%A3o-de-hash-garante-a-integridade-e-a-seguran%C3%A7a-dos-dados/ . Acesso em:15/03/2025.

Processos e Políticas de Segurança

1.Introdução

Os Processos e Políticas de Segurança organizações foram criados na finalidade principal de regras, diretriz das decisões e as práticas operacionais que refere sobre informações, instalações e equipamentos.

Na utilização das normas manter o ambiente profissional mais qualificado de forma positiva deste da criptografia, gestão de senhas e compartilhamento seguro de dados.

Para isso, deve conter ferramentas virtuais, documentações, comunicações de feedback e revisões que constroem uma união de um bom andamento dos funcionários ou parceiras com outras empresas.

2.Objetivos

Descrever sobre a ideia da criação de uma empresa fictícia desde dos risco até a proposta de solução.

3.Métodos

- A seguir vai ser descrito sobre uma empresa fictícia e todas etapas de problemas e como pode ser resolvido para o aumento de confiança e segurança.

3.1. Identificação de Riscos

Para realização obtive a escolha de uma empresa fictícia com o nome tech/tecnologia que a principal finalidade é elaboração de banco de dado para bancos nacionais e mundiais que todos os minutos investem, ou seja, bancos de empreendedores e abrange mais de 60 milhões de cliente pelo mundo os seus riscos são:

- Ataque a rede: Necessitam de uma segurança elaborada, pois o já conteve três vezes invasores o acesso a rede da empresa;

- Banco de dado sem manutenção ativa: Como os banco de dados é o ponto principal para empresa continuar o seu processo de trabalho não possuí uma manutenção semanal e com medo de perder os dados acabam não realizando uma melhor forma de manter em segurança e a facilidade do invasor é maior, pois essa situação já gerou perda de 12 milhões da confiança com cliente e necessitaram pagar aonde entraram em dívida;

- Senhas fracas: Seus e-mails, arquivos de senha e rede são senhas fracas com poucos caracteres e facilidade para o acesso de invasores que descobriu pelo ataque de rede e acabam mudando, mas não utilizam uma senha forte para manter mais seguros as redes sociais da empresa e meio de comunicação;

- Site sem certificado válido: Um do principal acesso da empresa com os clientes é o site que está incorreto a funcionalidade sem um certificado válido que contém mais segurança e com isso já foi roubado uma informação pelo chat que aciona a empresa para conversa sobre uma parceria com outra em

um trabalho que eles dividiriam o trabalho, mas acabou perdendo a confiança e não conseguiram avançar. Nesse caso, precisam de uma estratégia para serem reconhecidos novamente.

3.2. Interpretação de Políticas de Segurança

3.2.1. Política de Segura

Para interpretação de Políticas de Segurança obteve a descrição de uma que é importante para melhoria do prejuízo da empresa defina como:

- Proteger ativos organizacionais: Principal finalidade é proteger informações, instalações e equipamentos contra ameaças internas e externas.

3.2.2. Resolução

Diante a política de segurança escolhida e os ocorridos de prejuízos descrito sobre tech/tecnologia. A seguir vai contém os principais pontos descrito da resolução, ou seja, ideias analisadas que são:

- Ataque a rede: Necessitam utilizar ferramentas mais eficiente que são automatizadas para os funcionários conter ação de agilidade e procurar sempre aprimorar o conhecimento de seus funcionários sobre novas maneiras de resolução para prevenir que o ataque não seja concluído pelos invasores ou até mesmo uma engenharia social pelos funcionários da empresa que venda particularmente para outras empresas;

- Banco de dado sem manutenção ativa: Os funcionários que trabalham no departamento como analista de dado ou desenvolvedores precisam usar o auxílio da Inteligência Artificial para analisar em tempo real e aumentar a quantidade de funcionário que possa qualificar com treinamento da própria organização, pois o maior lucro da empresa está na criação de bancos de dados e manutenção. Dessa forma, utilizaram funções da linguagem de programação e descrever com mais eficiente com mudanças sem o medo de perder os dados armazenados;

- Senhas fracas: Para resolver a falta da criatividade de senhas fortes a melhor resolução é pagar o gerador de senha que criam e aumenta a segurança da empresa. Os geradores gratuitos são bons também, porém pode ser um erro escolher ainda mais quando referimos ao ambiente profissional;

- Site sem certificado válido: O site necessita de uma proteção que é importante a utilização das ferramentas de verificação para estar em segurança e não acontecer novamente a falta de confiança com outras empresas ou clientes.

3.3. Listagem de Normas Gerais de Segurança

- A seguir vai está descrito sobre normas gerais de ISO 27001, NIST e GDPR:

3.3.1.ISO 27001

- Reconhecida como o padrão e referência internacional para a gestão da Segurança da informação que é a união de ISO 27001 e a BS7799 de um documento publicado 1992 pelo departamento do governo Britânico que

contém a certificação do código de práticas relativas de gestão da Segurança da Informação na finalidade de identificar os riscos, implementação de controles de segurança da criptografia e políticas de acesso auditorias regulares e melhoria contínua do ISMS.

3.3.2. NIST

- NIST contém a principal funcionalidade de gerenciar os riscos cibernético oferecido pela identificação, proteção, detecção, resposta e recuperação de ameaças para governar, identificar, proteger, detectar, responder e recuperar pelo seu papel de compreensão para lidar com os riscos pelas metas, das operações e das partes interessadas de uma organização.

3.3.3. GDPR

- Um projeto definido para proteger dados e identificar cidadãos da união Europeia que começou a ser idealizado em 2012 e foi aprovado em 2016 na finalidade de coletar, processar, compartilhar e resguardar dados pessoais.

3.4. Experimento Prático em Configuração de Segurança

- No próximo tópico irei descrever sobre uma ferramenta de software com a principal funcionalidade de como utilizar VeraCrypt:

3.4.1. VeraCrypt

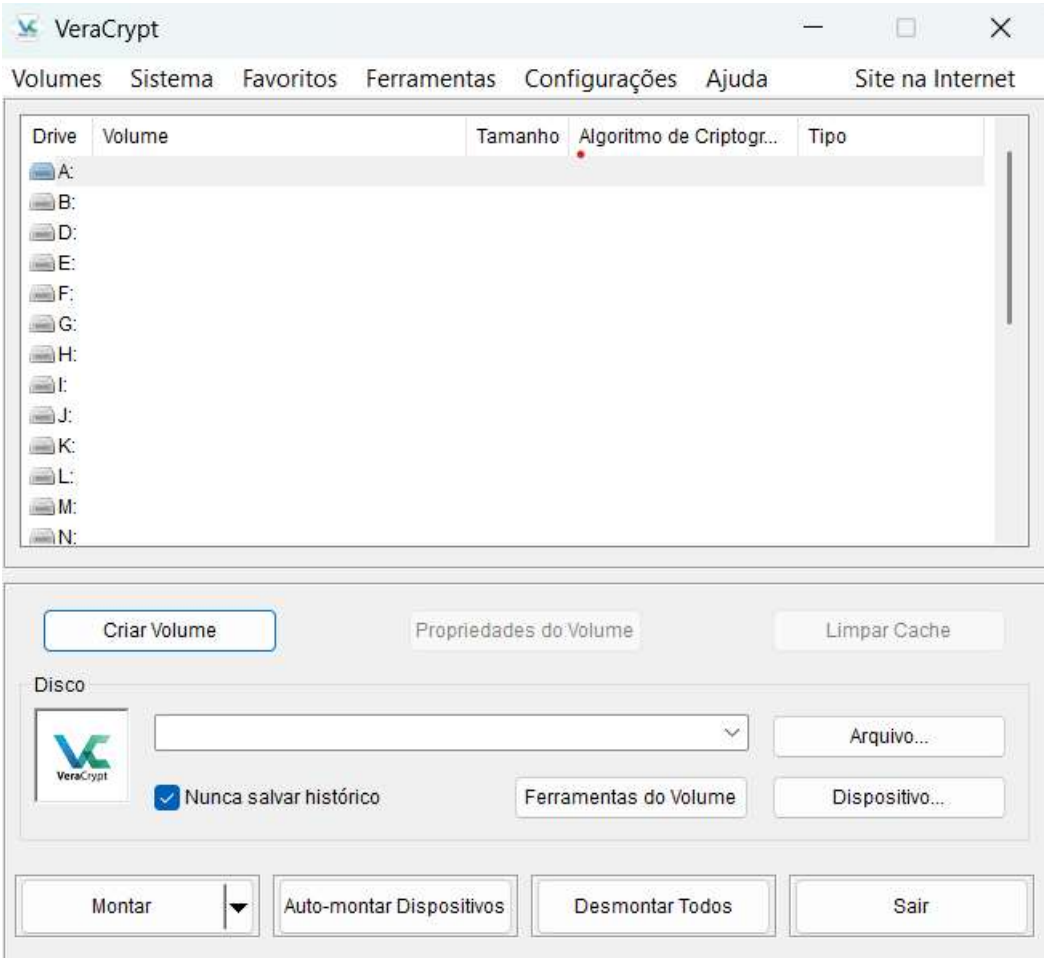
- Esse software contém a principal funcionalidade para realizar a criação de volume criptografado ou volume oculto.

3.4.1.1. Criação de Volume

- Para a criação de volume foi utilizado uma imagem na definição como exemplo conforme descrita em todas as etapas:

- Na FIGURA 1 contém como criar volume;

FIGURA 1:Criação de Volume



Fonte: autoria própria

- Selecionador da FIGURA 2 o tipo de volume padrão;

FIGURA 2:Volume padrão

Fonte: autoria própria

- Utilização do AES de criptografia e algoritmo de Hash SHA-512 como a FIGURA 3;

FIGURA 3:Opção sobre Volume

Fonte: autoria própria

- O tamanho demonstrado da FIGURA 4 do disco que foi 10 MB(Megabytes);

FIGURA 4:Tamanho do Volume

Fonte: autoria própria

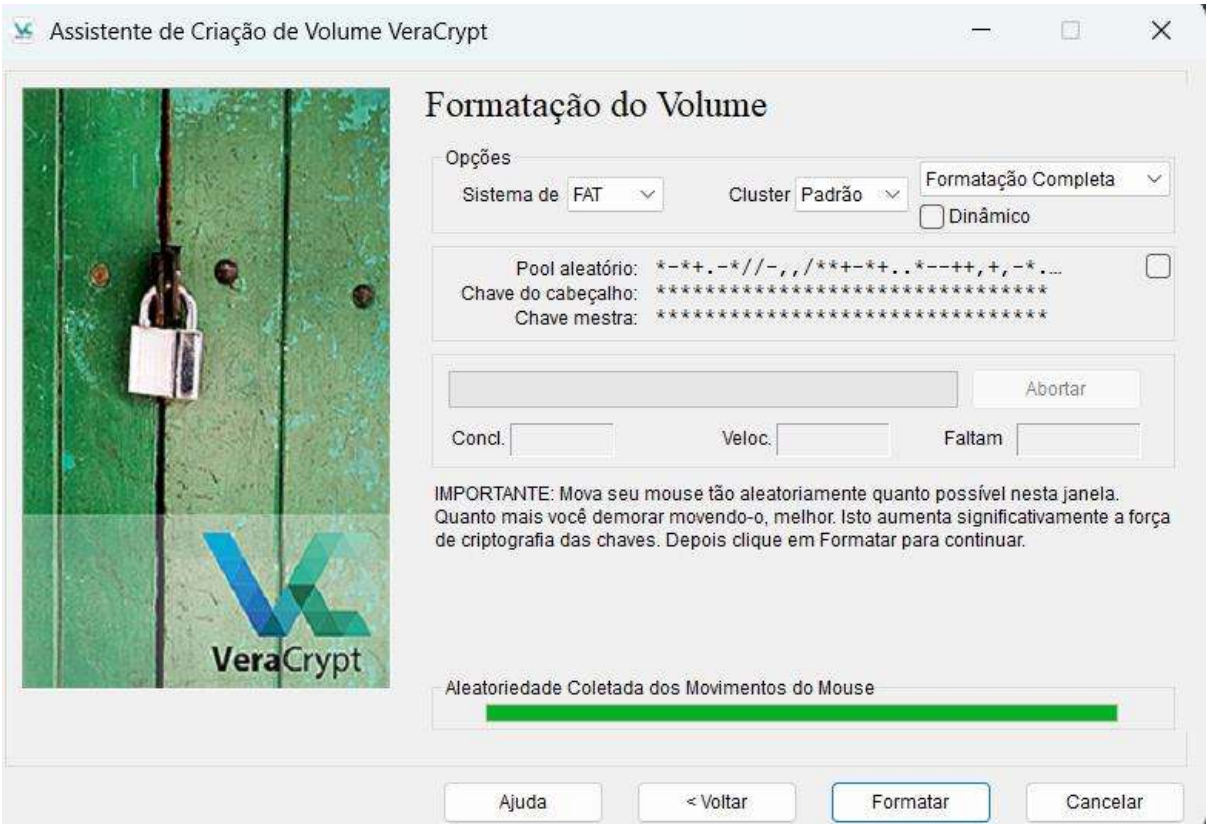
- Descrever a senha do volume na FIGURA 5;

FIGURA 5:Opção sobre Volume

Fonte: autoria própria

- A formatação do volume finalizada como FIGURA 6;

FIGURA 6:Formatação do Volume



Fonte: autoria própria

3.4.1.2. Criação de Volume Oculto

- Selecionar na FIGURA 7 o volume oculto;

FIGURA 7:Volume Oculto

Fonte: autoria própria

- A FIGURA 8 demonstra a quantidade de MB(Megabytes);

FIGURA 8:Tamanho do Volume Oculto

Fonte: autoria própria

- Na FIGURA 9 descreve a finalização.

FIGURA 9:Finalização do Volume Oculto

Fonte: autoria própria

4.Resultado

Durante a realização pelas pesquisas e análises foi abordado resoluções dos requisitos negativos sobre uma empresa na finalidade de estratégias objetivas, ferramentas, normas, administrativa, documentação e mais segurança com os dados da organização e cliente.

5.Conclusão

Conforme a ordem sobre Processos e Políticas de Segurança desde da sua importância para o ambiente profissional em pontos que necessitaram de melhoria pelas observações nos problemas encontrados e na situação complexa. Dessa forma, foi utilizado experiencia analista sobre dois grupos o profissionalismo e usuário para concluir uma solução corresponde prática e agilidade.

Para isso, também foi usado o software VeraCrypt na finalidade de demonstrar um exemplo sobre como criar um volume ou volume oculto de uma imagem.

6. Referências Bibliográficas

BLOG GESTÃO DE SEGURANÇA PRIVADA.JOSÉ SERGIO. Política de Segurança: Descubra o que é e Por que é Crucial para Segurança da sua Empresa Disponível em:https://gestaodesegurancaprivada.com.br/politica-de-seguranca-o-que-e-qual-sua-importancia-como-criar/ .Acesso em:24/03/2025.

ISO 27001.O que é a norma ISO 27001? Disponível em:https://www.27001.pt/.Acesso em:24/03/2025.

CENTRIC SOLUTION.Crie uma política de Segurança para sua empresa. Disponível em:https://centric.com.br/blog/politica-de-seguranca/.Acesso em:24/03/2025.

ISEO BLUE.Alan Parker.ISO 27001 Requirimentos e Principal Key.Disponível em:https://www.iseoblue.com/post/understanding-iso-27001-meaning-requirements-and-key-principles-for-effective-information-security?form=MG0AV3.Acesso em:24/03/2025.

STARTUP DEFENSE. Dominando a segurança com a estrutura de cibersegurança do NIST. Disponível em:.https://www.startupdefense.io/pt-br/blog/mastering-security-with-the-nist-cybersecurity-framework . Acesso em:24/03/2025.

EMERSON Alecrim.O que é GDPR e que diferença isso faz para quem é brasileiro.Disponível em:https://tecnoblog.net/responde/gdpr-privacidade-protecao-dados/.Acesso em:24/03/2025.

CÁTEDRA.GDPR:o que é e qual a diferença em relação à LGPD? . Disponível em:https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/ . Acesso em:24/03/2025.

Musashiden Tutoriais 2. Disponível em:https://www.youtube.com/watch?v=6ohj_AC0OPs .Acesso:24/03/2025.