**FACULDADE DE TECNOLOGIA SENAC GOIÁS**

**Tecnologia em Segurança da Informação**

LogoSenac

Aldo Filho  
Jordan Hugs  
Liniker Lettierre  
Rony Carneiro

**Uso de ferramentas de Segurança**

Francisco Xavier Calaça

GOIÂNIA,

2016

Aldo Filho  
Jordan Hugs  
Liniker Lettierre  
Rony Carneiro

**Uso de ferramentas de Segurança**

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina Segurança em Sistemas Operacionais, no curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Francisco Xavier Calaça

GOIÂNIA,

2016

**SUMÁRIO**

[1 INTRODUÇÃO 4](#_Toc469291257)

[2 DESENVOLVIMENTO 4](#_Toc469291258)

[2.1 Firewall 4](#_Toc469291259)

[2.2 AntiVírus 4](#_Toc469291260)

[2.3 Graylog 4](#_Toc469291261)

[2.4 VeraCrypt 5](#_Toc469291262)

[2.5 Windows Active Directory 5](#_Toc469291263)

[2.6 Proxy 6](#_Toc469291264)

[3 CONCLUSÃO 7](#_Toc469291265)

[4 REFERÊNCIAS BIBLIOGRÁFICAS Erro! Indicador não definido.](#_Toc469291266)

# INTRODUÇÃO

Para mantermos os pilares da Segurança da Informação (Integridade, Confidencialidade, Disponibilidade), conforme prescrito na Política de Segurança da Informação da VDM CORP. serão implementados procedimentos que mitiguem a possibilidade de perca/roubo de dados e registre qualquer acesso a todos os sistemas da empresa.

# DESENVOLVIMENTO

# Firewall

A nossa primeira barreira contra os ataques externos é um firewall. Será instalado na empresa o tipo de firewall NGFW(Next Generation Firewall) que faz a análise de todos os pacotes, a vantagem deste tipo de firewall é que alem dele atuar como um firewall tradicional fazendo analises de porta, IP’s ele consegue verificar se o pacote que está sendo tráfegado é realmente daquela aplicação/protocolo.

# AntiVírus

O programa AntiVírus serão instalados para mitigar as chances de infecção de worms, trojans e outros tipos de ameaças. O AntiVírus é nossa segunda barreira de proteção contra os ataques externos e internos e por este motivo será instalado em todas as estações de trabalho da empresa o Kaspersky Endpoint Security for Business | Select.

# Graylog

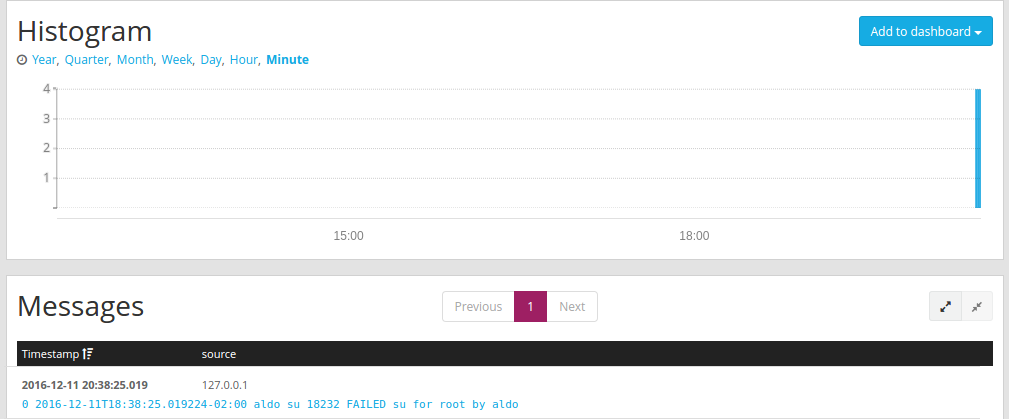
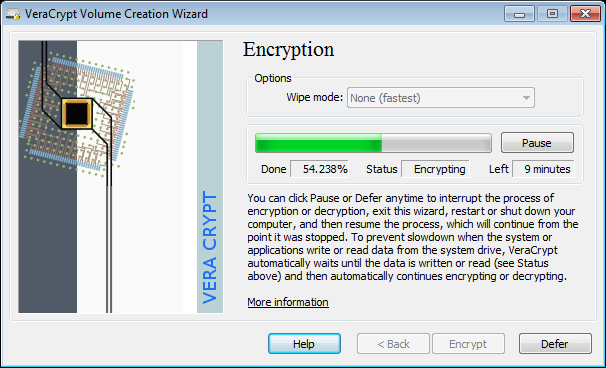
 Serviço de monitoramento dos servidores, com o intuito de descobrir e reduzir os problemas rapidamente e pro-ativamente. O graylog suporta grandes quantidades de informações e consegue manipula-las com extrema rapidez, nesta ferramenta podemos fazer vários tipos de filtros nos logs para disponibilizarmos as informações realmente importantes para um administrador de redes.

Figura 1. Autenticação do usuário root.

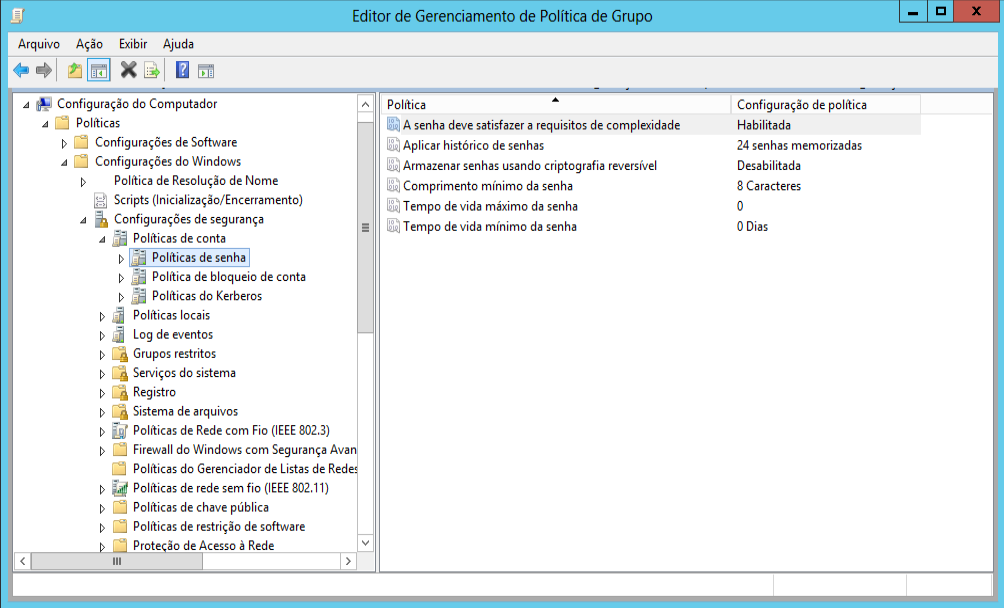
# VeraCrypt

Veracrypt é um software que utiliza OTFE(On-the-fly-encryption) e cria um disco virtual criptografado. On-the-fly-encryption significa que o dado é encriptado logo depois de ser salvo e descriptografado logo após ser carregado, sem nenhuma intervenção dos usuários. Todos os computadores da empresa precisam ter uma partição criptografada para armazenar todos os dados sensíveis da empresa, após o uso do disco criptgrafado os usuários devem desmontar a partição para evitar de um atacante conseguir acessa-la caso ele consiga acesso ao computador de algum usuário.

Figura 2. Encriptação do disco.

# Windows Active Directory

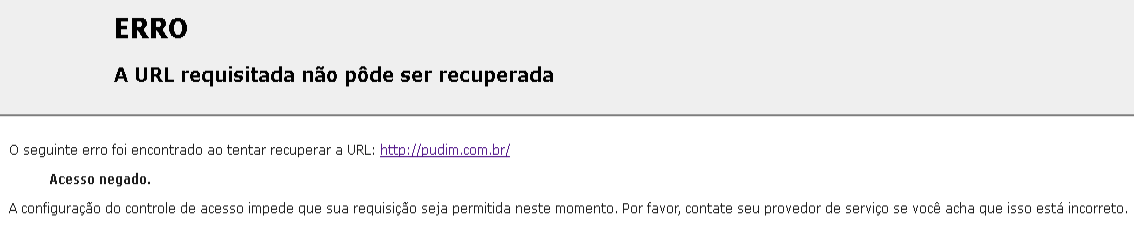
A ferramenta Active Directory nos permite controlar o domínio ao qual o usuário está cadastrado, com isto, é possível que um usuário siga as diretrizes estabelecidas na PSI, como por exemplo a política de senhas, ela pode ser facilmente implementada utilizando a GPO(Diretiva de Grupo).

Figura 3. Diretriz da Política de senha.

Além disto os usuário do domínio vão ser autenticados através do SSO(Single Sign-On) possibilitando que os usuários não precisem se preocupar com várias senhas, pois ele será autenticado e autorizado no sistema para acessar as demais aplicações da empresa.

# Proxy

O serviço de proxy é importante para a organização pois ele consegue além de bloquear os sites especificados é possível bloquear também os tipos de arquivos como .exe, .mp4, .jpg que iriam ser baixados. A implementação de um proxy na empresa, é vital para o monitoramento de todos os sites acessados pelos os usuários.

****

# CONCLUSÃO

O uso de ferramentas de segurança é de extrema importância para se utilizar em uma empresa, atender suas necessidades, monitorar, proteger, e reduzir o risco de incidentes de segurança.