Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Segurança da informação em ambientes Microsoft

Elaborador:	Elton Alexandre Teixeira
Orientador:	Edson Roberto Gaseta

FACULDADE DE TECNOLOGIA DE AMERICANA

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

T265s TEIXEIRA, Elton Alexandre

Segurança da informação em ambientes Microsoft. / Elton Alexandre Teixeira. – Americana, 2019.

20f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Edson Roberto Gaseta

1 Segurança em sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: *681.518.5*

FACULDADE DE TECNOLOGIA DE AMERICANA

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

ELTON ALEXANDRE TEIXEIRA

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES MICROSOFT

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 11 de Junho de 2019

Banca Examinadora:

Edson Roberto Gaseta (presidente)
Especialista
Fatec Americana

Benedito Aparecido Cruz
Mestre
Fatec Americana

Diógenes de Oliveira
Mestre
Fatec Americana

SUMÁRIO

Lista de figuras

1 Objetivo deste documento

Já faz um bom tempo que a informação deixou para trás o conceito de conjunto de dados agrupados para se tornar um dos ativos mais importantes para a maioria das organizações. Isso se deu pelo fato dela proporcionar benefícios muito importantes a estas organizações, como vantagem competitiva e auxílio na tomada de decisões. Diante de tamanha importância, garantir a segurança da informação hoje é fator crucial dentro das organizações. Segundo FONTES [2006, PXX] Proteger a informação significa garantir:

> *Disponibilidade*: a informação deve estar acessível para o funcionamento da organização e para o alcance dos seus objetivos e missão.
>
> *Integridade*: a informação deve estar correta, ser verdadeira e não estar corrompida.
>
> *Confidencialidade*: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia.
>
> *Legalidade*: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como com os princípios éticos seguidos pela organização e desejados pela sociedade.
>
> *Auditabilidade*: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.
>
> *Não repúdio de autoria*: o usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Uma das maneiras de se atingir os objetivos da segurança da informação é através da análise prévia e aplicação de medidas, que visam mitigar as vulnerabilidades em um determinado ambiente.

Em meio à grande diversidade de ambientes computacionais existentes no mercado, os ambientes baseados em sistemas operacionais Microsoft representam uma grande fatia do mercado.

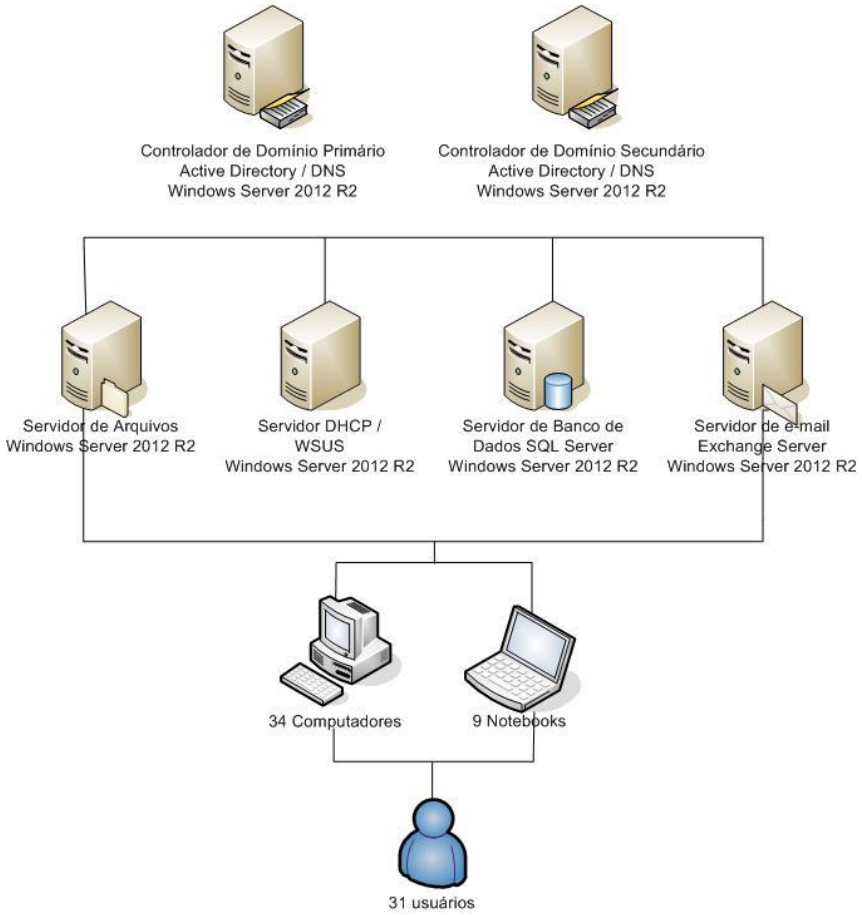
O objetivo específico deste trabalho é apresentar através de um estudo de caso a análise e implementação de medidas necessárias para a garantia da segurança da informação um ambiente computacional baseado em sistemas operacionais Microsoft.

2 Desenvolvimento

2.1 O ambiente escolhido

O ambiente computacional escolhido para elaboração deste relatório técnico conta com 31 usuários e 43 computadores clientes, conforme ilustra a figura 1, e está baseado na arquitetura cliente servidor. De acordo com BURGESS (2006), um servidor não é um *host*, mas um programa ou processo executado em um *host*, e um cliente seria qualquer programa que precise dos serviços de um servidor.

Figura 1 - Diagrama da rede

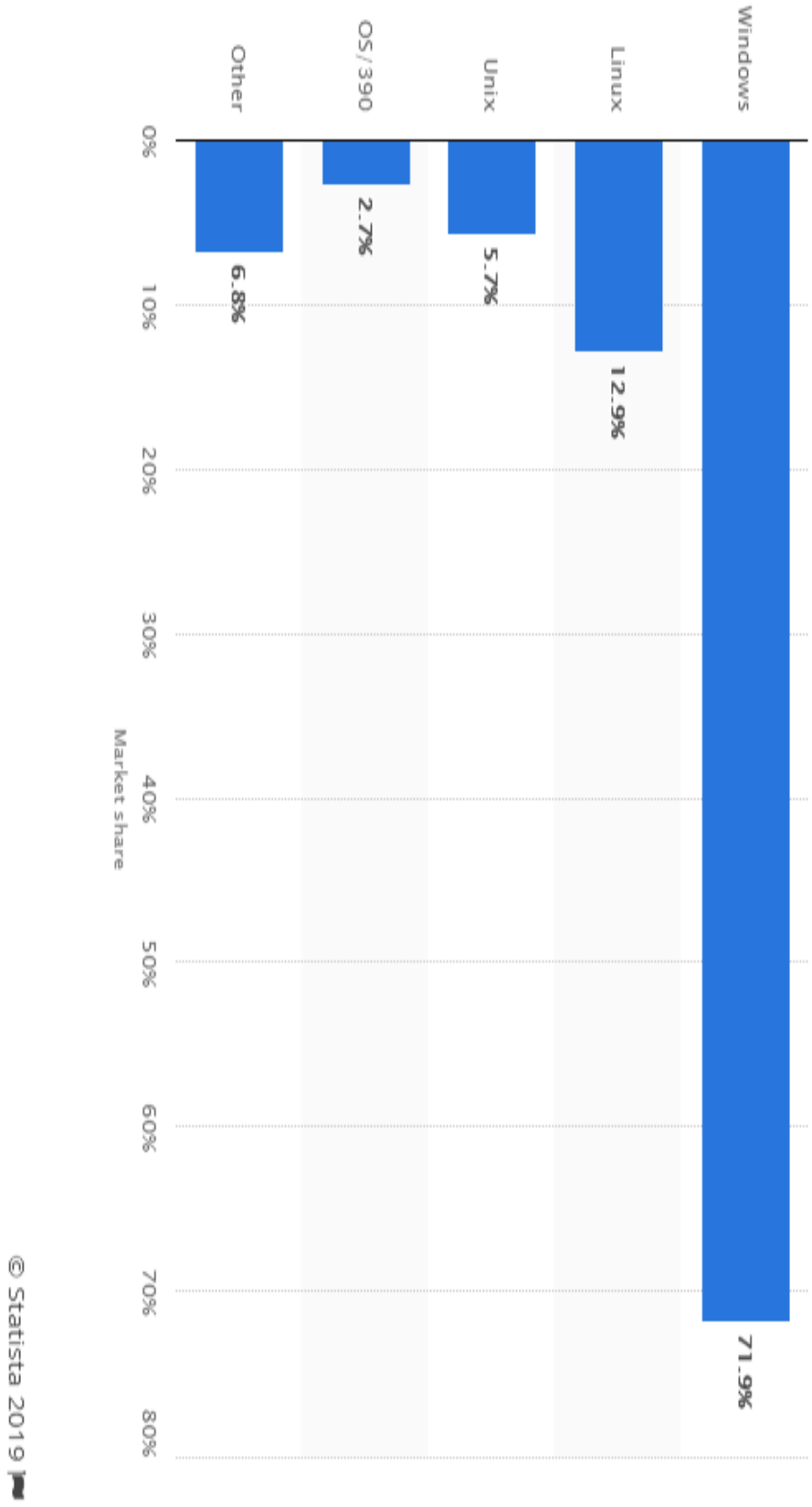


Fonte: Elaborado pelo próprio autor

O sistema operacional dos servidores analisados é o Windows Server 2012 e neles se hospedam serviços essenciais para o funcionamento da rede corporativa, como: Autenticação de usuários, DNS, DHCP, servidor de arquivos, banco de dados SQL, correio eletrônico e VPN

A escolha deste ambiente se deu pela grande representatividade de tais sistemas operacionais nos ambientes corporativos. A figura 2 ilustra a participação dos sistemas operacionais Microsoft Windows no mercado de servidores.

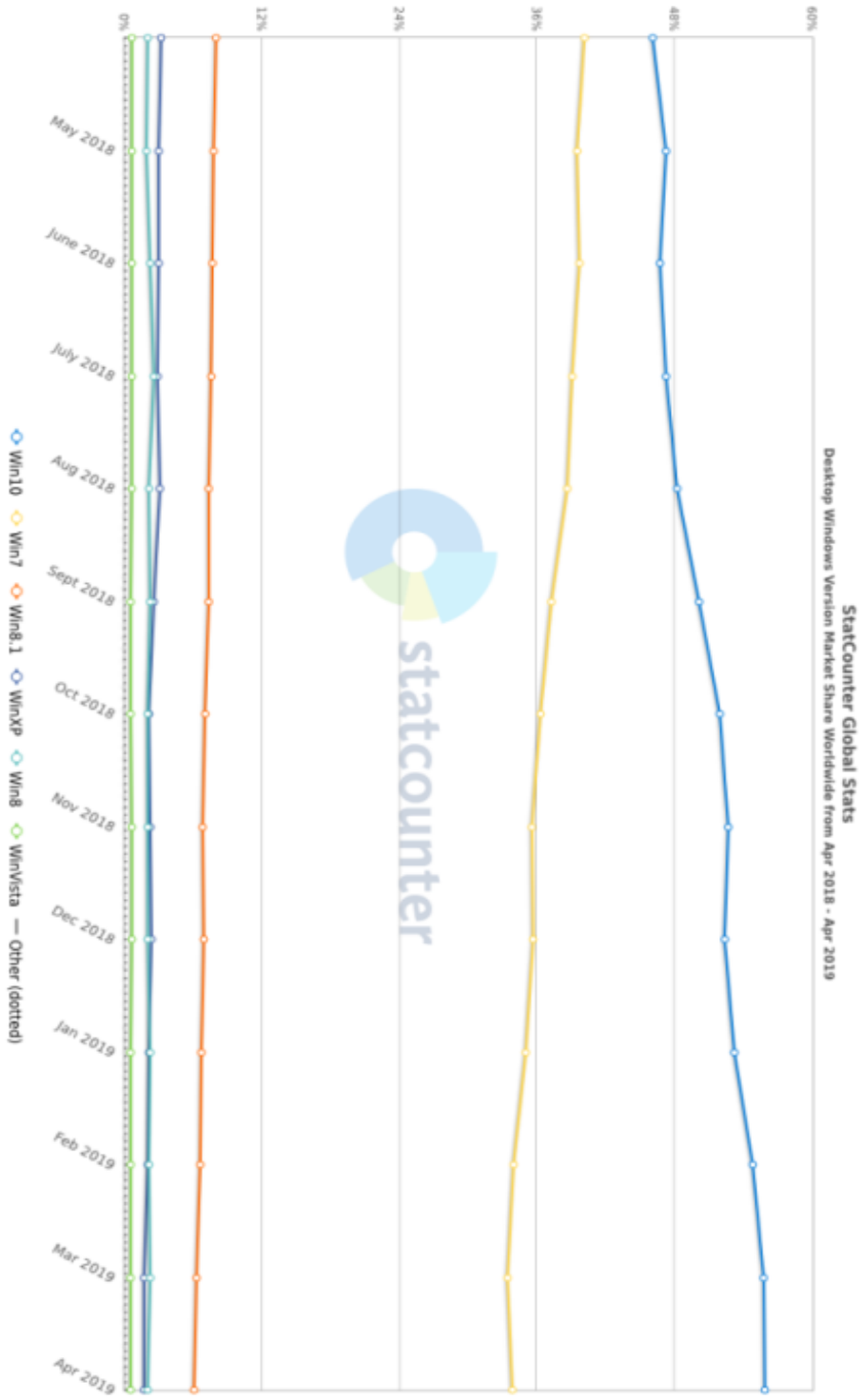
Figura 2 - Participação de mercado dos sistemas operacionais Windows Server:



Fonte: https://www.statista.com/statistics/915085/global-server-share-by-os/

O parque de estações de trabalho é misto e possui equipamentos com os seguintes S.O. instalados: Windows 7 Pro, Windows 8.1 Pro e Windows 10 Pro. A figura 3 ilustra a participação dos sistemas operacionais Microsoft Windows no mercado de desktops:

Figura 3 - Participação de mercado dos sistemas operacionais Microsoft Windows para desktops:



Fonte: http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

Dentro do ambiente escolhido, o escopo do trabalho executado para a elaboração deste relatório foi a análise e aplicação de contramedidas para tentar conter as vulnerabilidades existentes nas contas de usuário do *Active Directory* e a aplicação de GPOs para melhoria da segurança da informação em todo o cenário.

2.2 Active Directory

Quando falamos de redes de computadores, temos duas possibilidades de configuração lógica dos computadores, utilizando grupos de trabalho ou domínios.

Em uma rede configurada em grupo de trabalho, toda a administração dos objetos é feita de forma descentralizada em cada computador. Imagine uma rede com cerca de 44 computadores e 32 usuários, onde existe a necessidade do compartilhamento de arquivos e outros recursos entre diversos usuários e em diversos computadores. Toda vez que fosse necessário criar uma conta usuário, e caso este usuário necessitasse acessar recursos em todos os computadores, este usuário teria de ser criado 44 vezes, uma vez em cada computador. Caso este usuário resolvesse trocar sua senha de rede, esta também teria de ser trocada em todos os 44 computadores, um a um.

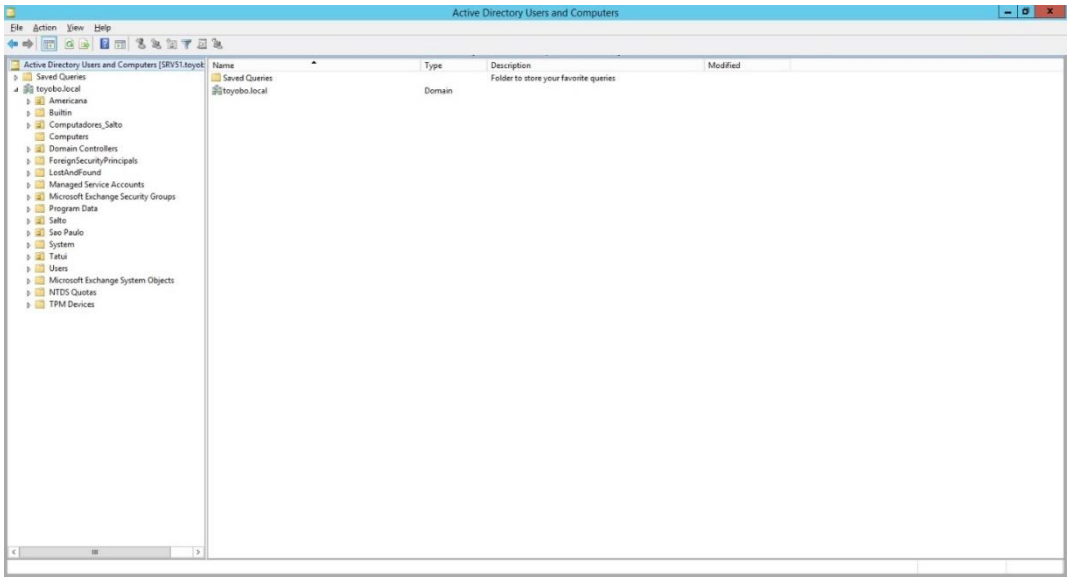
No modelo de rede baseada em domínio, o gerenciamento de usuários é feita de forma centralizada, através do serviço de diretórios. Segundo BURGESS (2006, p140), a definição de um serviço de diretório seria: "*Um conjunto de sistemas abertos que cooperam para manter um banco de dados lógico de informações sobre vários objetos do mundo real. O serviço de diretório é um serviço de nomes generalizado*" (APUD padrão X.500, 167). No Microsoft Windows, o recurso responsável pela administração de usuários e outros objetos em um domínio é o *Active Directory*. Podemos compará-lo a um banco de dados, funcionando como um catálogo que reúne diversas informações sobre os usuários, como nome, sobrenome, senha, grupos de segurança e etc. Caso um usuário membro do domínio decida trocar sua senha, esta é replicada automaticamente para todos os computadores da rede.

Dentre os objetos gerenciados pelo *active directory*, podemos citar:

- OU ou unidades organizacionais:
- Contas de usuários:
- Grupos de segurança:
- Computadores:

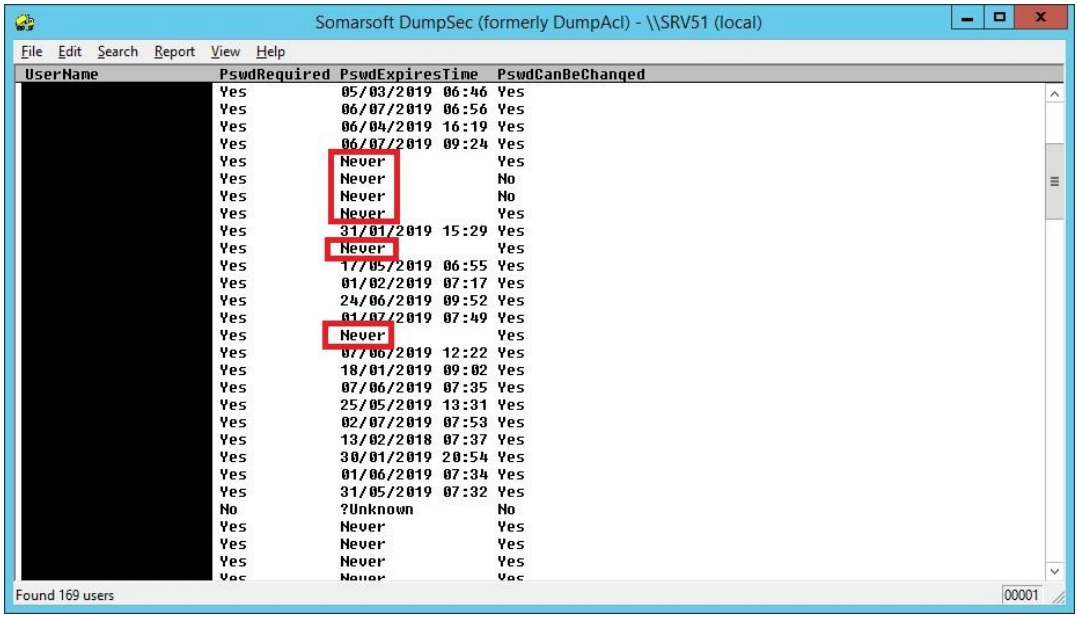
Neste trabalho, foram analisados os aspectos de segurança com relação às contas de usuários no *Active Directory*. A análise do ambiente foi efetuada utilizando o próprio console de gerenciamento do *Active Directory*, ilustrado pela figura 4 e também com o auxílio da ferramenta DUMPSEC, ilustrada na figura 5.

Figura 4 - Console de administração do *Active Directory* no Windows Server 2012:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

Figura 5 - Ferramenta DUMPSEC para análise do Active Directory.



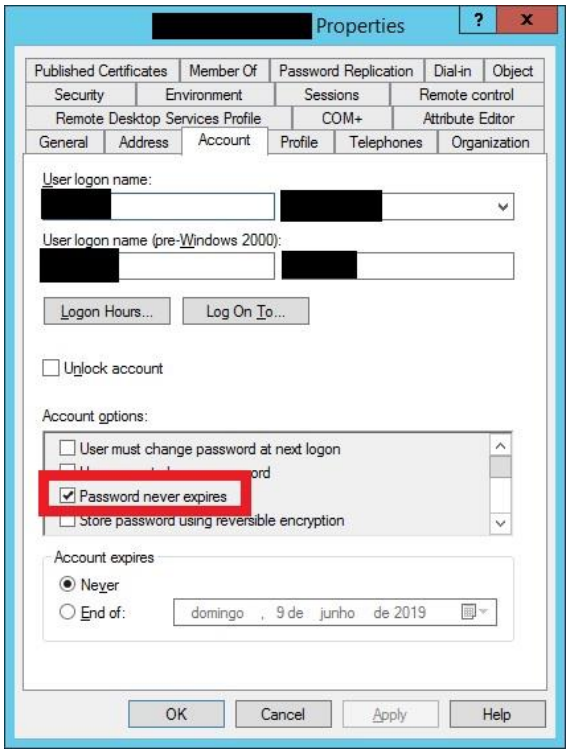
Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

A partir da análise do *Active Directory*, foi possível identificar as seguintes vulnerabilidades com relação às contas de usuário:

Contas de usuário configuradas para nunca mudar de senha:

Durante a análise, foram encontradas contas de usuários, em sua maioria de cargos de alta gestão que não seguiam a política de troca de senhas periódica. A troca compulsória de senha em um período determinado de tempo reduz o risco de acesso indevido às informações, pois se uma credencial antiga for encontrada por alguém mal intencionado, muito provavelmente esta já não terá mais validade.

Figura 6 - Conta de usuário configurada para nunca expirar a senha:



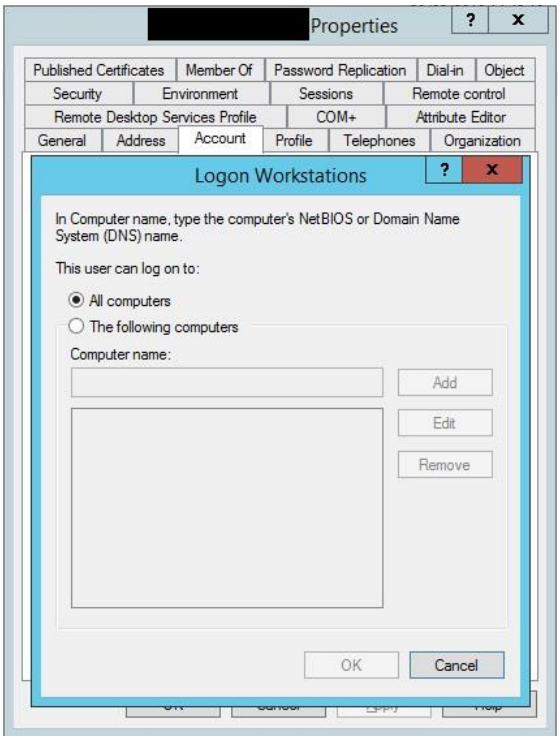
Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

Após a análise, todas as contas marcadas com o parâmetro para não expirar a senha, tiveram este parâmetro desabilitado manualmente e a senha redefinida pelo administrador de rede, obrigando o proprietário da conta a cadastrar uma nova senha dentro das diretrizes definidas no próximo *log on*.

Usuários com permissão para efetuar *log on* em qualquer computador:

O fato de um usuário poder efetuar *log on* em quaisquer computadores da rede nos traz o risco do acesso indesejado a arquivos e programas. O desejável para a organização é que o colaborador acesse somente a estação de trabalho que lhe foi designada ou apenas as estações de trabalho de seu departamento.

Figura 7 - Conta de usuário com permissão de *log on* em todos os computadores:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

As contas de cada usuário foram ajustadas manualmente para *log on* somente nas estações de trabalho desejadas de acordo com o inventário de computadores que a empresa já possuía.

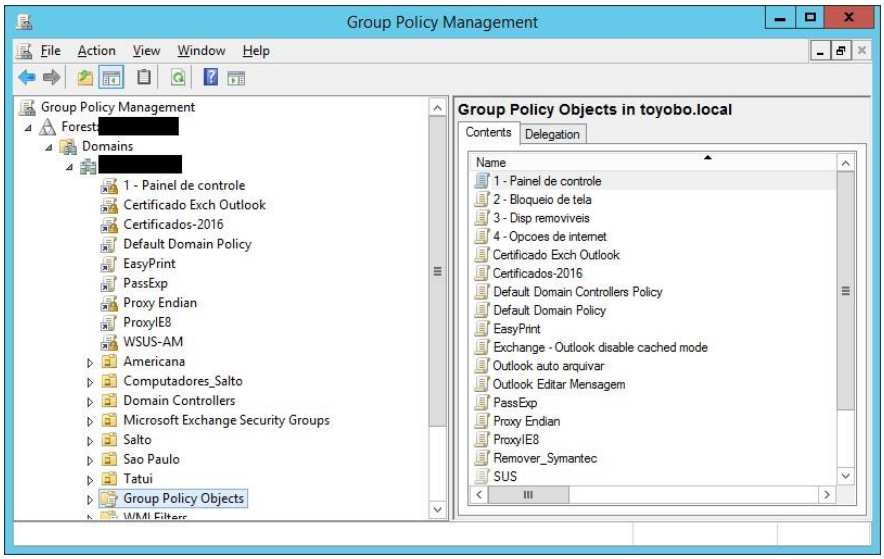
2.3 Aplicação das GPOs para garantir a segurança dos clientes finais

As GPOs, ou objetos de política de grupo, é um recurso presente no Windows Server desde a versão 2000, e podem ser aplicadas à computadores e servidores que façam parte de um domínio. Através do uso de GPOs, podemos efetuar a parametrização de diversas configurações existentes no Windows instalado nos clientes finais, tudo de forma centralizada, sem a necessidade de acessar diretamente a estação de trabalho do usuário. Resumindo, funciona como um conjunto de regras a serem seguidas e podem ser aplicadas à qualquer objeto do domínio, como usuários, computadores e grupos de segurança.

No âmbito da segurança da informação, as GPOs são muito úteis para inibir ao usuário final o acesso indevido as configurações do sistema operacional e também a execução de alguns recursos. A alteração indevida de uma configuração por parte do usuário pode ocasionar a indisponibilidade do computador, assim como o uso de alguns recursos de forma incorreta pode comprometer a segurança do computador e toda a rede.

A criação de uma GPO pode ser feita através do console de gerenciamento, neste caso, localizado em: *Start / Administrative Tools / Group Policy Management*, ou através da execução do comando GPMC.MSC no menu executar.

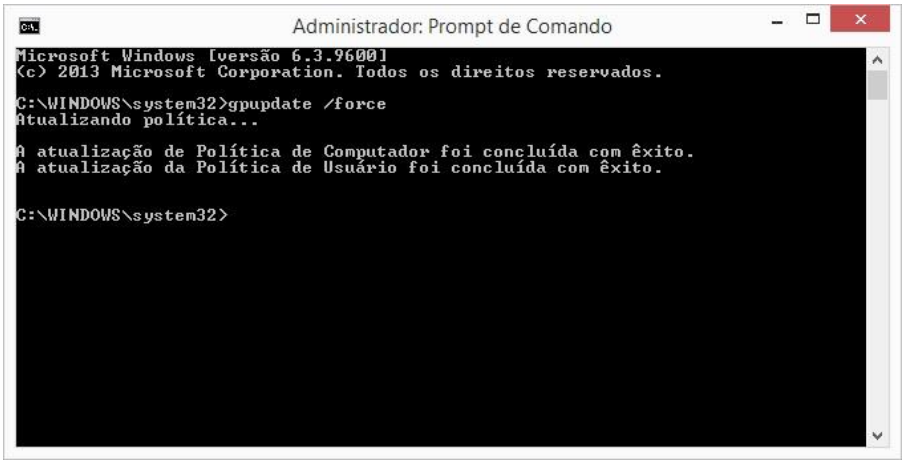
Figura 8 - Console de gerenciamento de GPO:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

Após a criação de uma GPO, para que ela seja aplicada imediatamente a um computador, podemos utilizar o comando GPUPDATE, executado à partir do prompt do DOS. A sintaxe do comando a ser utilizada para isso é: GPUPDATE /FORCE.

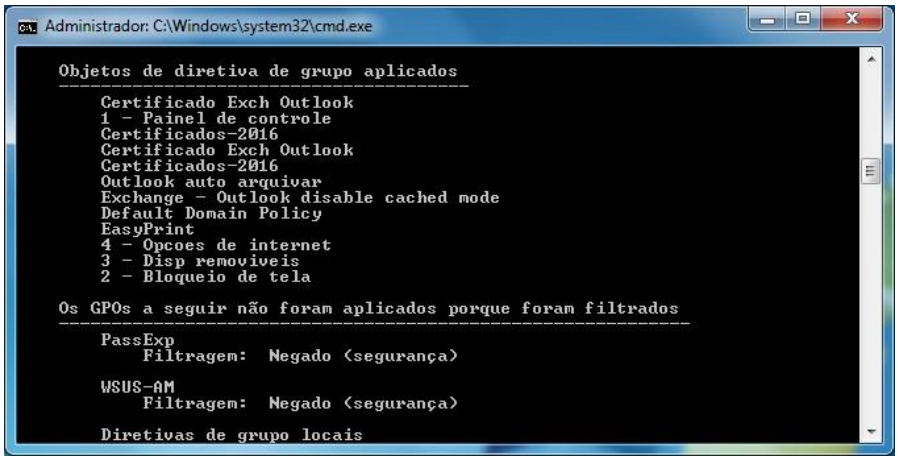
Figura 9 - Execução do comando GPUPDATE /FORCE:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

Para verificar quais as GPOs estão senda aplicadas no computador, podemos utilizar o comando GPRESULT, também executado a partir do prompt de comando, utilizando a sintaxe GPRESULT /R

Figura 10 - Execução do comando GPRESULT /R:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

Com o intuito de agregar mais segurança ao ambiente computacional escolhido, foram aplicadas as seguintes GPOs:

2.3.1 Bloqueio do painel de controle

O painel de controle do Windows reúne ferramentas de gerenciamento de diversos recursos do computador, seja de *software* ou de *hardware*. A partir dele é possível alterar configurações de rede, vídeo e som, instalar programas e drivers de dispositivos e também habilitar ou desabilitar funções de segurança do sistema, como por exemplo, o firewall do Windows.

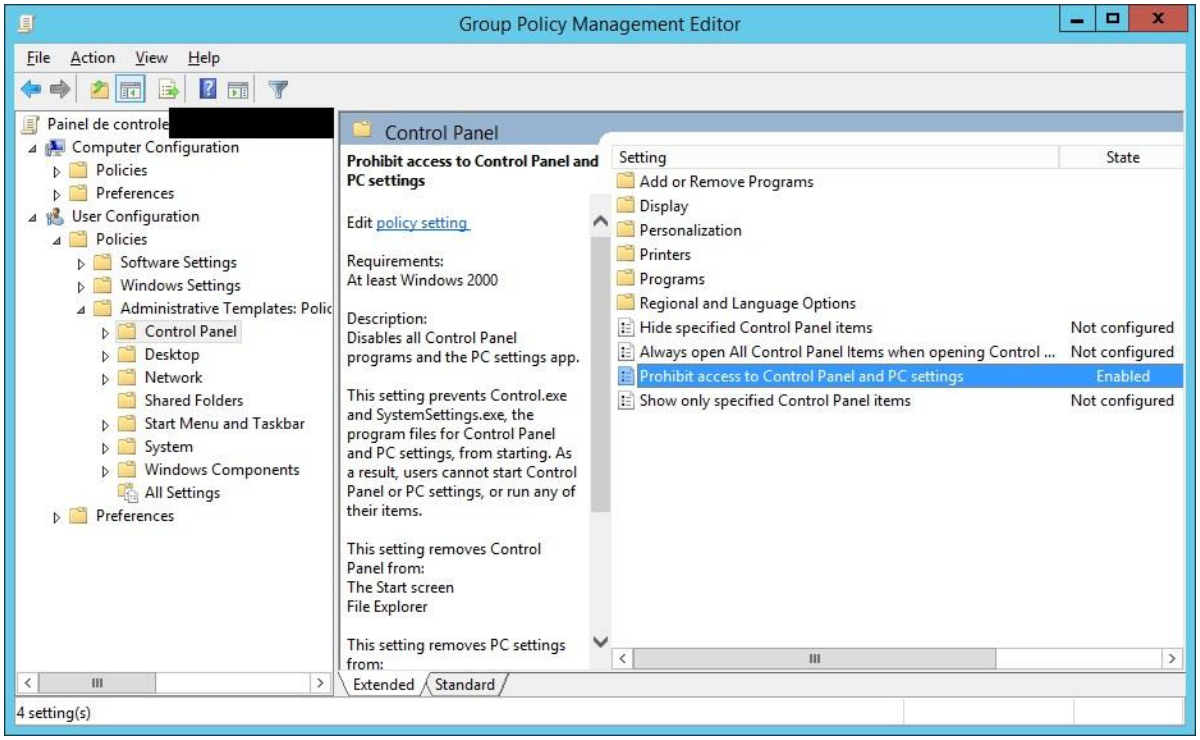
Figura 11 - Painel de controle do Windows:

Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

O uso indevido do painel de controle pelos usuários pode representar uma ameaça à segurança da informação, pois componentes importantes podem ser desativados sem autorização.

Para bloqueio do painel de controle, foi criada uma GPO habilitando o parâmetro "*Prohibit acces to control panel and PC Settings*", contido em *User Configuration / Policies / Administrative Template Policies / Control Panel.*

Figura 12 - GPO para bloqueio do painel de controle:



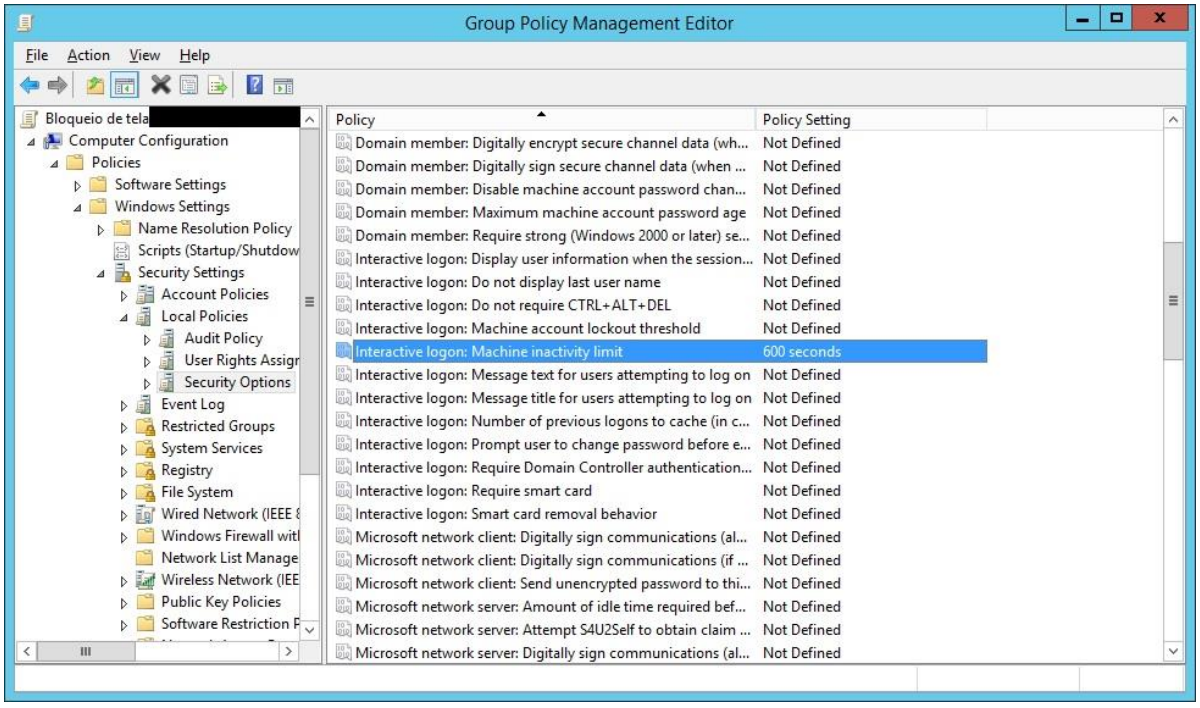
Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

2.3.2 Bloqueio do computador após tempo de inatividade

Durante a ausência, bloquear o computador para que ele exija novamente a senha no desbloqueio é um recurso muito importante, pois de nada adianta os usuários garantirem o sigilo de suas senhas e deixarem seus computadores escancarados para que alguém possa usar. Infelizmente nem sempre os usuários se lembram de efetuar o bloqueio ao deixarem seu ambiente de trabalho.

Na tentativa de tentar minimizar este problema, foi criada uma GPO habilitando o parâmetro “Interactive logon: Machine inactivity limit” e configurando o mesmo com 600 segundos (10 minutos), este parâmetro está localizado em Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options.

Figura 13 - GPO para bloqueio do computador por tempo de inatividade:



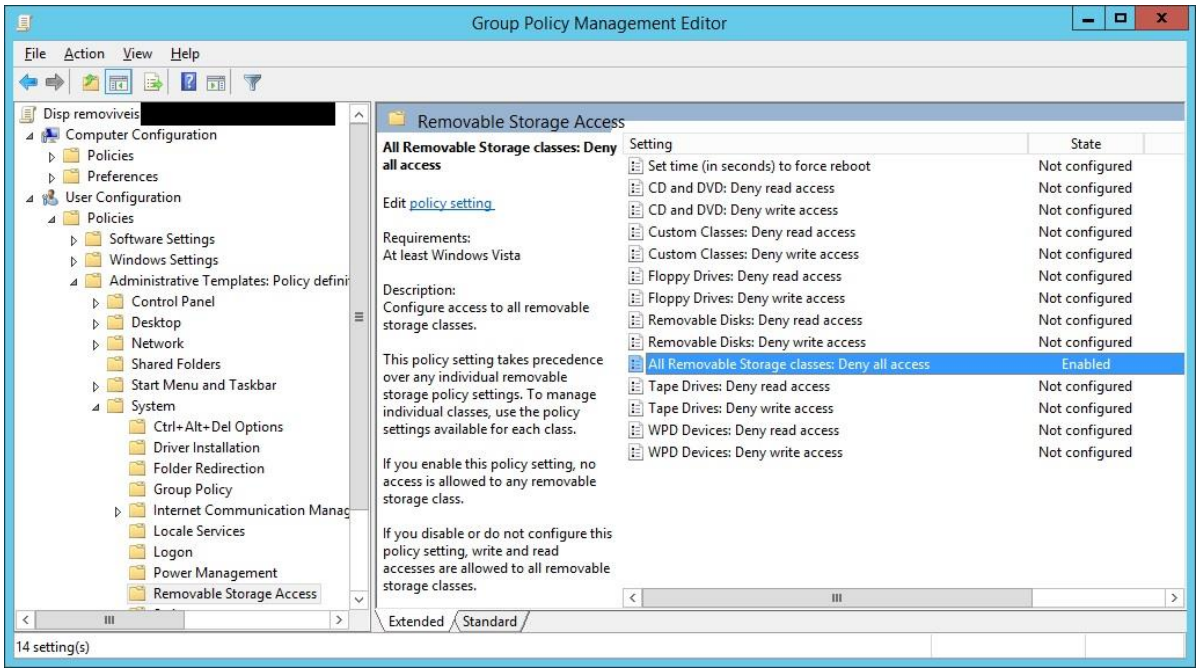
Fonte: Print screen da tela da aplicação no Windows Server 2012.

2.3.3 Bloqueio de unidades de armazenamento externas:

Dispositivos de armazenamento externo, como pen drives e hd's externos são uma fonte de ameaças para o ambiente computacional, pois não há como impedir um colaborador de trazer um dispositivo infectado com vírus ou *malware* e conectar aos computadores da empresa. Há também o risco da cópia indevida de informações da empresa para estes dispositivos, violando os princípios da confidencialidade.

Foi criada uma GPO que bloqueia o uso de qualquer dispositivo de armazenamento removível nos computadores, através da habilitação do parâmetro *All Removable Storage classes: Deny all access*, localizado em *User Configuration / Policies / Administrative Template Policies / System / Removable Storage Access*.

Figura 14 - GPO para bloqueio de unidades externas de armazenamento:

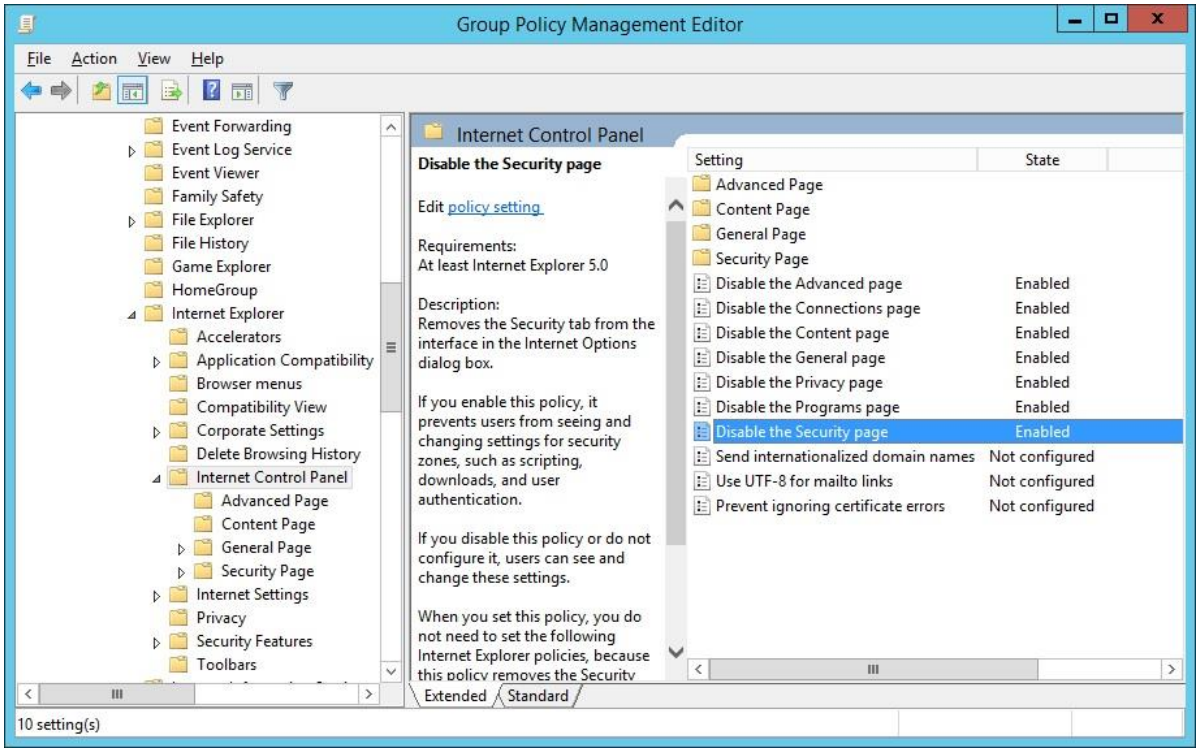


Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

2.3.4 Bloqueio das propriedades do navegador de internet:

O bloqueio das propriedades do navegador de internet tem a função de impedir que os colaboradores alterem qualquer configuração do navegador, garantindo assim que o navegador esteja configurado em um nível seguro para uso na *web*. Desta forma os usuários não conseguem alterar configurações de segurança, como a execução de scripts não confiáveis e também configurações de servidor proxy.

Figura 15 - GPO para bloqueio das propriedades do navegador de internet:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

2.3.5 Melhorando a segurança no log on de usuários utilizando a GPO padrão do domínio:

A GPO padrão do Windows Server 2012 conta com uma política de senhas para as contas de usuário que engloba os seguintes parâmetros:

Histórico de senhas: Verifica o histórico de senhas armazenadas para uma conta de usuário e não permite que seja cadastrada uma senha caso esta já tenha sido utilizada. O padrão do Windows Server 2012 é armazenar as ultimas 24 senhas do usuário.

Tempo máximo de senha: Este parâmetro determina o prazo de validade da senha para as contas de usuários, seguindo o padrão de 42 dias. Assim que for atingido o prazo, o usuário é obrigado a efetuar a troca da senha, ou fica impedido de efetuar o *log on.*

Complexidade de senha: Indica quais são as diretivas necessárias para que os usuários cadastrem ou alterem a senha de sua conta em um domínio. Por padrão, as seguintes diretivas dever ser seguidas:

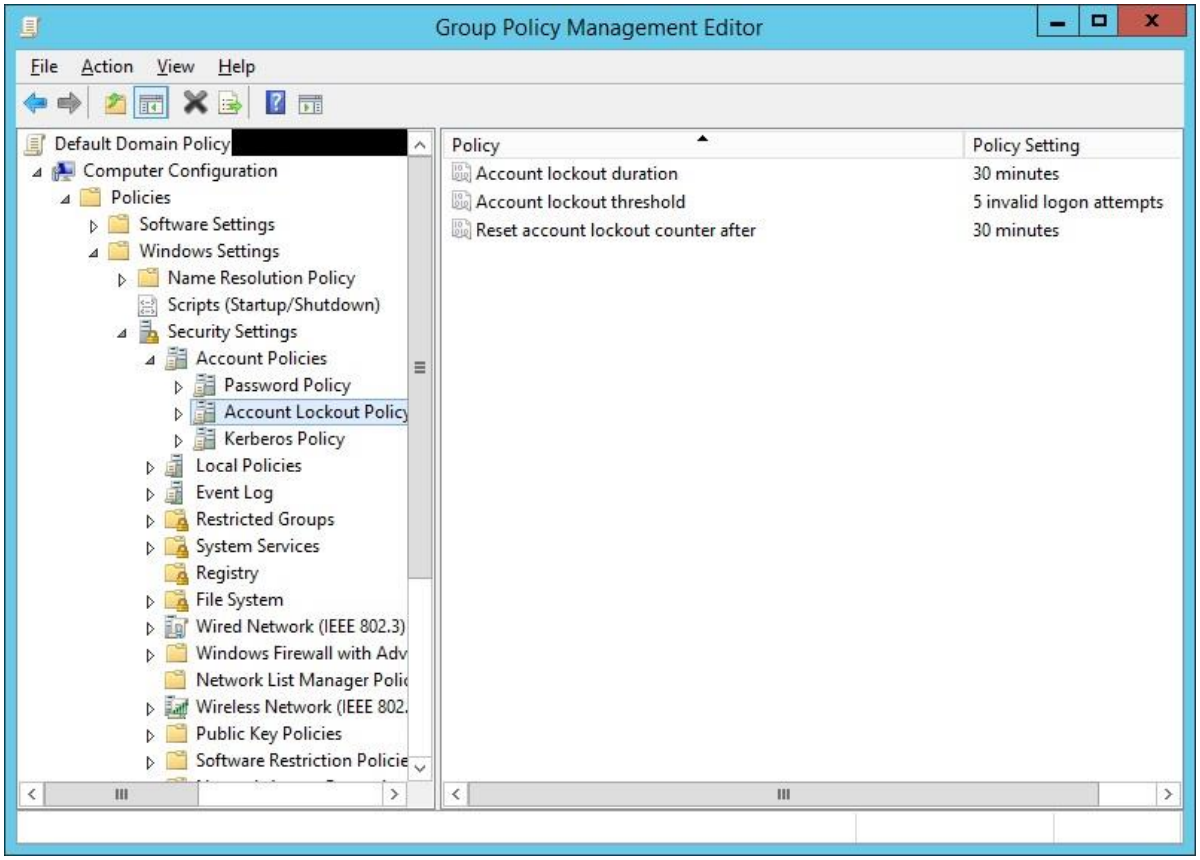
Não conter o nome da conta de usuário ou partes do nome completo do usuário que exceda dos caracteres consecutivos;

- Ter o comprimento mínimo de seis caracteres;
- Conter caracteres de três das quatro categorias abaixo:
- Caracteres maiúsculos (A à Z)
- Caracteres minúsculos (A à Z)
- Caracteres numéricos (0 à 9)
- Caracteres especiais (!, $, #, %, por exemplo)

2.3.6 Bloqueio da conta de usuário após tentativas sem sucesso:

Além da política padrão de senhas já pré-estabelecida pela Microsoft, foi adicionada à GPO padrão do domínio o recurso de bloqueio da conta de usuário após 5 tentativas incorretas de *log on*. A duração do bloqueio é de 30 minutos, após isso a conta é desbloqueada automaticamente. Este recurso se mostra muito útil contra programas que utilizam força bruta para tentar obter a senha de uma conta de usuário.

Figura 16 - GPO para bloqueio de conta de usuário:



Fonte: *Print screen* da tela da aplicação no Windows Server 2012.

3 Resultados

Com a adoção das medidas mencionadas neste relatório, posso concluir que houve um acréscimo sensível de segurança ao ambiente objeto do estudo.

Com a correção do problema nas contas de usuário que estavam marcadas para nunca trocar a senha, a segurança no processo de *log on* de usuários foi fortalecida, diminuindo a possibilidade de uso indevido de credenciais por pessoas não autorizadas.

A limitação dos usuários para que consigam efetuar o log on somente nos computadores onde estão autorizados, agregou mais segurança no quesito da confidencialidade, uma vez que oferece a garantia de que nenhum usuário curioso acesse ou modifique informações ou recursos em um computador que não esteja autorizado à usar.

A aplicação da GPO que faz o bloqueio do painel de controle impede que os usuários façam alterações indesejadas das configurações do sistema e contribuiu para a diminuição da indisponibilidade dos computadores para os próprios usuários e geração de chamados para a equipe de T.I.

Apesar de receberem instrução para bloquearem o computador com senha ao se ausentarem do posto de trabalho, muitos usuários deixam de tomar essa ação, deixando expostas as informações para qualquer um que tenha acesso físico ao computador. Neste sentido, o bloqueio automático do computador por tempo de inatividade se mostrou eficaz na proteção das informações do usuário, pois diminui o risco de acesso indevido.

O bloqueio do uso de unidades de armazenamento externo nas estações de usuário se mostrou extremamente importante, primeiro pelo fato de diminuir a incidência de infecções por vírus e *malwares*, em segundo por dificultar o vazamento de informações da empresa, que poderiam facilmente ser gravadas nestes dispositivos.

Com o bloqueio das propriedades do navegador de internet para os usuários, a navegação de internet se tornou mais segura, pois impede que o usuário altere o nível de segurança especificado pelo administrador de redes.

4 Conclusões e considerações finais

O profissional de segurança da informação deve estar preparado para utilizar todos os recursos tecnológicos à sua disposição a fim de tentar inibir ao máximo a ação indevida dos usuários e dificultar a propagação de ameaças no ambiente computacional.

O uso do *Active Directory* juntamente com o auxílio das GPOs, traz uma enorme vantagem na administração do ambiente de rede para o administrador desta, facilitando a implementação de medidas preventivas de segurança.

A adoção das medidas de segurança citadas neste relatório contribuiu para a diminuição do risco de incidentes de segurança da informação dentro da organização, pois diminui o risco de erro humano na operação dos computadores. Aliadas a outras medidas preventivas e de proteção, ajudaram a elevar o nível de maturidade da segurança da informação dentro da organização.

5 REFERÊNCIAS BIBLIOGRÁFICAS:

BRANDÃO, Robson. Introdução a Group Policy (GPO). 2018. Disponível em: https://technet.microsoft.com/pt-br/library/cc668545(d=printer).aspx. Acesso em: 17 nov. 2018.

BURGESS, Mark, Princípios de administração de redes e sistemas / Mark Burgess; tradução Aldir José Coelho Corrêa da Silva; revisão técnica Rodney Ferreira de Carvalho. – Rio de Janeiro : LTC, 2006.

FONTES, Edison, Segurança da informação: o usuário faz a diferença / Edison Fontes – São Paulo : Saraiva, 2006.

MICROSOFT. Visão geral dos serviços de domínio do Active Directory. 2017. Disponível em: <https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>. Acesso em: 22/05/2019.

PORTALGSTI. O que é Active Directory (AD). Disponível em https://www.portalgsti.com.br/active-directory/sobre/. Acesso em 31/05/2019