Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

ARTHUR ANDRÉ DA SILVA VIEIRA

PROPOSTA DE *HARDENING* DE AMBIENTE *WINDOWS* PARA INSTITUIÇÃO BANCÁRIA

Brasília
2015

ARTHUR ANDRÉ DA SILVA VIEIRA

PROPOSTA DE *HARDENING* DE AMBIENTE *WINDOWS* PARA INSTITUIÇÃO BANCÁRIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof.Esp. Sylas Mendes

Brasília
2015

ARTHUR ANDRÉ DA SILVA VIEIRA

PROPOSTA DE *HARDENING* DE AMBIENTE *WINDOWS* PARA INSTITUIÇÃO BANCÁRIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. Esp. Sylas Mendes

Brasília, ___ de _____ de 2015.

Banca Examinadora

_____

Prof. Dr. Nome completo

_____

Prof. Dr. Nome completo

DEDICATORIA

Dedico este trabalho final de conclusão do curso a minha família, que me apoiou;

Ao UniCEUB, por ter acreditado na Pós-Graduação em Redes de Computadores com ênfase em Segurança e a meu orientador, Professor que, me orientou no decorrer deste trabalho

RESUMO

Este estudo de caso apresenta uma proposta para implantar o *Hardening* de Ambiente *Windows* na instituição financeira Banco X. Serão demonstradas técnicas de proteção para servidores e estações, utilizando normas técnicas e soluções de software para preservação de dados, monitoração, autenticação e controle de acesso à rede e proteção de dados manipulados pelos usuários finais. Na busca das informações, utilizou-se para o desenvolvimento do estudo a pesquisa bibliográfica e análise de estruturas existente em instituição real. No decorrer do trabalho serão analisadas a estrutura atual da empresa e suas falhas de segurança da informação, que geraram a necessidade de proteger os dados e as motivações para implantação de um piloto de *Hardening* de Ambiente *Windows* em um setor limitado do Banco, além do detalhamento do processo e projeções futuras. Tendo como resultado, o controle total do que está sendo atualizado nos servidores e estações com a aplicação WSUS e a ferramenta GPO, ambas nativas do Sistema Operacional Windows Server. Mantendo as falhas sempre mitigadas pelo fabricante. Como resultado nas estações de trabalho, essa proposta irá proteger as máquinas contra instalações não autorizadas de softwares no parque tecnológico e o controle total de informações que estão trafegando nos dispositívos móveis que os usuários utilizam.

Palavras-chave: *Hardening*. *Windows*. Segurança.

ABSTRACT

This case study presents a proposal to deploy Windows Environment Hardening the financial institution Bank X. It will be demonstrated protection techniques for servers and workstations, using technical standards and software solutions for data preservation, monitoring, authentication and access control network and data protection manipulated by end users. In the search for information, it was used to study the development literature search and analysis of existing structures in real institution. During the work will be analyzed the current structure of the company and its information security failures that led to the need to protect data and motivations for deploying a Windows Environment Hardening pilot in a limited sector of the Bank, in addition to detailing the process and future projections. As a result, the full control of what is being updated on the servers and stations with the WSUS application and GPO tool, both native OS Windows Server. Keeping failures always mitigated by the manufacturer. As a result the workstations, this proposal will shield machines, facilities against unauthorized software Technology Park and in total control of information that is traveling on the mobile devices that users use.

Keywords*: Hardening. Windows. Security.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AIF – Área de informática

CLI – *Command Line Interface*

CPU – *Central Processing Unit*

DHCP – *Dynamic Host Configuration Protocol*

DNS – *Domain Name System*

ePO – *ePolicy Orchestrator*

FTP – *File Transport Protocol*

GPO – *Group Policy Object*

IIS – *Internet Information Services*

MMC – *Microsoft Management Console*

NTP – *Network Time Protocol*

RAM – *Read Access Memory*

SCCM – *System Center Configuration Manager*

SID – *Security Identifiers*

SO – Sistema Operacional

SP2 – *Service Pack* 2

SQL – *Structured Query Language*

TI – Tecnologia da Informação

WINS – *Windows Internet Name Service*

WSUS – *Windows Server Update Services*

SUMÁRIO

INTRODUÇÃO

De acordo com Nascimento (2014), as instituições bancárias, assim como as atividades deste segmento estão seguindo a tendência evolutiva do mercado, onde o volume de informações armazenadas e trafegadas cresce de forma exponencial, onde cresce cada vez mais o número de ameaças à integridade e confidencialidade desses dados.

Segundo a Federação Brasileira de Bancos, a capacidade de dados dos bancos cresceu mais de 350% nos últimos cinco anos. Tamanha exposição faz com que os bancos se tornem alvos constantes de crimes envolvendo invasão e fraudes em seus sistemas. Estima-se que os 10 maiores bancos brasileiros perderam mais de R$3 bilhões com fraudes em 2012 (FEBRABAN, 2014).

Silva (2015) diz que:

> No meio tecnológico, o principal causador desses problemas são pessoas denominadas como *Crackers*, caracterizados por possuírem certo nível específico de conhecimentos informáticos, e utilizam este para invadir sistemas, coletar dados e informações, por brechas e lacunas que na maioria das vezes são desprezadas pelos administradores de sistemas. Normalmente eles executam teste de segurança, explorando as vulnerabilidades, pontos falhos e, a partir daí, iniciam seus ataques através da internet, passando assim a adquirir informações sigilosas utilizando-as para benefício próprio.

Com esta evolução, a segurança da informação tornou-se um assunto para sempre estar em evidência neste modelo de organização, sendo necessário existir a necessidade de blindar o ambiente contra a manipulação e extração de dados indevidamente. Um processo comum e muito eficiente é o *Hardening*, que é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas (DIOGENES; MAUSER, 2014).

A TI do Banco X começou o estudo de uma proposta para implantação do processo de *Hardening* de ambiente Windows, que atenderá primeiramente à AIF/DF (Área de Informática/Distrito Federal), como ambiente de homologação.

Baseado na análise dos produtos, optou-se por utilizar as ferramentas nativas do Windows Server, WSUS (Windows Server Update Services) e GPO (Group Policy Object), para organizar atualizações e propagar medidas de

segurança para o ambiente destacado (*MICROSOFT*, 2015). Além das ferramentas da Mcafee, DLP (Data Loss Prevention) e *Application Control*, aproveitando a estrutura básica já implementada a nível nacional (MCAFEE, 2015).

OBJETIVO GERAL

Propor e especificar meios e processos, para implantar o *Hardening* de Ambiente Windows na instituição Banco X.

OBJETIVOS ESPECÍFICOS

- Efetuar o levantamento de infraestrutura, para criar uma base de conhecimento para iniciar uma implementação piloto na AIF/DF (Área de Informática)
- Apresentar os conceitos técnicos do WSUS e GPO, além da Suíte McAfee (DLP e *Application Control*) para gerenciamento do ambiente Windows.
- Demonstrar os passos de instalação e configuração dos serviços propostos.

Para alcançar esses objetivos, procedeu-se da seguinte maneira: uso de literatura específica e atualizada, consulta a normas internacionais, documentação das tecnologias propostas e embasamento em situações reais.

Espera-se demonstrar com este estudo a importância de controlar o fluxo de informações, tanto no meio lógico, quanto no cotidiano dos colaboradores, mitigando todos os riscos possíveis contra-ataques e ameaças.

O presente trabalho foi então estruturado em 4 capítulos.

No primeiro capítulo apresenta-se a Revisão Conceitual, abordando as tecnologias utilizadas para o projeto e suas devidas funcionalidades e processos. No segundo capítulo, o estudo de caso é apresentado, com descrição da empresa e infraestrutura implementada atualmente. Em seguida, no terceiro capítulo, a etapa técnica da proposta será apresentada, mostrando a instalação e configuração das ferramentas em destaque. Finalizando com o quarto capítulo, apresentando os

projetos futuros, expansão da implementação e novas tecnologias que poderão ser aplicadas.

1 REVISÃO CONCEITUAL

1.1 *Hardening*

Segundo Yuri Diogenes e Daniel Mauser (2013), *hardening* é um processo de reforço de segurança de sistema, onde todos os componentes interconectados em uma rede e que fazem uso dele, como dispositivos, sistemas e aplicativos, terão diretrizes especificas de reforço de segurança.

De acordo com Reis, Verbena e Júlio (2015), com o grande aumento no número de ameaças existentes na Internet é fundamental que o sistema de um servidor esteja preparado para superar todas as tentativas de invasão. Esta técnica não deve ser implementada somente em servidores que ficam conectados diretamente a Internet, muitas vezes fornecendo serviços como, por exemplo servidores web, mas também em máquinas que provêm serviços internos de rede como servidores de arquivos e de impressão. Com o *hardening* de sistemas é possível aumentar o desempenho do hardware, liberando recursos que estão sendo utilizados por aplicativos desnecessários, implementando configurações específicas em alguns serviços, além de gerar um ambiente mais seguro.

Devido ao crescente número de ameaças existentes na Internet e dentro dos ambientes corporativos, se faz necessária a utilização de técnicas capazes de proporcionar maior segurança, estabilidade e tranquilidade para os administradores de redes (*HARDENING*, 2015).

A técnica de *Hardening* pode ser utilizada em qualquer sistema operacional, implementando medidas e ações com o objetivo de fortalecer a segurança e proteger o sistema de possíveis invasores. A implementação das diretivas de segurança deve ser seguida antes, durante e após a instalação e configuração do sistema operacional em uso (TECNOLOGIA DA INFORMAÇÃO, 2013).

1.2 WSUS

Um dos aspectos básicos do *hardening* nos sistemas é aplicação de atualizações de segurança para que haja resistência a ataques. Dependendo do sistema operacional, existem diferentes terminologias para assegurar que esta atualização é voltada para a correção de vulnerabilidades de segurança. O termo geral mais comum é patch de segurança. (DIOGENES; MAUSER, 2014, p.57).

As atualizações de segurança são hoje publicadas pelos fabricantes do Sistema Operacional de forma periódica, e um desafio inicial era o gerenciamento das mesmas. O usuário pode optar e configurar os sistemas e tomar algumas decisões sobre como elas serão instaladas: (DIOGENES; MAUSER, 2014)

- Instalar atualizações automaticamente
- Baixar atualizações, mas permitir que eu escolha quando instalá-las;
- Procurar atualizações, mas permitir que eu escolha quando baixá-las e instalá-las;
- Nunca verificar se há atualizações.

Algumas empresas precisam de um controle mais preciso sobre atualizações, não apenas sobre o aspecto de segurança de controlar se eles estão aplicados de maneira consistente, mas também sobre funcionalidade, onde algumas atualizações de segurança podem introduzir problemas de compatibilidade. Há alguns casos em que algumas aplicações falham ou mudam de comportamento.

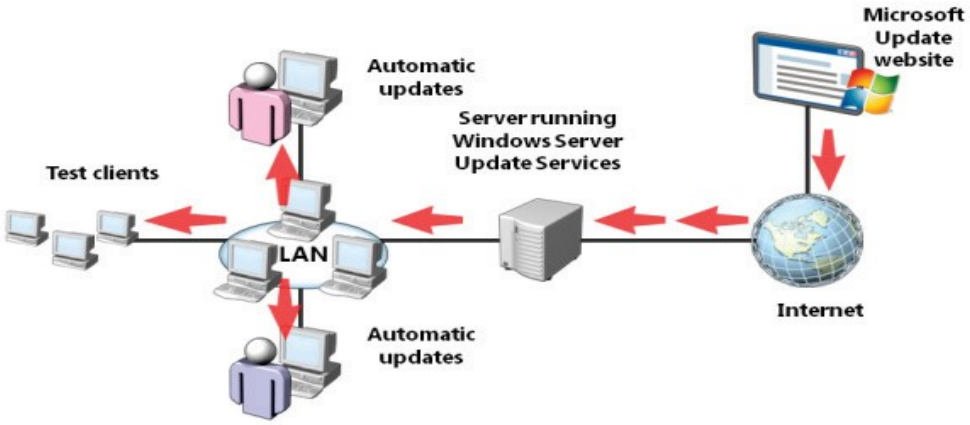
As empresas necessitam de um gerenciamento de atualizações, de forma a minimizar o impacto introduzido pelas atualizações. Isto é feito de forma controlada através de um sistema de gerenciamento de atualizações e um ambiente de homologação ou rede de laboratório, para que as mesmas sejam testadas antes de serem implementadas. (DIOGENES; MAUSER, 2014, p.60).

Para se adequar ao Sistema Operacional Windows Server 2012, utiliza-se o WSUS, a fabricante Microsoft (2015) demonstra que:

> Windows Server Update Services. O Windows Server Update Services (WSUS) permite que os administradores de tecnologia da informação implantem as atualizações mais recentes dos produtos nos computadores que estiverem executando o sistema operacional Windows.

A figura 1 demonstra a estrutura do WSUS:

Figura 1: Estrutura do WSUS



Fonte: Adminstering Windows Server 2012 – Microsoft, 2011

O WSUS pode obter atualizações que são aplicáveis para os S.O Windows e aplicativos como Office e SQL Server. As organizações podem criar uma hierarquia de servidores WSUS. Neste cenário um único servidor WSUS centralizado obtém as atualizações do Microsoft Update e outros servidores WSUS recebem atualizações a partir dele. (MICROSOFT,2012)

Pode-se organizar computadores em grupos para simplificar a aprovação das alterações. Por exemplo, pode-se configurar um grupo piloto para ser o primeiro conjunto de computadores que são usados para testar atualizações.

O WSUS pode gerar relatórios para ajudar com monitoramento de instalação da atualização. Estes relatórios podem identificar qual os computadores não foram aplicados as atualizações recém aprovadas. Com base nestes relatórios pode-se investigar o motivo de não serem aplicadas.

O processo de gerenciamento de atualizações permite que gerencie e mantenha o WSUS e suas atualizações. Este processo é um ciclo continuo, durante o qual pode-se reavaliar e ajustar a implantação para responder às novas necessidades. (MICROSOFT,2012)

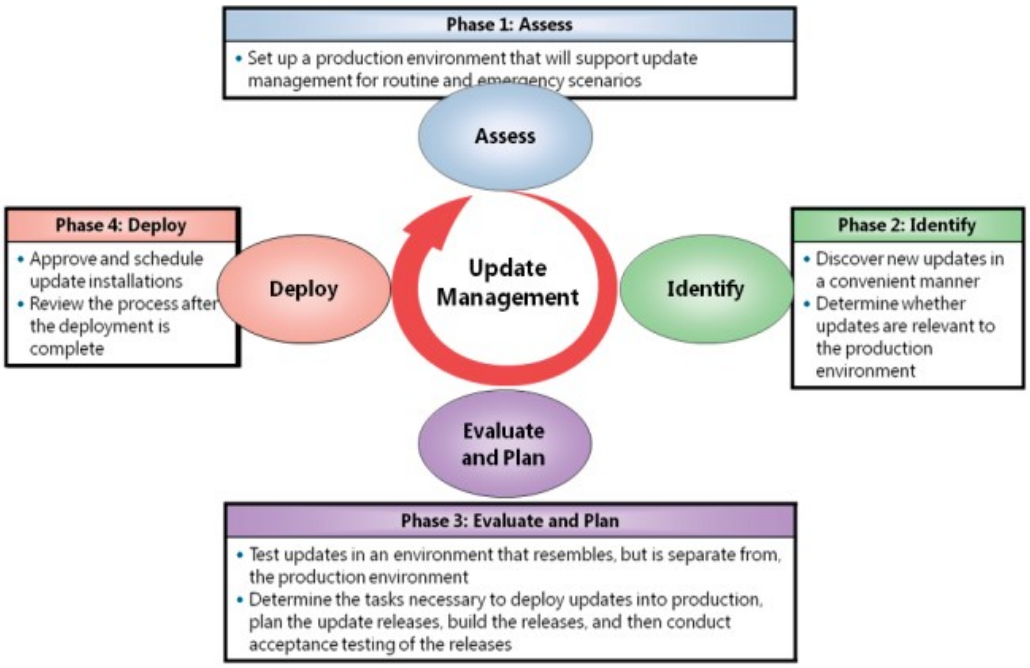
As quatro fases do gerenciamento de atualizações são:

- Avaliar
- Identificar

- Avaliar e Planejar
- Implantar

A figura 2 demonstra o processo de execução das quatro fases:

Figura 2: Fases de execução do WSUS



Fonte: Adminstering Windows Server 2012 – Microsoft, 2011

1.3 GPO

Uma das gigantescas tarefas de um administrador de sistemas é gerenciar usuários, grupos e computadores da rede. Imagine um parque de máquinas com 1500 *desktops* para gerenciar e precisa mudar uma configuração em todas elas. (PORTAL EDUCAÇÃO, 2008)

Manter um ambiente consistente em toda a organização é um desafio. Os administradores precisam de um mecanismo para configurar e impor configurações e restrições de usuário e computador. *Group Policy* (GPO) pode fornecer essa consistência, permitindo que os administradores possam gerenciar e aplicar definições de configuração central. (BRANDÃO, 2015)

A GPO, é capaz de mudar configurações, restringir ações ou até mesmo distribuir aplicações em seu ambiente de rede. As vantagens são muitas, e podem ser aplicadas em sites, domínios e *organizational units* (OUs). Se você criou uma OU para cada departamento da sua empresa, poderá então, fazer diferentes configurações de GPO para cada departamento. (BRANDÃO, 2015)

GPO é um objeto que contém uma ou mais definições de política aplicam definições de configuração para usuários, computadores ou ambos. GPOs são armazenadas no SYSVOL, e podem ser gerenciados usando o Console de Gerenciamento de Diretiva de Grupo (GPMC). Dentro do GPMC, você pode abrir e editar um GPO usando o Editor de Gestão de Políticas de Grupo. GPOs são logicamente vinculados a contêineres AD para aplicar as configurações para os objetos nesses recipientes. (MICROSOFT, 2015)

As GPOs são baseadas em *templates* que possuem uma lista de opções configuráveis de forma amigável. A maioria dos itens de uma GPO tem 3 diferentes opções:

Enable: Especifica que aquele item será ativado.

Disable: Especifica que aquele item será desativado.

Not Configured: Deixa a opção neutra, nem ativa e nem desativa o item, ou seja, fica como está agora. Esta é a configuração padrão (Portal Educação,2015).

Usuários e computadores possuem cada um, três áreas de configuração, como descritas na tabela a seguir:

Figura 3: Áreas de configuração GPO

Section	Description
Software settings	Contain software settings that can be deployed to either the user or the computer. Software that is deployed to a user is specific to that user. Software that is deployed to the computer is available to all users of that computer.
Windows operating system settings	Contain script settings and security settings for both user and computer, and Internet Explorer maintenance for the user configuration.
Administrative templates	Contain hundreds of settings that modify the registry to control various aspects of the user and computer environment. New administrative templates may be created by Microsoft or other vendors. You can add these new templates to the GPMC. For example, Microsoft has Office 2010 templates that are available for download, and that you can add to the GPMC.

Fonte: Administering Windows Server 2012 – Microsoft, 2011

1.4 *SolidCore: Application Control*

Empresas de todos os tamanhos precisam de uma maneira eficiente de padronizar sistemas e servidores para se certificar de que eles estão executando apenas softwares homologados, sem impactar a produtividade. O *Application Control* adiciona maior controle para a estratégia de segurança dos sistemas, sempre em sintonia com as necessidades operacionais das empresas. (MCAFEE, 2015)

O *Application control* é recomendado para empresas que possuem terminais aonde o cliente realiza funções críticas e muitas vezes armazenam dados confidenciais. Estende-se a uma camada de proteção para sistemas de função fixa, não tem impacto no ambiente, requerendo baixo nível de processamento.

Application Control é uma solução simples, que fornece:

- Fácil instalação e baixo custo operacional inicial e permanente.
- Impacto mínimo sobre os ciclos da CPU e usa menos de 10MB de RAM
- Não realiza varredura nos arquivos, ação que gera impacto no desempenho do sistema
- Não requer atualizações de assinatura.
- Fornece um gerenciamento dinâmico e flexível de *whistelist*. Podendo suportar múltiplas configurações para diferentes necessidades de negócios.

Utilizando um modelo de fonte confiável, elimina a necessidade dos Administradores de TI, manterem manualmente lista de aplicações aprovadas. Apenas softwares permitidos são executados e não podem ser alterados. Impede tentativas de manipulação de arquivos protegidos, cria eventos para cada tentativa, gerando logs para as mesmas. (MCAFEE,2015)

1.5 DLP

A perda de dados é quando a informação confidencial ou privada deixa a empresa como resultado de uma comunicação não autorizada, através de canais como aplicativos, dispositivos físicos ou protocolos de rede.

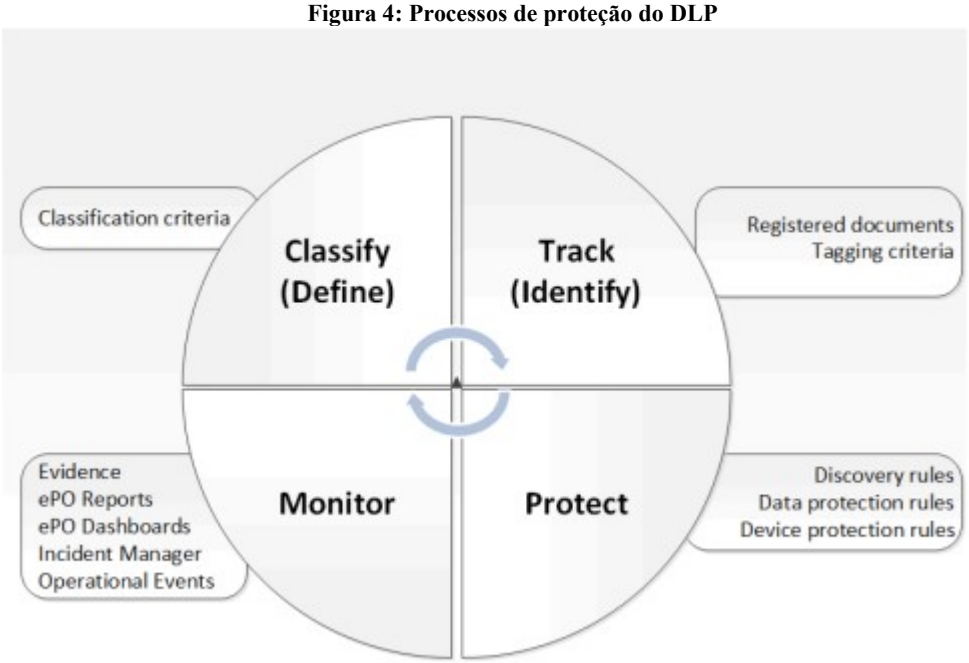
Um software de prevenção de perdas reforça as políticas de segurança da informação pré-definidas para evitar tais perdas. No caso o McAfee DLP, que é gerenciado pelo McAfee ePolicy Orchestrator (MCAFEE, 2015).

De acordo com a McAfee, fabricante do produto, o DLP é uma solução que inspeciona as ações dos usuários empresariais, em matéria de conteúdo sensível em seu próprio ambiente de trabalho, seus computadores.

DLP, protege informações empresariais sensíveis, implantando políticas, que consiste em definições, classificações, conjuntos de regras e configurações do cliente endpoint. Ele monitora as políticas e ações definidas com conteúdo sensível. Pode criptografar o conteúdo sensível antes de permitir o prosseguimento do processo. Por último, cria relatórios para análise e controle, podendo armazenar o conteúdo como evidência. (MCAFEE, 2015)

Os processos de proteção podem ser vistos na Figura 3 abaixo:

Figura 4: Processos de proteção do DLP



Fonte: ***McAfee Data Loss Prevention – Product Guide***

O cliente DLP Endpoint, é responsável por classificar, controlar e proteger os aspectos do processo. A extensão DLP em McAfee ePO, é responsável por

configurar a classificação, condições, critérios de rastreamento e regras de proteção que se aplicam a dados copiados, enviados, impressos ou transmitidos a partir do ponto de extremidade (MCAFEE, 2015).

2 DESCRIÇÂO DA EMPRESA

O Banco X é uma instituição financeira de grande porte, suas principais áres de atuação são a promoção da cidadania, o desenvolvimento sustentável do país, o agenciamento de políticas públicas do governo federal e os financiamentos de habitação, financiamentos educacionais, além de executar a carteira comercial, captando recursos através de conta poupança e conta corrente.

O Banco X está presente em todas as capitais e municípios brasileiros, atualmente, conta com 3000 agências espalhadas pelo Brasil, 100.000 empregados e 50.000 colaboradores entre estagiários e prestadores.

2.1 Infraestrutura

A Rede do Banco X encontra-se em um baixo nível de maturidade relacionada a segurança da informação e padronização de servidores. Apesar do investimento massivo aplicado à tecnologia, existe muitos pontos falhos nesta estrutura.

Toda a rede está em um modelo que interliga suas agências ao *datacenter*, possuindo prédios administrativos aonde encontra-se as AIF's (Área de Informática - Centralizadora de Informática), que funcionam como filiais e concentradoras de rede.

Todo o ambiente do Banco X é baseado em *software* Micrososft, apresentando Windows 2012 Server em seus servidores e Windows 8 nas estações de trabalho.

Nele encontra-se servidores com diversas aplicações:

- *Active Directory*/ DNS/ WINS/ DHCP
- *Exchange* – Correio Eletrônico
- Banco de Dados SQL Server
- Aplicação *Web* – *Sites*
- Intranet
- Servidores de Virtualização – VMWare

- Aplicações Bancárias
- Chaves de Criptografia
- Endpoint ePO (Anti Vírus) – McAfee
- Armazenamento (FTP)

Neste trabalho será apresentado um piloto da implantação de *Hardening* nos servidores críticos e estações de trabalho no prédio da AIF/DF. Nela existem 400 funcionários e colaboradores e 450 máquinas entre servidores e estações.

2.3 Ameaças

O controle de políticas, atualizações e aplicações presentes no ambiente Windows, é uma necessidade para mitigar riscos contra as informações presentes na mesma. A administração de um ambiente com um grande número de máquinas, se tornaria complicada se tivesse a necessidade de controlar se todas estão com as devidas atualizações, se as aplicações estão em conformidade com o plano de negócio da organização e o que o usuário está inserindo ou retirando da respectiva estação. Sem contar com toda as brechas de segurança encontrada neste caso.

Partindo dessa necessidade, empresas implementam o *Hardening* de Servidores e estações, blindando seu ambiente contra falhas em pontos chaves da rede, aonde todas as respectivas atualizações de Sistemas e softwares sejam homologadas e aplicadas, limitação de aplicações ao objetivo proposto, controle de permissões de acesso para cada área, controlando e monitorando o que pode ser armazenado e transferido das estações e o mais significativo, conscientizando o usuário sobre segurança da informação.

O Banco X, com os resultados de testes de vulnerabilidade, solicitados à equipe de segurança interna, identificou sistemas e aplicações sem packs de correções, muitos serviços e softwares obsoletos e sem uso, logs de eventos falhos, sem informações concretas e de difícil interpretação e a situação mais crítica, contas de *Admin* e *Guest* habilitadas, mostrando um baixo nível de maturidade da organização em relação à segurança de seus ativos e patrimônio de informações.

Com os testes de vulnerabilidade e relatórios extraídos do AntiVírus, constatou-se um enorme número de detecções provenientes de pen drives, com arquivos não pertinentes ao negócio da organização, além de um grande número de

aplicações não homologadas nestas estações, focadas aos interesses pessoais de seus respectivos usuários.

2.4. Justificativa

Com o objetivo de demonstrar uma infraestrutura com a técnica de *Hardening* aplicada de forma automatizada, será elaborado um piloto na AIF/DF com as tecnologias citadas.

3 PROJETO PROPOSTO

No ambiente do Banco X, temos as áreas contendo os servidores, que fornecem os serviços necessários às atividades da AIF/DF e as respectivas estações dos colaboradores da organização.

Após a análise de vulnerabilidade realizada pela equipe de segurança, constatou-se vulnerabilidades no ambiente dos servidores e estações. Os servidores não estavam devidamente atualizados e sincronizados, deixando brechas já detectadas pelo fabricante do Sistema Operacional expostas. As senhas utilizadas não atendiam a um padrão de segurança e os eventos que ocorriam nos servidores não estava sendo registrados e devidamente analisados. Além de não existir uma sincronia no relógio dos servidores e estações, trazendo um funcionamento irregular de várias aplicações.

Para tratar as referidas vulnerabilidades, as ferramentas WSUS e GPO serão propostas para atender a estas necessidades relatadas, trazendo conformidade e padronização ao ambiente dos servidores.

As vulnerabilidades das estações de trabalho são referentes às ações de seus usuários, movimentação indevida de dados e informações, instalação de aplicações não homologadas pela organização, necessitando de um maior controle e restrição de uso por parte dos mesmos. Com o uso do DLP e Application Control, estas necessidades serão atendidas.

3.1 Instalação do WSUS

O WSUS é distribuído gratuitamente pela fabricante Microsoft, a versão escolhida para ser instalada no ambiente é a WSUS 3.0 SP2 (MICROSOFT,2015).

Um servidor Windows Server 2012 será dedicado a este serviço, sendo instalado via executável WUSSetup.exe.

A ferramenta possui os seguintes pré-requisitos:

- *Windows 2003 ~ 2012 Server*
- *Internet Information Services (IIS) 6.0 or newer*
- *Microsoft .NET Framework 2.0 or newer*
- *Microsoft Management Console (MMC) 3.0*
- *Microsoft Report Viewer Redistributable 2008 or later*
- *SQL Server 2012, SQL Server 2008, SQL Server 2005 SP2, or Windows Internal Database*

Como requisitos de *hardware*, são os mesmos solicitados para instalar o Sistema Operacional *Windows Server*, solicitando 10GB para instalação e 30GB para *download* de *updates*. Um único WSUS pode suportar milhares de *clients*, porém recomenda-se que em casos extremos existam vários WSUS's, para amenizar o consumo dos links de rede (MICROSOFT, 2015).

Para instalar os seguintes passos serão executados:

1. – Fazer *logon* no servidor com uma conta membro do grupo Administradores
2. – Executar o arquivo de instalação WSUSSetup.exe
3. – Selecione Instalação Completa do servidor incluindo o Console de Administração
4. – Aceitar os termos do Contrato de Licença
5. – Especificar aonde os clientes obterão as atualizações.
6. - Selecionar o software e base do banco de dados.
7. – Selecionar o site Web que o WSUS usará.
8. – Finalize a instalação do WSUS 3.0 SP2

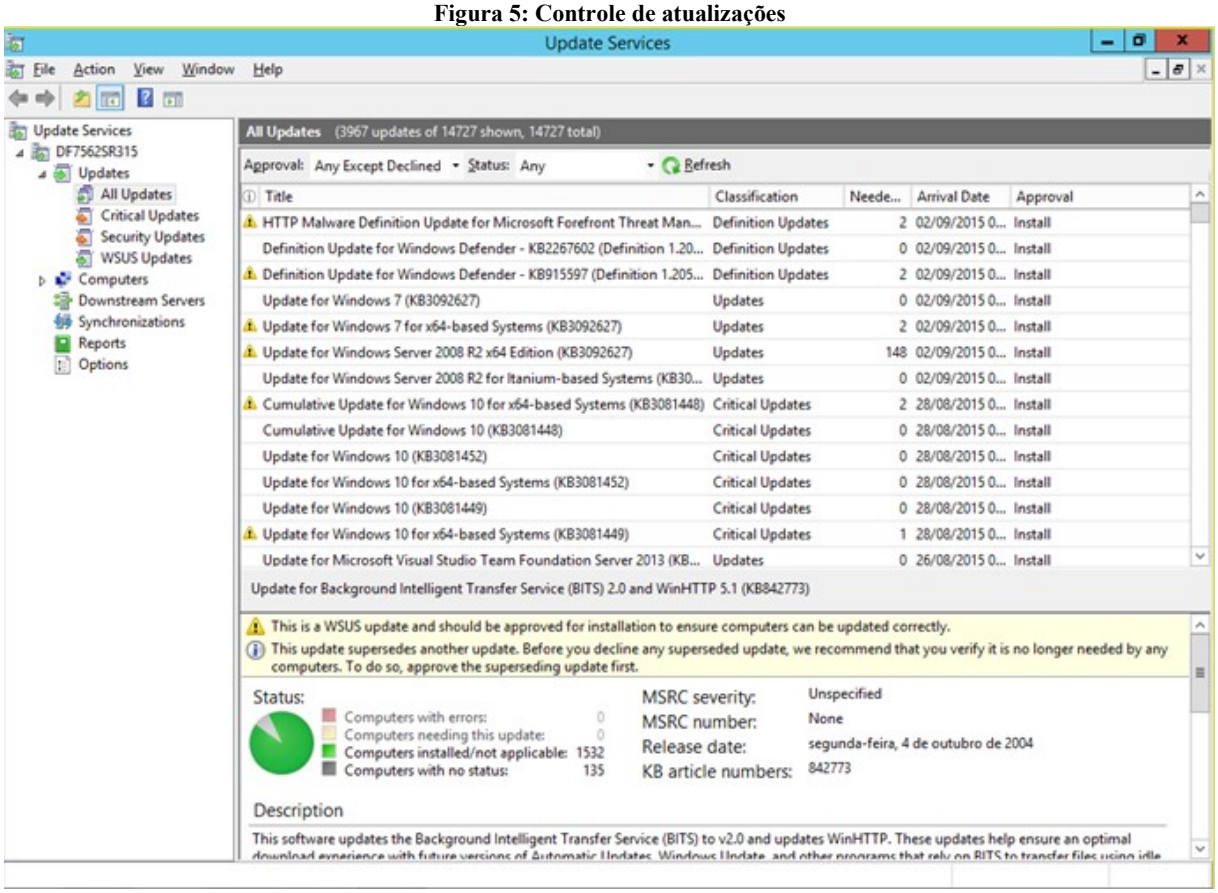
Utilizando a GPO para configurar *updates* automáticos, serão configurados os seguintes itens:

- Frequência de *updates*, determina a frequência em que os *updates* serão detectados.
- Agendamento de instalação de *updates*, determina quando os *updates* serão instalados.
- Determinar quando o computador será reiniciado, dependendo da solicitação dos *updates*.

A ferramenta será utilizada para:

- Identificar e baixar atualizações

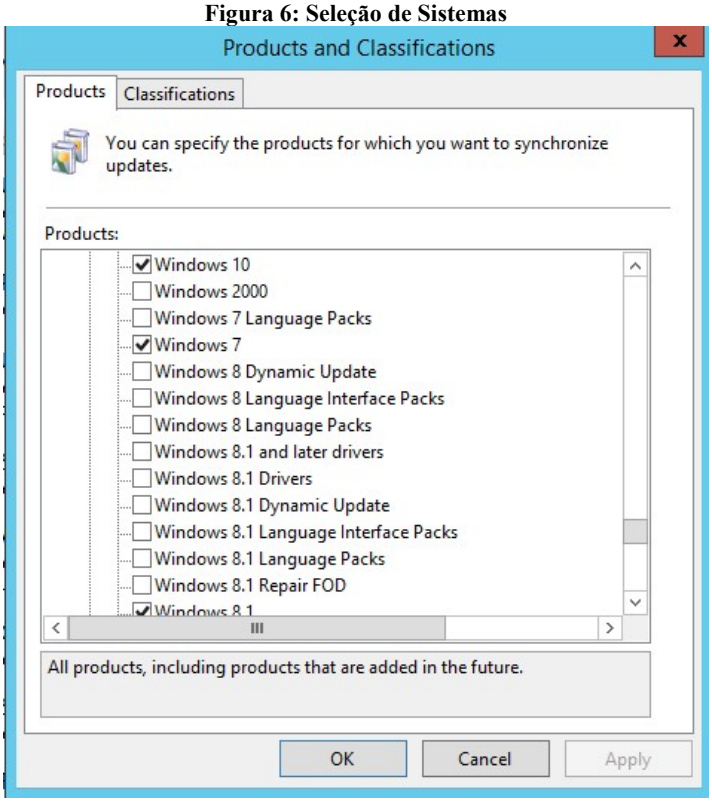
Figura 5: Controle de atualizações



Fonte: Elaboração do autor

- Aprovar atualizações para distribuição desejada

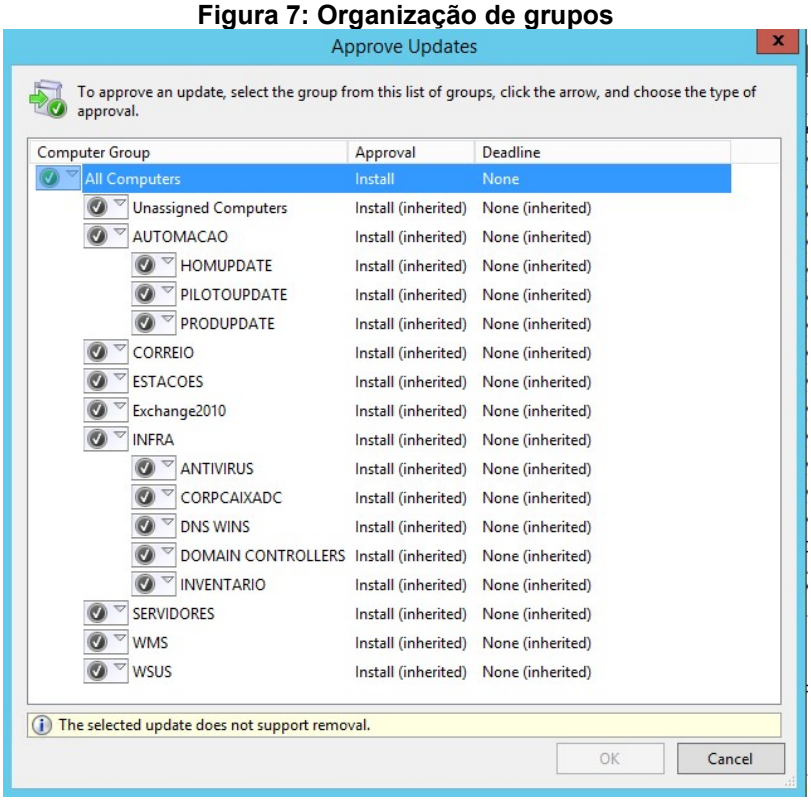
Figura 6: Seleção de Sistemas



Fonte: Elaboração do autor

- Organizar computadores em grupos

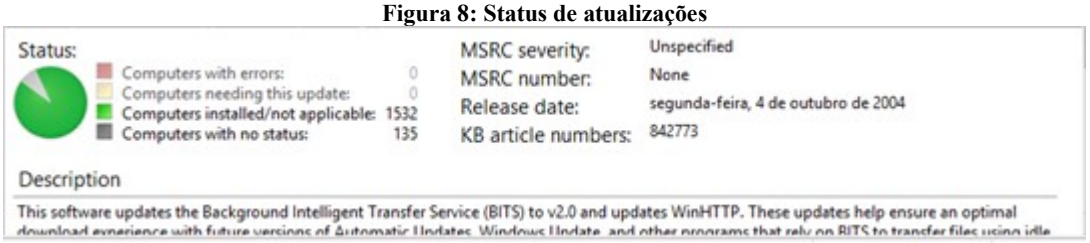
Figura 7: Organização de grupos



Fonte: Elaboração do autor

- Revisar o status de atualizações nos computadores

Figura 8: Status de atualizações



Fonte: Elaboração do autor

- Gerar relatórios

3.2 Implementação dp *Hardening Windows Server*

Para implementar o *Hardening* em servidores com o sistema operacional Windows Server, serão seguidos os itens abaixo (*HARDENING WINDOWS SERVER*, 2014):

- Instalação de *service pack* e *hotfix*

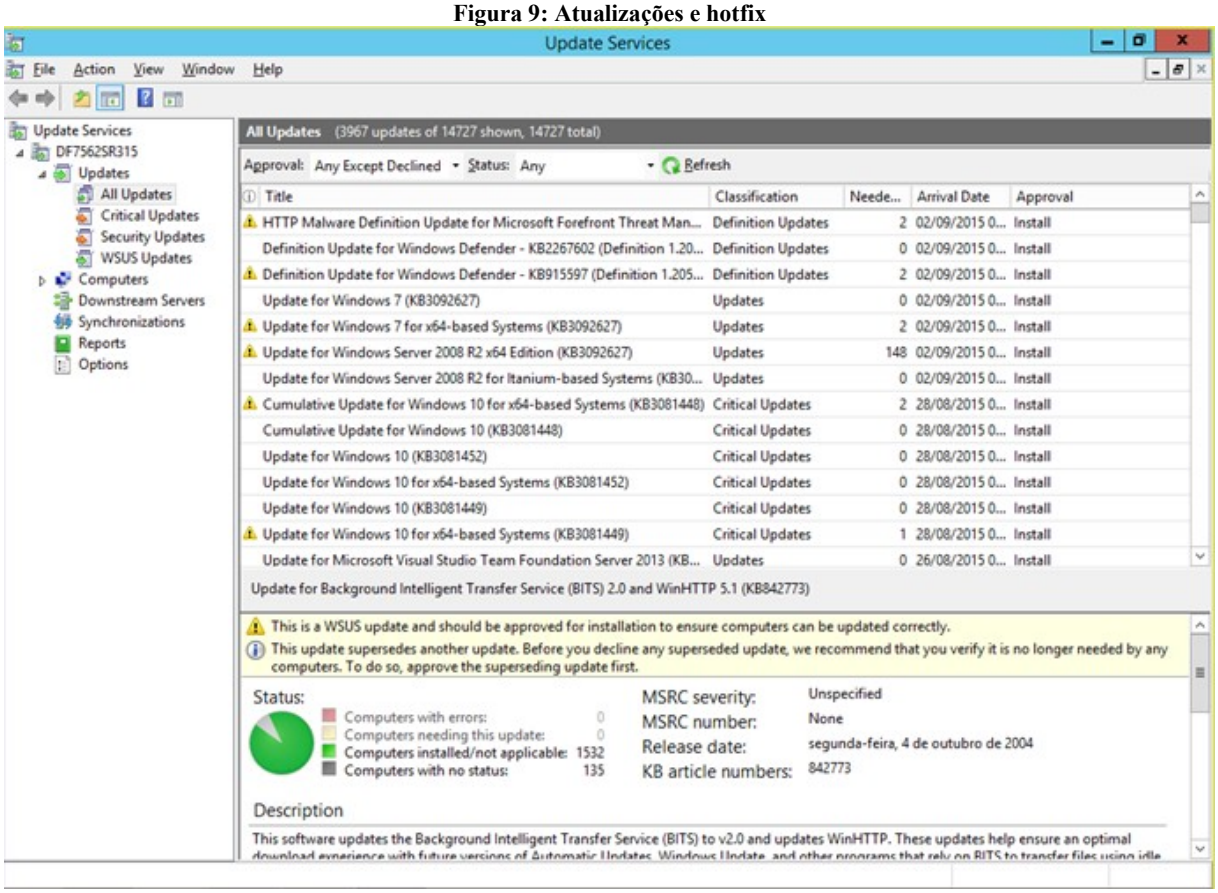
- Habilitar diretivas de senhas e log de eventos
- Habilitar auditorias
- Opções de segurança para o domínio
- Utilização de NTP para sincronismo do relógio do Windows
- Alteração do nome do usuário Administrador do Windows
- Desabilitar a conta *Guest*

3.2.1 Instalação de service Pack e Hotfix

Um dos aspectos básicos do *hardening* nos sistemas é aplicação de atualizações de segurança para que haja resistência a ataques. Dependendo do sistema operacional, existem diferentes terminologias para assegurar que esta atualização é voltada para a correção de vulnerabilidades de segurança. O termo geral mais comum é patch de segurança. (DIOGENES; MAUSER, 2014, p.57).

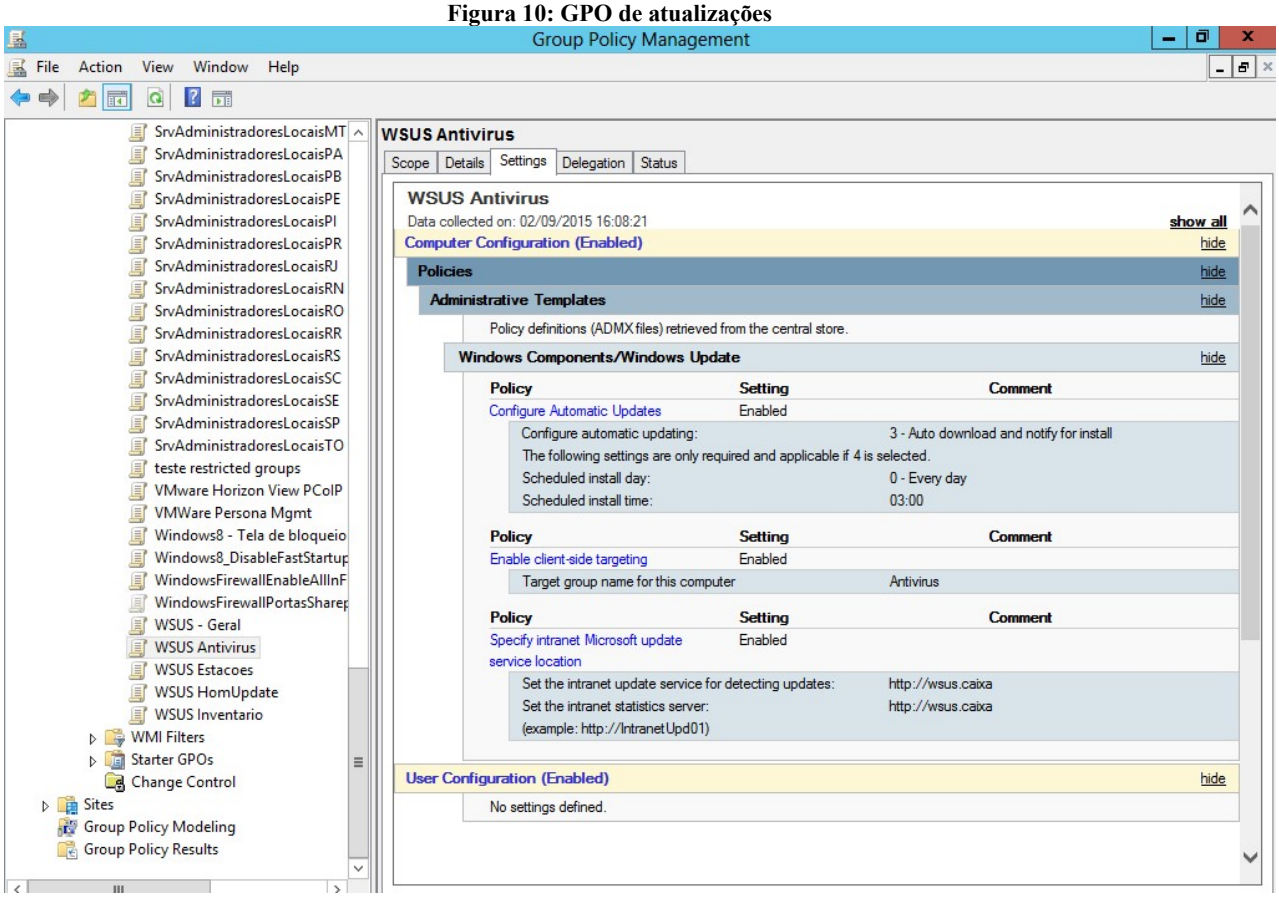
Realizado através do WSUS e habilitado através de GPO do domínio

Figura 9: Atualizações e hotfix



Fonte: Elaboração do autor

Figura 10: GPO de atualizações



Fonte: Elaboração do autor

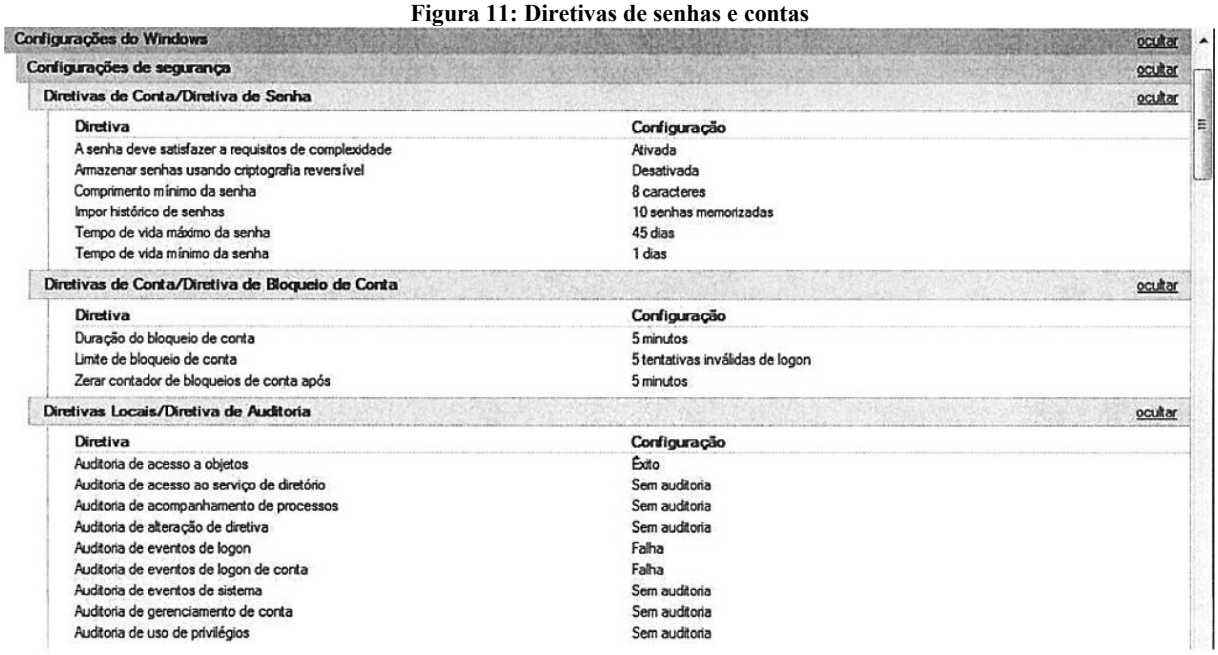
3.2.2. Habilitar diretivas de senhas e log de eventos

A diretiva de senha é um conjunto de regras criadas para melhoria da segurança dos sistemas, recomendando ou forçando que os usuários utilizem senhas fortes e evitando que usuários não autorizados façam uso da rede.

Logs são registros de atividades gerados por programas e serviços de um computador. Eles podem ficar armazenados em arquivos, na memória do computador ou em bases de dados. São um conjunto de registros com marcação temporal, que suportam apenas inserção, e que representam eventos que aconteceram em um computador ou equipamento de rede (MULLER, 2014).

Habilitado através de GPO do domínio

Figura 11: Diretivas de senhas e contas



Configurações do Windows — ocultar

Configurações de segurança — ocultar

Diretivas de Conta/Diretiva de Senha — ocultar

Diretiva	Configuração
A senha deve satisfazer a requisitos de complexidade	Ativada
Armazenar senhas usando criptografia reversível	Desativada
Comprimento mínimo da senha	8 caracteres
Impor histórico de senhas	10 senhas memorizadas
Tempo de vida máximo da senha	45 dias
Tempo de vida mínimo da senha	1 dias

Diretivas de Conta/Diretiva de Bloqueio de Conta — ocultar

Diretiva	Configuração
Duração do bloqueio de conta	5 minutos
Limite de bloqueio de conta	5 tentativas inválidas de logon
Zerar contador de bloqueios de conta após	5 minutos

Diretivas Locais/Diretiva de Auditoria — ocultar

Diretiva	Configuração
Auditoria de acesso a objetos	Êxito
Auditoria de acesso ao serviço de diretório	Sem auditoria
Auditoria de acompanhamento de processos	Sem auditoria
Auditoria de alteração de diretiva	Sem auditoria
Auditoria de eventos de logon	Falha
Auditoria de eventos de logon de conta	Falha
Auditoria de eventos de sistema	Sem auditoria
Auditoria de gerenciamento de conta	Sem auditoria
Auditoria de uso de privilégios	Sem auditoria

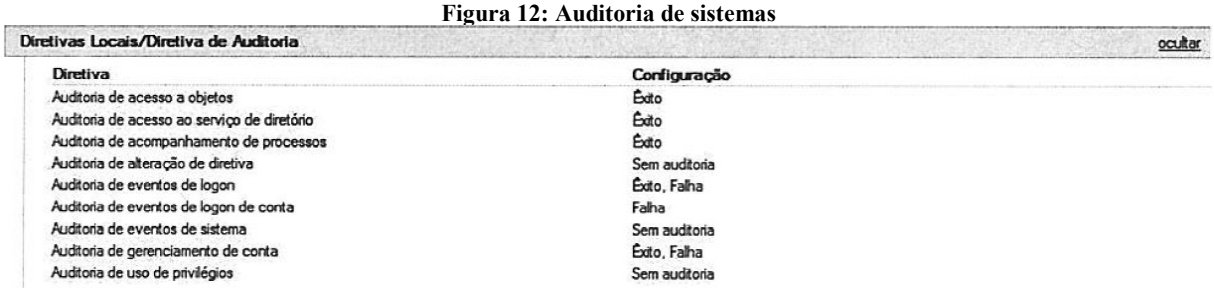
Fonte: Elaboração do autor

3.2.3. Habilitar auditorias

Auditoria de segurança é uma das ferramentas mais avançadas para ajudar a manter a segurança do seu sistema. Como parte da estratégia de segurança geral, você deve determinar o nível de auditoria adequado para seu ambiente. A auditoria deve identificar ataques, bem-sucedidos ou não, que representem uma ameaça à rede ou ataques contra recursos que você tenha considerado importantes na avaliação de riscos (MICROSOFT, 2010).

Habilitado através de GPO do domínio

Figura 12: Auditoria de sistemas



Diretivas Locais/Diretiva de Auditoria — ocultar

Diretiva	Configuração
Auditoria de acesso a objetos	Êxito
Auditoria de acesso ao serviço de diretório	Êxito
Auditoria de acompanhamento de processos	Êxito
Auditoria de alteração de diretiva	Sem auditoria
Auditoria de eventos de logon	Êxito, Falha
Auditoria de eventos de logon de conta	Falha
Auditoria de eventos de sistema	Sem auditoria
Auditoria de gerenciamento de conta	Êxito, Falha
Auditoria de uso de privilégios	Sem auditoria

Fonte: Elaboração do autor

3.2.4 Opções de segurança para o domínio

Habilitar através de GPO do domínio

Figura 13: Segurança para domínio

Diretivas Locais/Opções de Segurança		ocultar
Controlador de domínio		ocultar
Diretiva	**Configuração**	
Controlador de domínio: requisitos de assinatura de servidor LDAP	Nenhum	
Membro do Domínio		ocultar
Diretiva	**Configuração**	
Membro do domínio: criptografar ou assinar digitalmente os dados de canal seguro (sempre)	Ativada	
Segurança de Rede		ocultar
Diretiva	**Configuração**	
Segurança de rede: nível de autenticação LAN Manager	Enviar somente resposta NTLM	
Servidor de Rede Microsoft		ocultar
Diretiva	**Configuração**	
Servidor de rede Microsoft: assinar digitalmente a comunicação (se o cliente concordar)	Ativada	
Servidor de rede Microsoft: assinar digitalmente a comunicação (sempre)	Ativada	

Fonte: Elaboração do autor

3.2.5 Utilização de NTP para sincronismo do relógio do Windows

De acordo com Network Time Protocol (2014).

> O NTP é um protocolo para sincronização dos relógios dos computadores baseado no UDP para sincronização do relógio de um conjunto de computadores em redes de dados com latência variável. O NTP permite manter o relógio de um computador com a hora sempre certa e com grande exatidão.

Habilitado através de GPO do domínio

Figura 14: NTP

Sistema/Serviço de Tempo do Windows/Provedores de Tempo			ocultar
Diretiva	**Configuração**		**comentário**
Configurar Windows NTP Client	Ativada		
NtpServer		172.20.30.155	
Type		NTP	
CrossSiteSyncFlags		2	
ResolvePeerBackoffMinutes		15	
ResolvePeerBackoffMaxTimes		7	
SpecialPollInterval		3600	
EventLogFlags		0	
Diretiva	**Configuração**		**comentário**
Habilitar Windows NTP Client	Ativada		
Habilitar Windows NTP Server	Ativada		

Fonte: Elaboração do autor

3.2.6 Alteração do nome do usuário Administrador do Windows

Essa configuração de segurança determina se um nome de conta diferente está associado ao identificador de segurança (SID) da conta Administrador. Como é notória a existência da conta Administrador em todos os computadores da família Windows Server, renomear a conta torna um pouco mais difícil para pessoas

não autorizadas adivinhar essa combinação de senha e nome de usuário com privilégios. (*HARDENING WINDOWS SERVER*, 2014)

3.2.7. Desabilitar a conta Guest

A conta *Guest* é usada por pessoas que não tem uma conta real no computador. Um usuário cuja conta está desativada, mas não excluída, também pode usar a conta convidado. A conta é desativada por padrão e recomenda-se que ela permaneça assim. (*HARDENING WINDOWS SERVER*, 2014)

3.3 *Hardening das estações de trabalho*

3.3.1 Implementação Data Loss Prevention

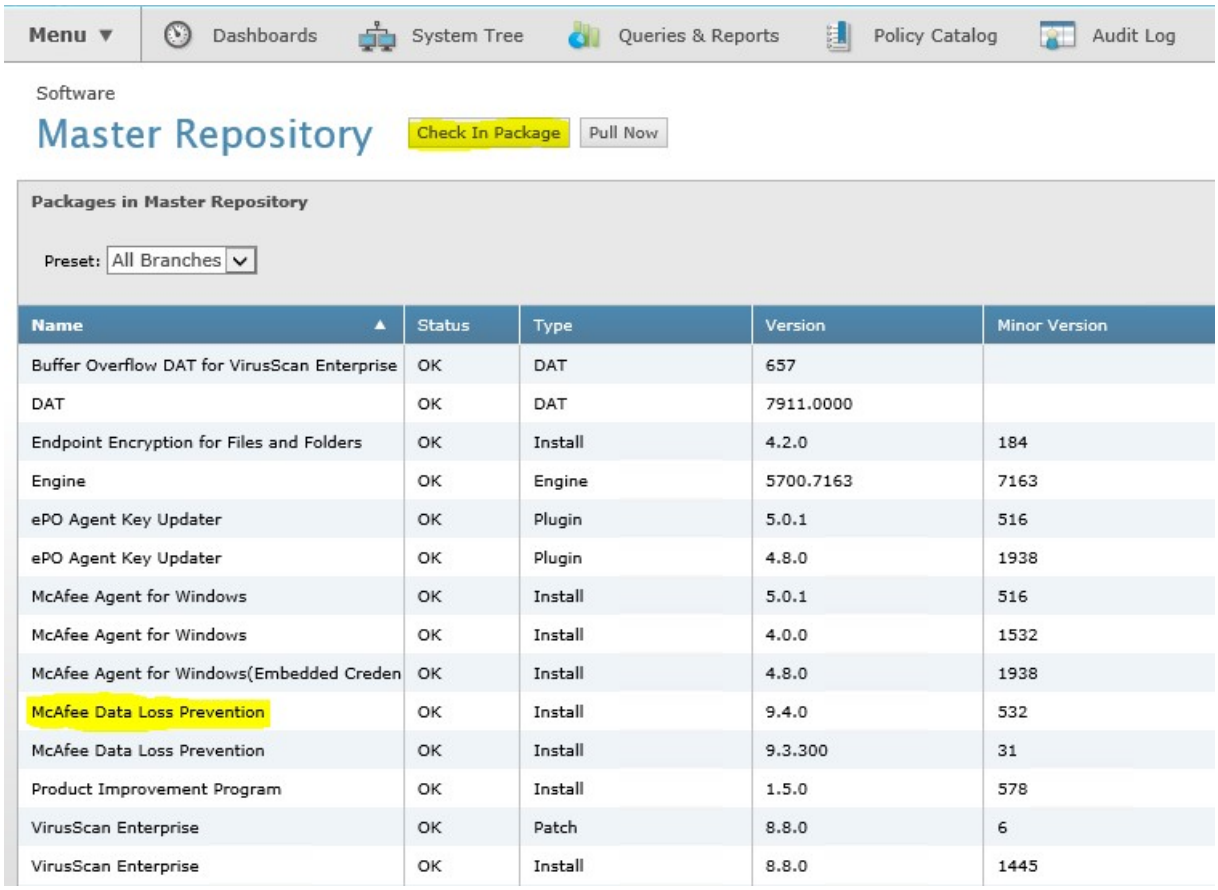
Sendo um produto McAfee, utilizando o número de licença já existente devido ao uso da aplicação de *Endpoint* e *AntiVírus* da mesma, realiza-se o download diretamente pelo site do fabricante.

A versão utilizada é a mais recente, DLP 9.4, possuindo os mesmos requisitos de Hardware e Sistema Operacional que o *Endpoint ePolicy Orchestrator* (ePO), plataforma que irá receber a aplicação DLP e controlar as regras e políticas para aplicação nas estações de trabalho, ao qual a ferramenta será destinada. (MCAFEE,2015)

Com os arquivos contendo o Pacote de Instalação e as Extensões de *report* de informações, deve-se checá-las no ePO.

No campo *Master Repository*, checar os Pacotes de Instalação:

Figura 15: Master Repository DLP

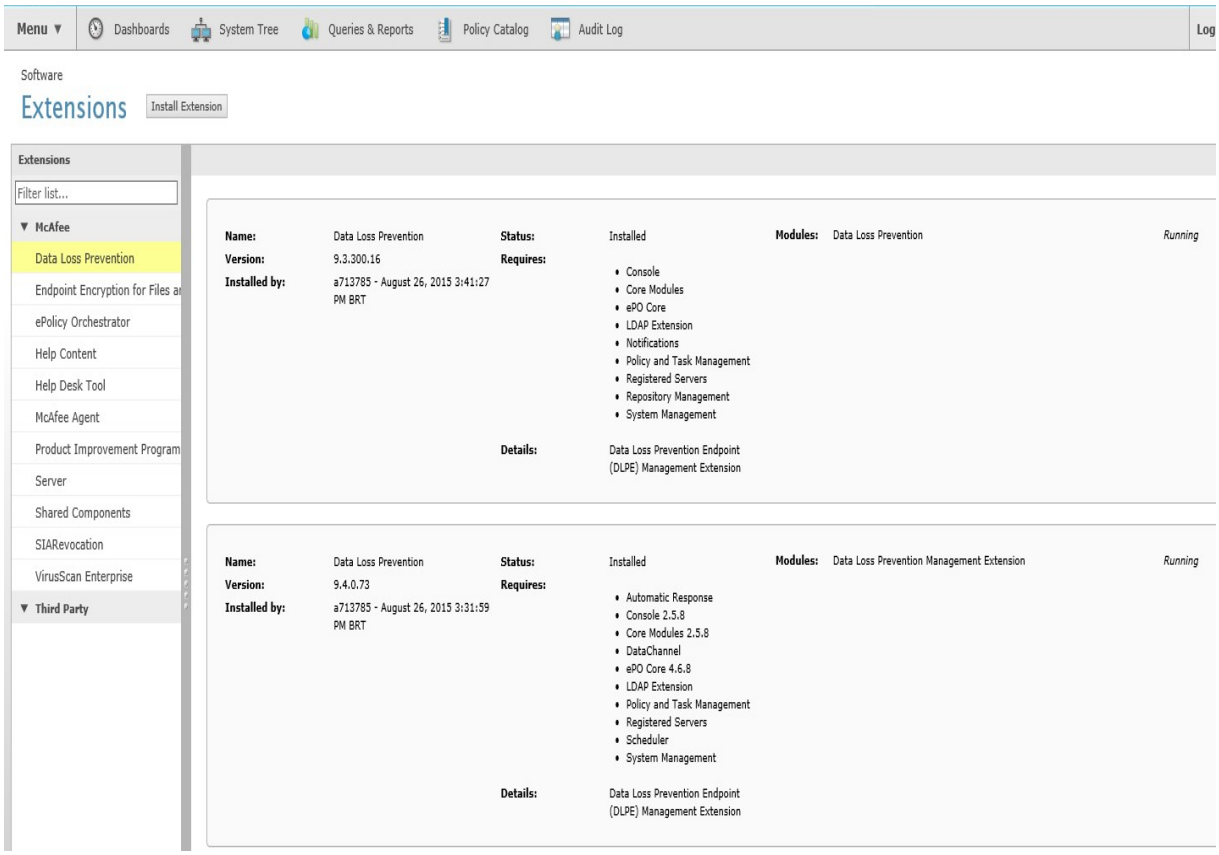


Name	Status	Type	Version	Minor Version
Buffer Overflow DAT for VirusScan Enterprise	OK	DAT	657	
DAT	OK	DAT	7911.0000	
Endpoint Encryption for Files and Folders	OK	Install	4.2.0	184
Engine	OK	Engine	5700.7163	7163
ePO Agent Key Updater	OK	Plugin	5.0.1	516
ePO Agent Key Updater	OK	Plugin	4.8.0	1938
McAfee Agent for Windows	OK	Install	5.0.1	516
McAfee Agent for Windows	OK	Install	4.0.0	1532
McAfee Agent for Windows(Embedded Creden	OK	Install	4.8.0	1938
McAfee Data Loss Prevention	OK	Install	9.4.0	532
McAfee Data Loss Prevention	OK	Install	9.3.300	31
Product Improvement Program	OK	Install	1.5.0	578
VirusScan Enterprise	OK	Patch	8.8.0	6
VirusScan Enterprise	OK	Install	8.8.0	1445

Fonte: Elaboração do autor

No campo *Extension*, checar as extensões de report do produto:

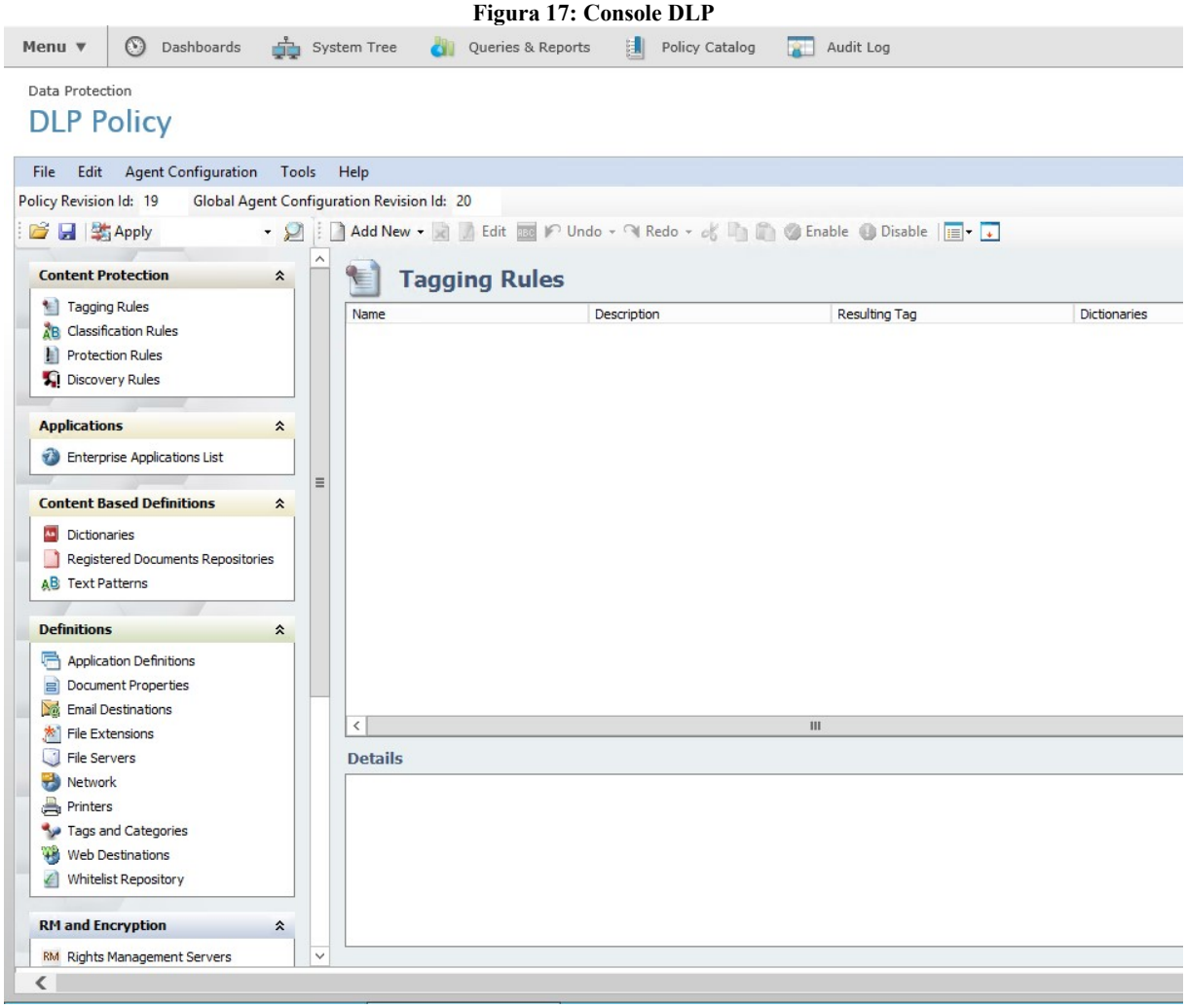
Figura 16: Extension DLP



Fonte: Elaboração do autor

Após estes passos, uma console própria da ferramenta DLP estará disponível para configuração das regras, de acordo com a política fornecida pela empresa.

Figura 17: Console DLP



Fonte: Elaboração do autor

Nesta console, encontra-se todas as configurações necessárias para implementar um sistema de monitoramento e bloqueio de tráfego de conteúdo por dispositivos móveis e similares.

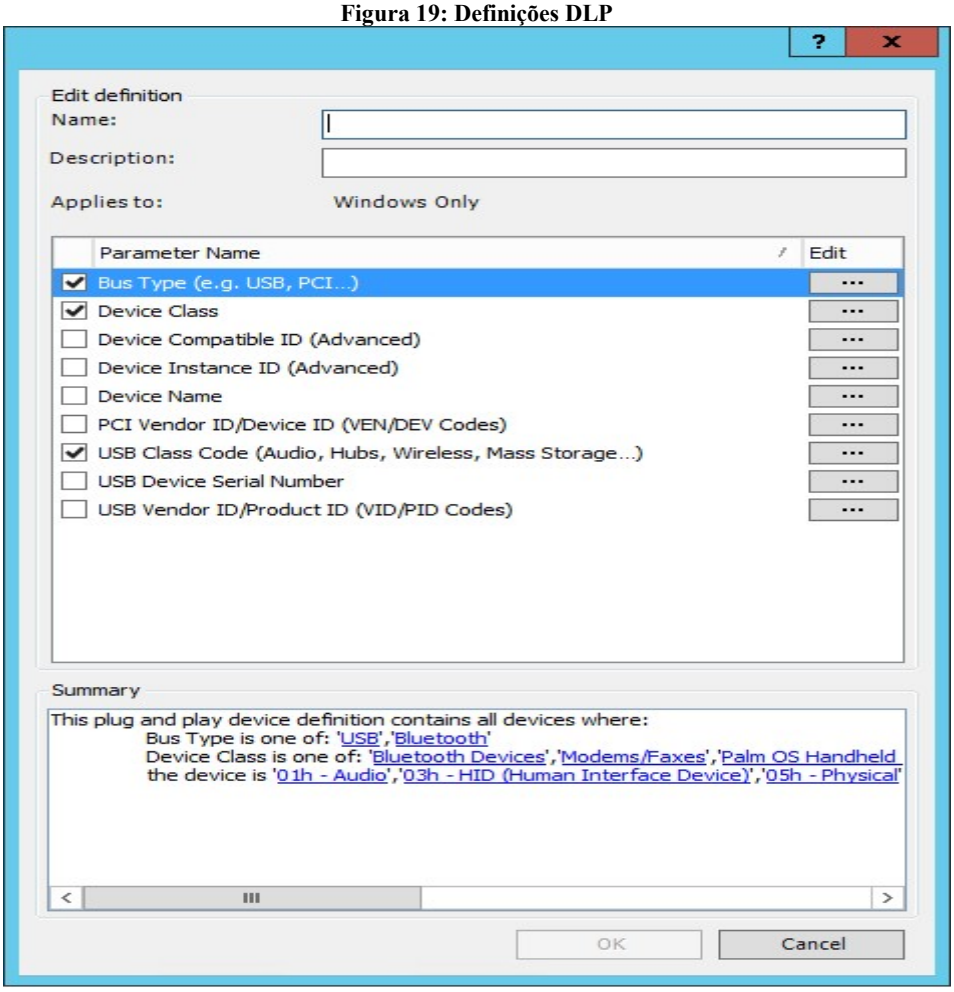
O foco da configuração de acordo com a política da empresa será o monitoramento e bloqueio de dispositivos móveis, em conjunto com o controle de conteúdo e bloqueio de extensões que representem possíveis ameaças (.exe .bat .bin, etc) (MCAFEE,2015).

Figura 18: Configurações DLP

Fonte: Elaboração do autor

O primeiro passo é configurar as definições de dispositvos que serão monitorados, podendo bloquear alguns tipos, como celulares, modem 3G/4G, dispositívos *flash*, e monitorar dispositívos de armazenamento.

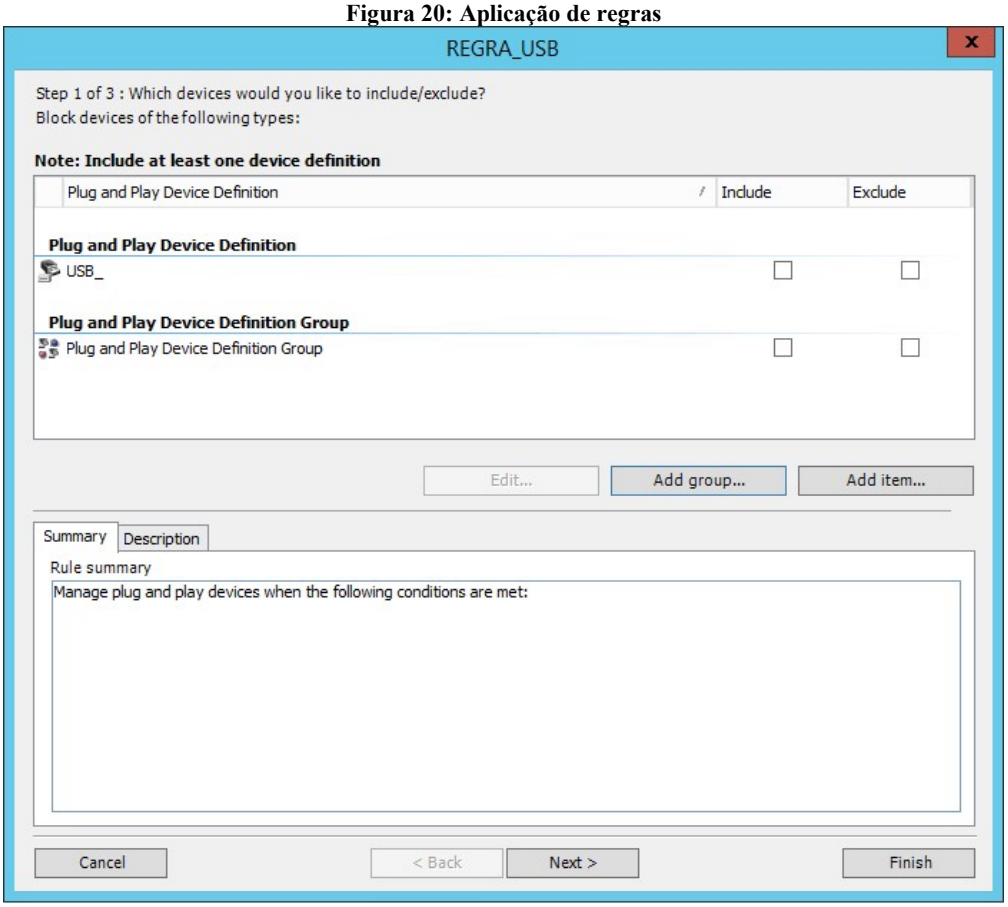
Figura 19: Definições DLP



Fonte: Elaboração do autor

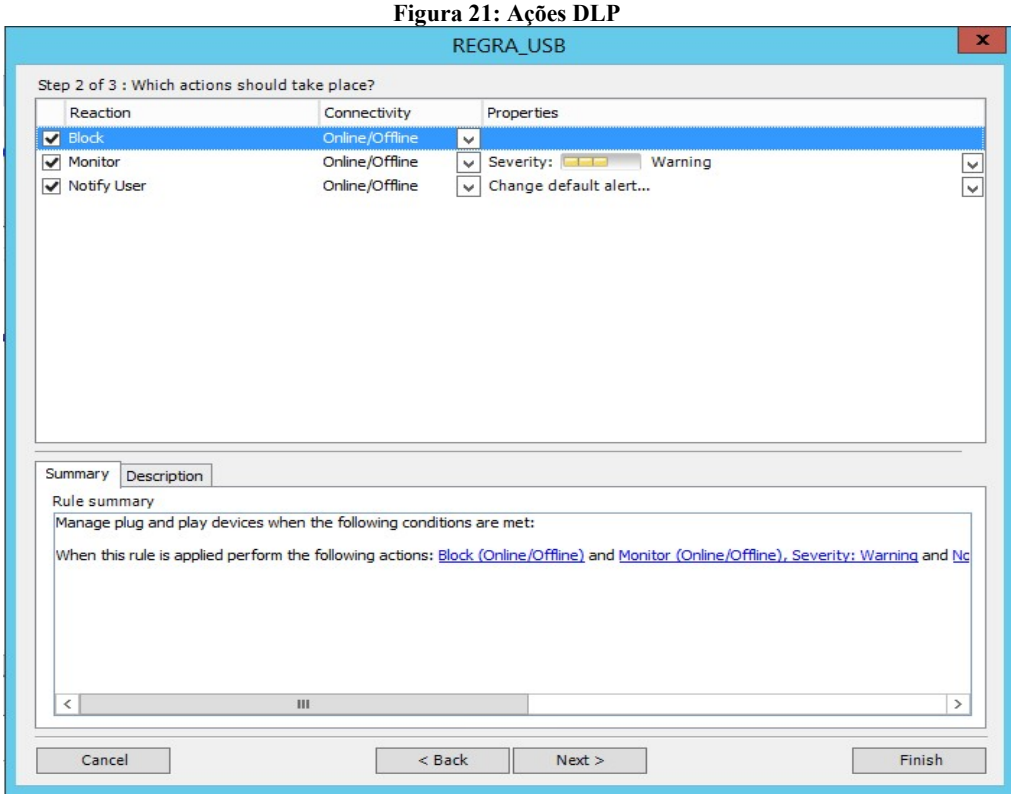
Em seguida, as regras devem ser estabelecidas, configurando o nível de monitoramento ou o bloqueio, notificações ao usuário e definição do grupo de usuários que serão atingidos.

Figura 20: Aplicação de regras



Fonte: Elaboração do autor

Figura 21: Ações DLP

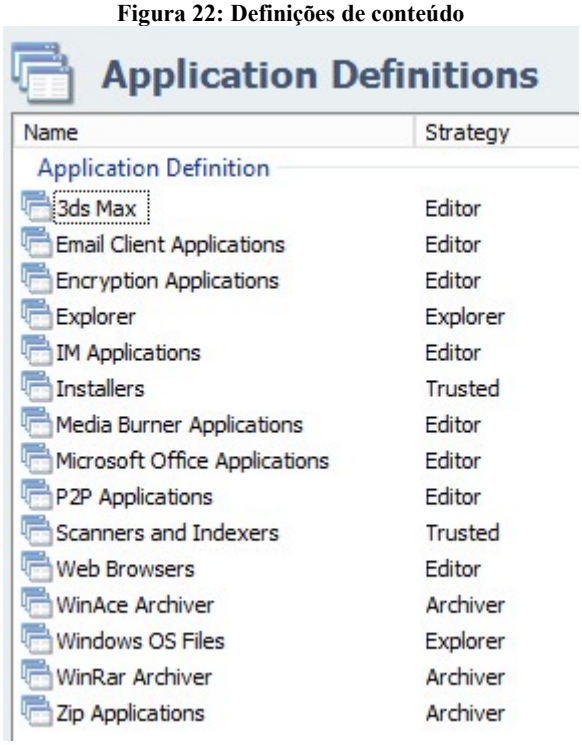


Fonte: Elaboração do autor

Com esta configuração básica, é possível avançar ao nível de controle de conteúdo do que se carrega nestes dispositivos.

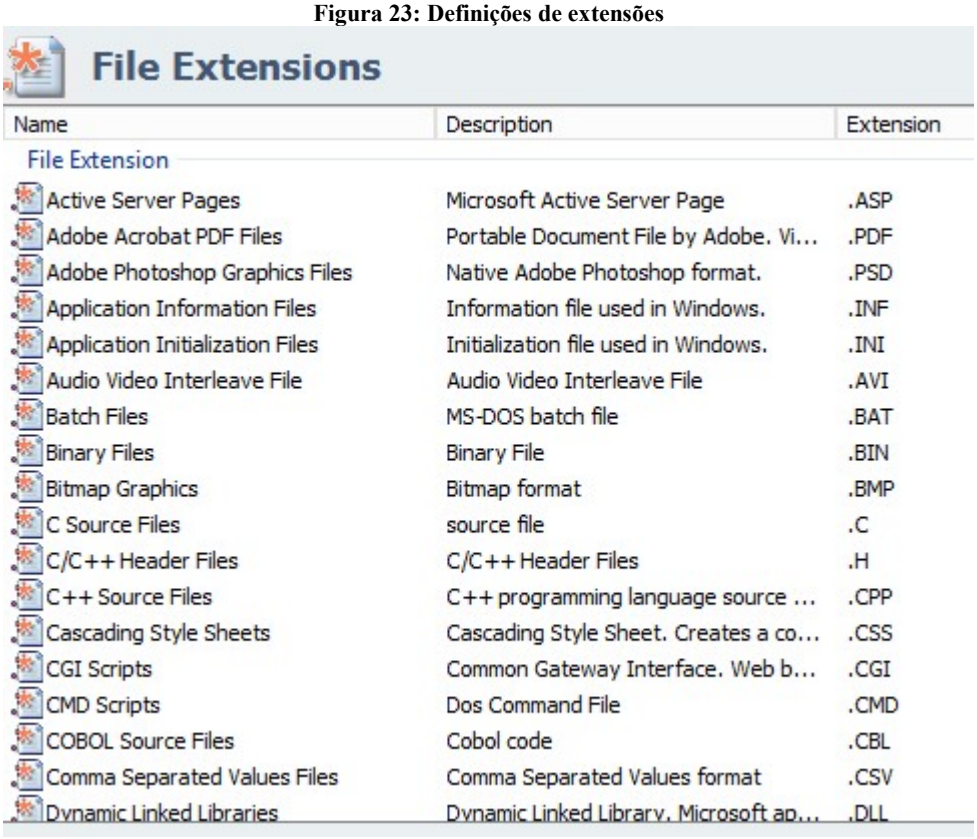
Assim como no controle de dispositivos, deve-se definir o tipo de aplicações, extensões e propriedades dos documentos que estarão presente no controle.

Figura 22: Definições de conteúdo



Fonte: Elaboração do autor

Figura 23: Definições de extensões



File Extensions

Name	Description	Extension
File Extension		
Active Server Pages	Microsoft Active Server Page	.ASP
Adobe Acrobat PDF Files	Portable Document File by Adobe. Vi...	.PDF
Adobe Photoshop Graphics Files	Native Adobe Photoshop format.	.PSD
Application Information Files	Information file used in Windows.	.INF
Application Initialization Files	Initialization file used in Windows.	.INI
Audio Video Interleave File	Audio Video Interleave File	.AVI
Batch Files	MS-DOS batch file	.BAT
Binary Files	Binary File	.BIN
Bitmap Graphics	Bitmap format	.BMP
C Source Files	source file	.C
C/C++ Header Files	C/C++ Header Files	.H
C++ Source Files	C++ programming language source ...	.CPP
Cascading Style Sheets	Cascading Style Sheet. Creates a co...	.CSS
CGI Scripts	Common Gateway Interface. Web b...	.CGI
CMD Scripts	Dos Command File	.CMD
COBOL Source Files	Cobol code	.CBL
Comma Separated Values Files	Comma Separated Values format	.CSV
Dynamic Linked Libraries	Dynamic Linked Library. Microsoft ap...	.DLL

Fonte: Elaboração do autor

Com todas as definições de categorias de dispositivos, regras de monitoramento/bloqueio e definição dos grupos de usuários, com uso do próprio ePO, é realizado a distribuição do *Agent* DLP para todas as estações de trabalho, recebendo essas políticas e gerando relatórios para controle da Área de Segurança (MCAFEE, 2015).

3.3.2 Implementação SOLIDCORE: Application Control

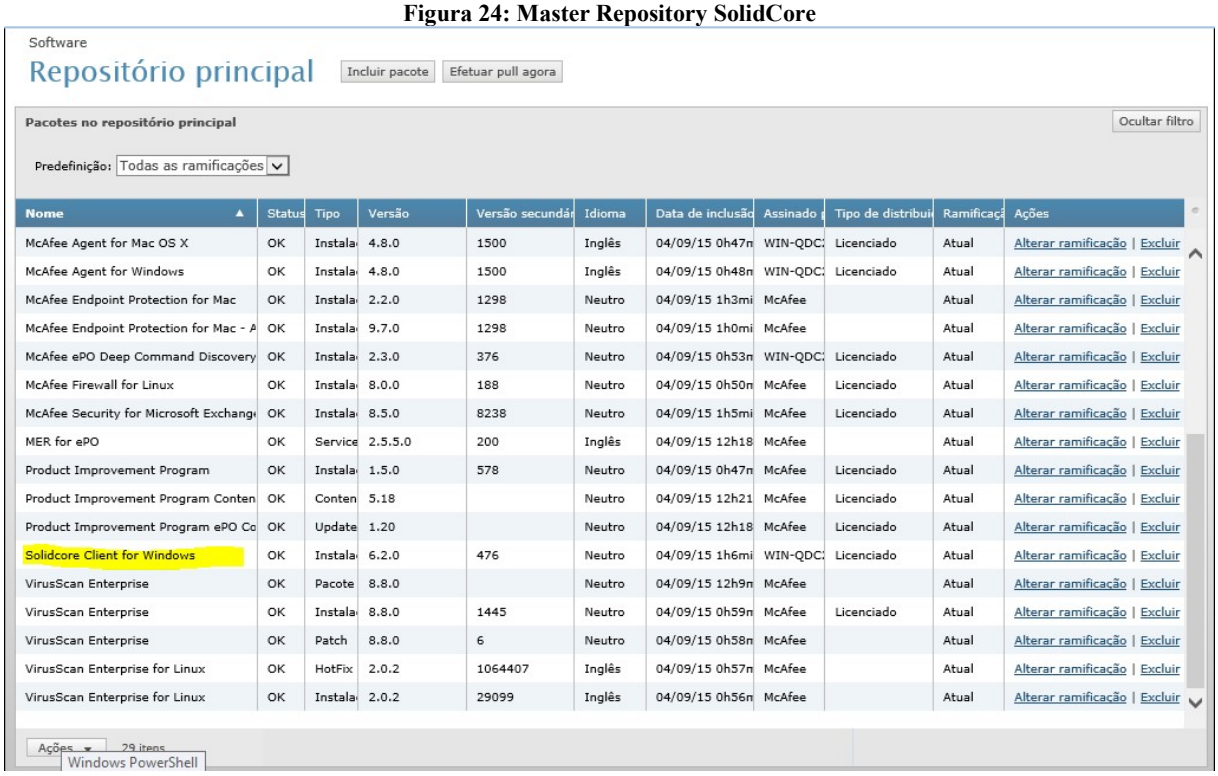
Sendo um produto McAfee, utilizando o número de licença já existente devido ao uso da aplicação de *Endpoint* e AntiVírus da mesma, realiza-se o *download* diretamente pelo site do fabricante.

A versão utilizada é a mais recente, *SolidCore*: *Application Control* 6.2, reconhecida no ePO como *Solidcore*, possuindo os mesmos requisitos de Hardware e Sistema Operacional que o *Endpoint ePolicy Orchestrator* (ePO), plataforma que irá receber a aplicação *Application Control* e controlar as regras e políticas para aplicação nas estações de trabalho, ao qual a ferramenta será destinada (MCAFEE, 2015).

Com os arquivos contendo o Pacote de Instalação e as Extensões de *report* de informações, deve-se checá-las no ePO.

No campo Master *Repository*, checar os Pacotes de Instalação:

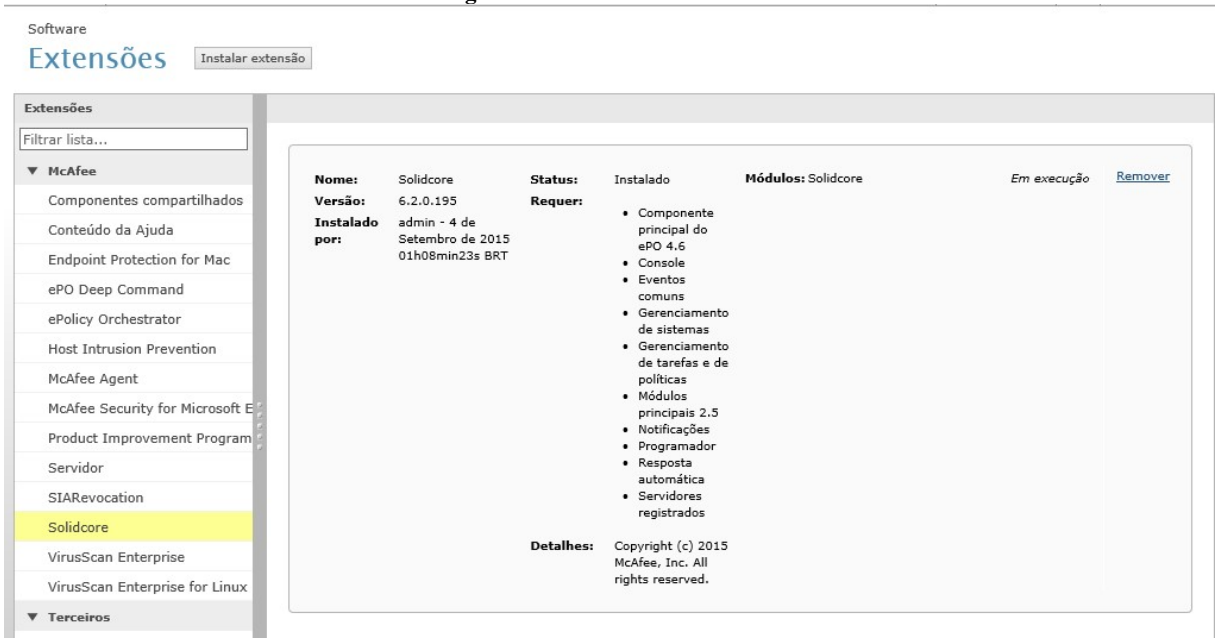
Figura 24: Master Repository SolidCore



Fonte: Elaboração do autor

Logo após deve-se checar as extensões de *report* no campo extensões:

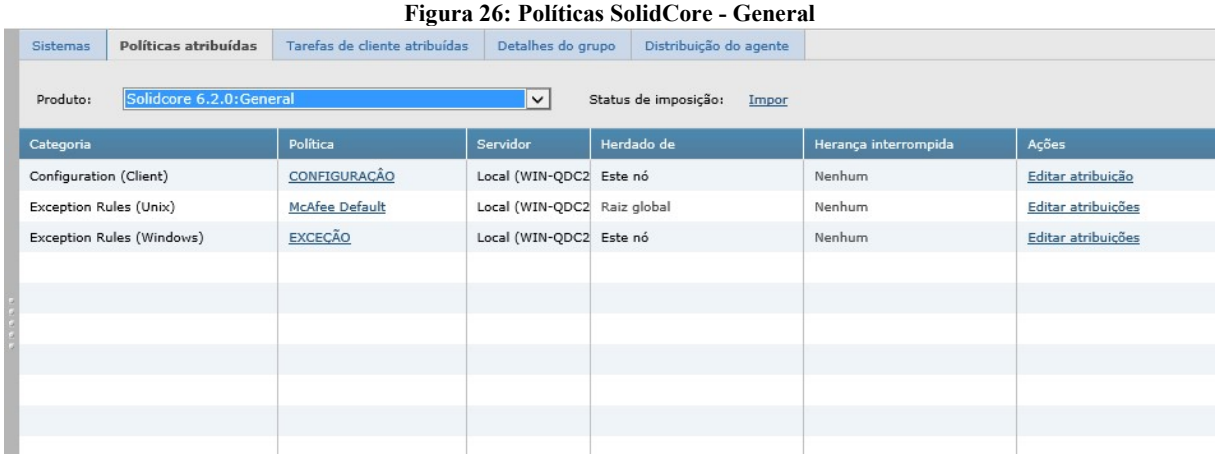
Figura 25: Extensions SolidCore



Fonte: Elaboração do autor

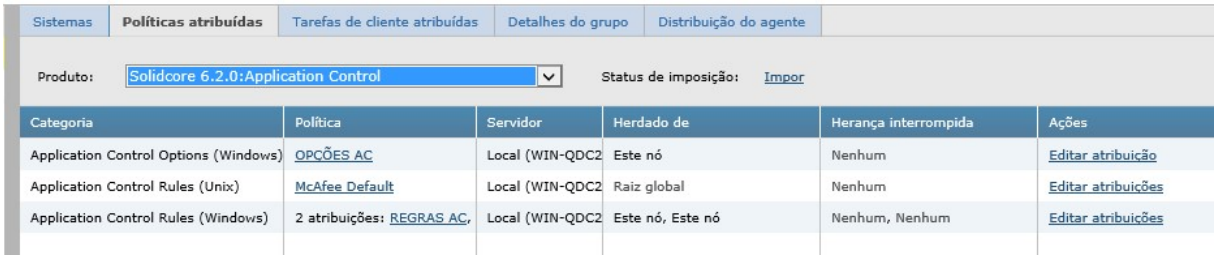
No campo das políticas serão encontrados dois tipos de configurações, *Solidcore: General e Solidcore: Application Control*

Figura 26: Políticas SolidCore - General



Fonte: Elaboração do autor

Figura 27: Políticas SolidCore - Application Control



Fonte: Elaboração do autor

Na política General encontra-se a categoria de Configurações, nela configura-se os seguintes campos:

CLI: Senha de acesso ao *Command Line Interface* (CLI), permite que configurações sejam realizadas diretamente na estação pelo usuário via linha de comando.

Figura 28: Políticas CLI

Fonte: Elaboração do autor

Throttling: Configuração de controle de fluxo de dados entre o *client* e o *McAfee ePO Server*.

Figura 29: Políticas Throttling

Fonte: Elaboração do autor

Na política *Application Control*, será configurado o que deve ser protegido e o que pode ser liberado pela aplicação, como será reportado, informado ao usuário e gerado os devidos relatórios (MCAFEE, 2015).

Em *Application Control Options*, encontra-se o texto que será apresentado ao usuário ao detectar algum evento não permitido, os dados de contato do Administrador de Segurança e mensagens de alerta ao acionar determinadas aplicações críticas.

Figura 30: Mensagens Application Control

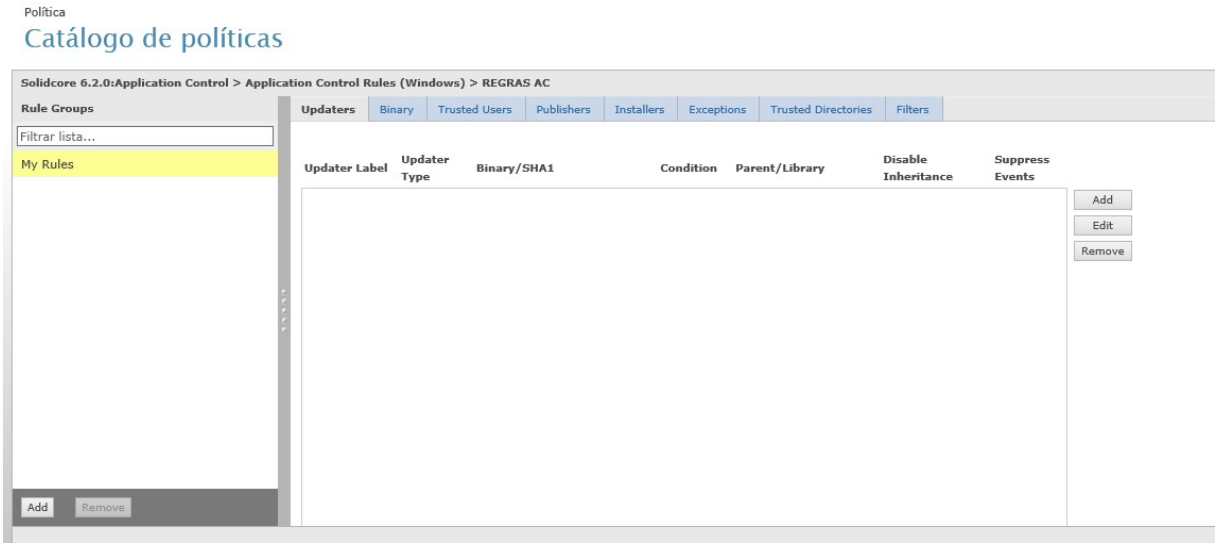
Fonte: Elaboração do autor

Figura 31: Notificações para usuário

Fonte: Elaboração do autor

Finalizando as configurações da aplicação, está a principal regra, o gerenciamento da *whitelist*, com o alinhamento de processos e aplicações realmente necessárias à organização em mãos, é necessário inserir as exclusões, aplicações que precisam ser atualizadas e outras que podem ser instaladas livremente. Também segregando regras por usuários distintos, caminhos, etc (MCAFEE, 2015).

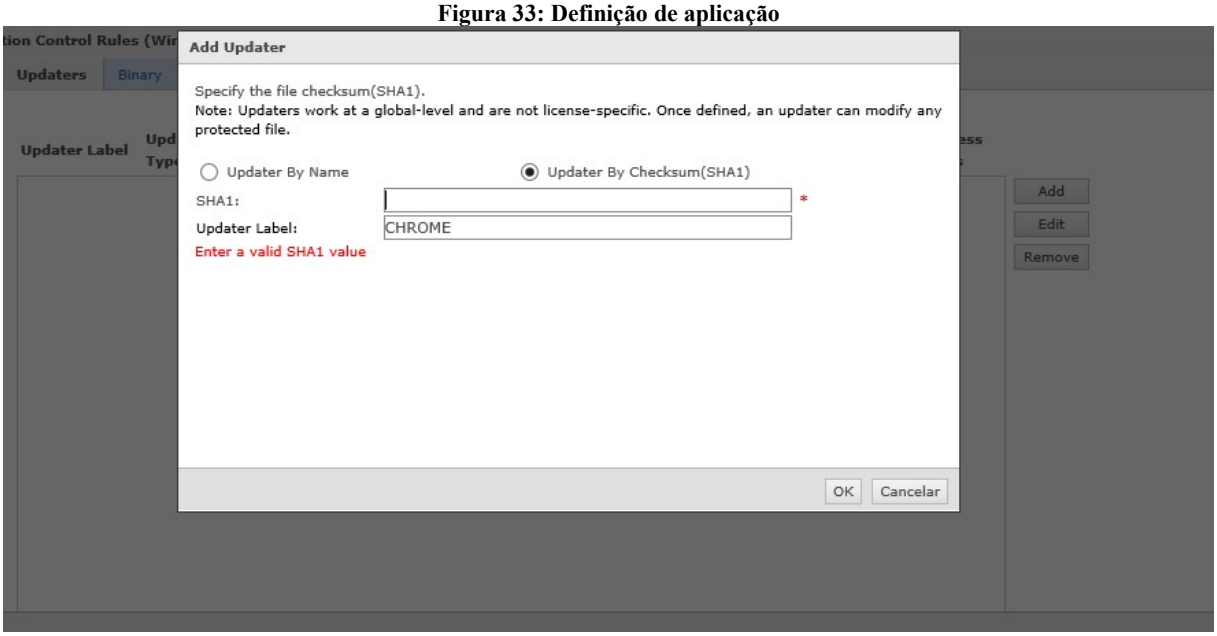
Figura 32: Classificação de aplicações



Fonte: Elaboração do autor

Para diferenciar cada aplicação, a ferramenta identifica o *Checksum* da mesma, que é o código *hash* que de cada aplicativo e pode ser gerado por uma calculadora própria para isso, acusando se é liberada ou bloqueada para atualizar.

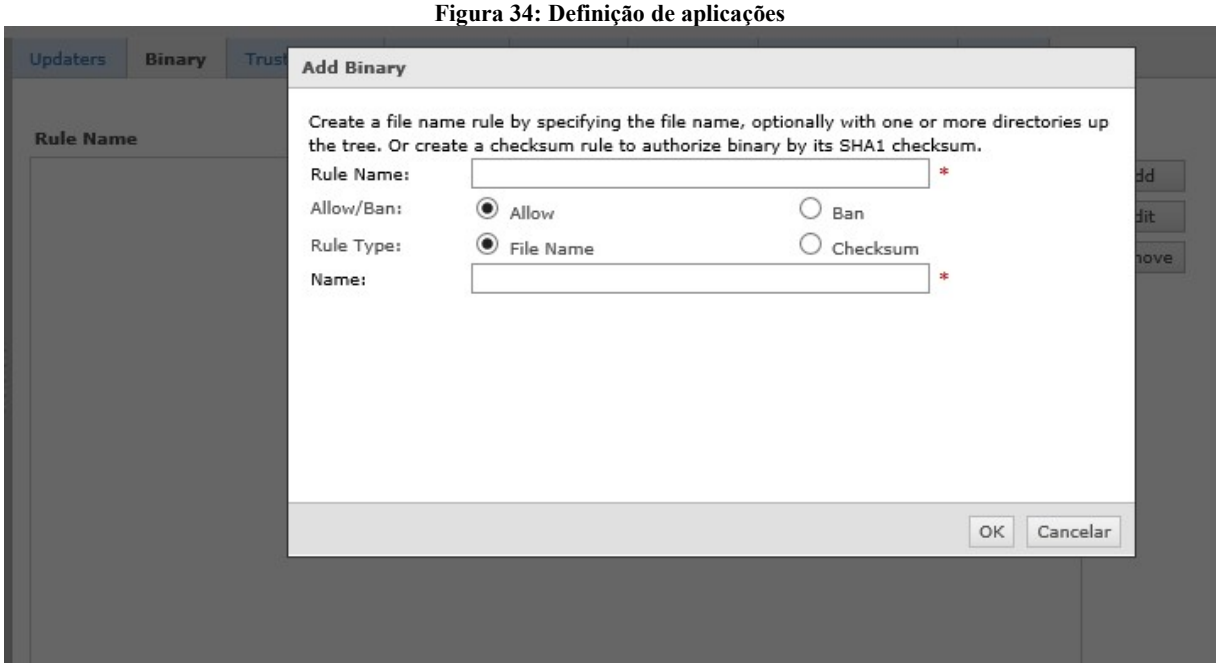
Figura 33: Definição de aplicação



Fonte: Elaboração do autor

Para autorizar a instalação de uma nova aplicação, que seja de interesse da organização, o princípio será o mesmo usado na regra anterior, gerando o código *Checksum* de determinada aplicação, permitindo ou negando sua execução, podendo ser alterado a qualquer momento pelo administrador.

Figura 34: Definição de aplicações



Fonte: Elaboração do autor

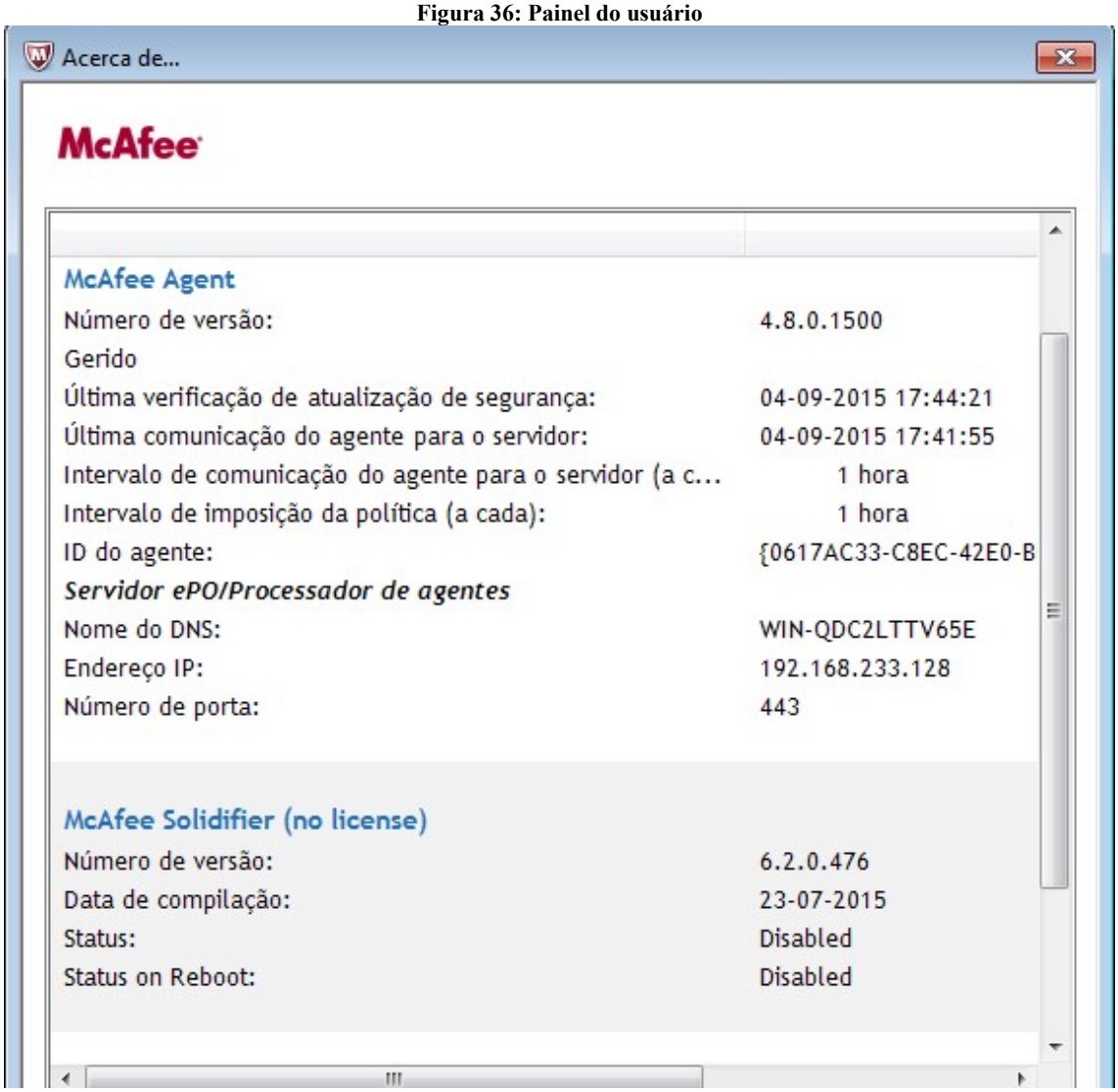
Após finalizar a configuração das regras na console da ferramenta, é possível acompanhar todo o progresso da implantação diretamente nas estações.

Figura 35: Tarefa para Instalar SolidCore

Fonte: Elaboração do autor

Ao executar a tarefa de instalação nas estações do *Solidcore*, irá ser demonstrada no painel do *McAfee Agent* da estação de trabalho.

Figura 36: Painel do usuário



Fonte: Elaboração do autor

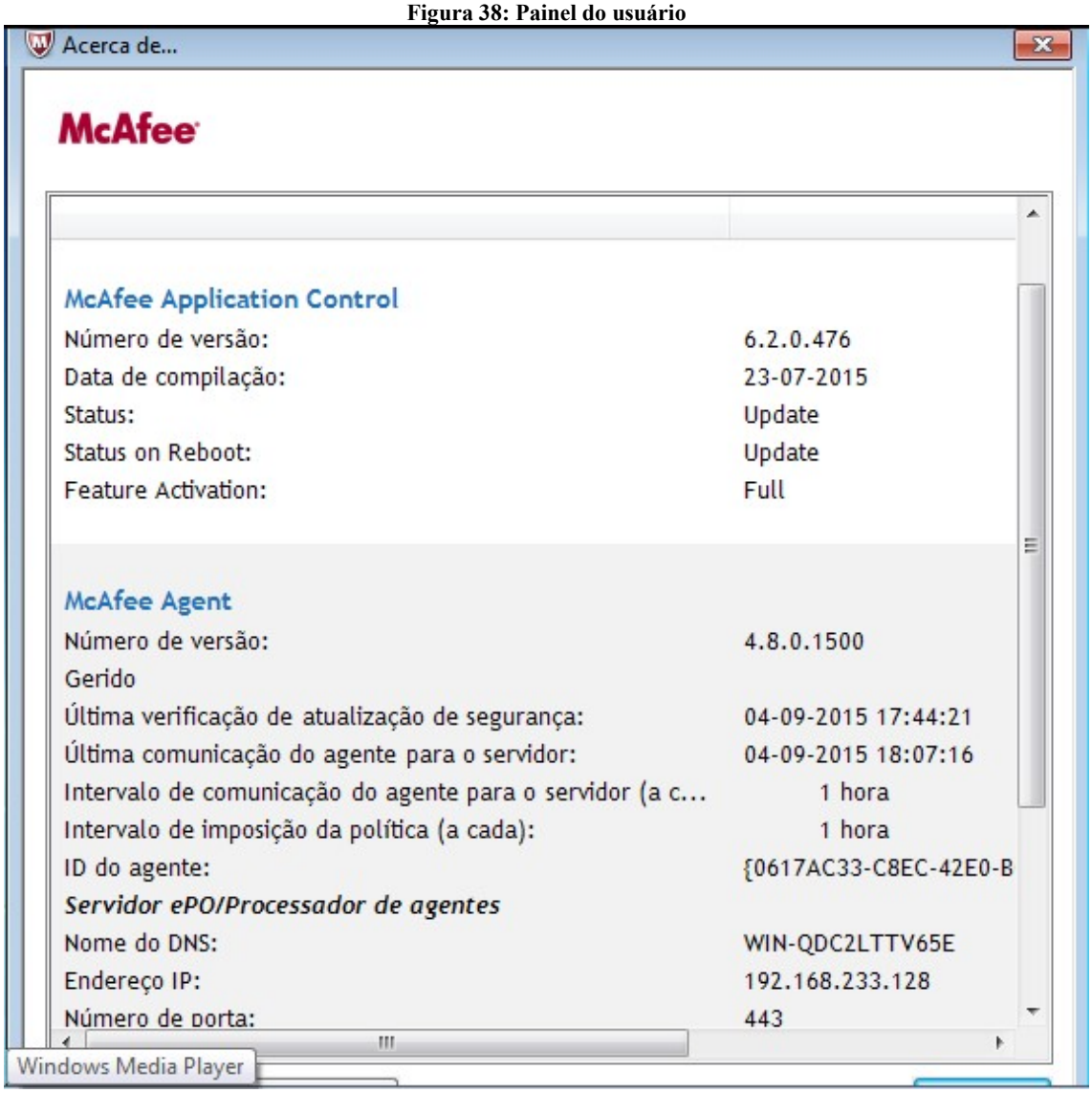
Após a instalação, deve-se habilitar o *status* do cliente para receber as políticas e regras de funcionamento, com a política configurada no ePO, será realizada de forma automática para todo o parque de estações.

Figura 37: Tarefa para habilitar SolidCore

Fonte: Elaboração do autor

O status na estação será alterado imediatamente e o nome da aplicação será alterado para a que está licenciada no ePO.

Figura 38: Painel do usuário



Fonte: Elaboração do autor

Voltando ao ePO, configura-se as seguintes tarefas para que o produto trabalhe de acordo com o esperado, tarefa *CHANGE CLI*, irá bloquear ou permitir ao usuário o uso de linhas de comando para gerenciar o Solidcore, tarefa de *UPDATE*, que realizará a ação de atualizar aplicações homologadas e autorizadas de acordo com a necessidade da organização (MCAFEE, 2015).

Figura 39: Tarefas SolidCore

Predefinição: Sem filtro Busca rápida: Aplica

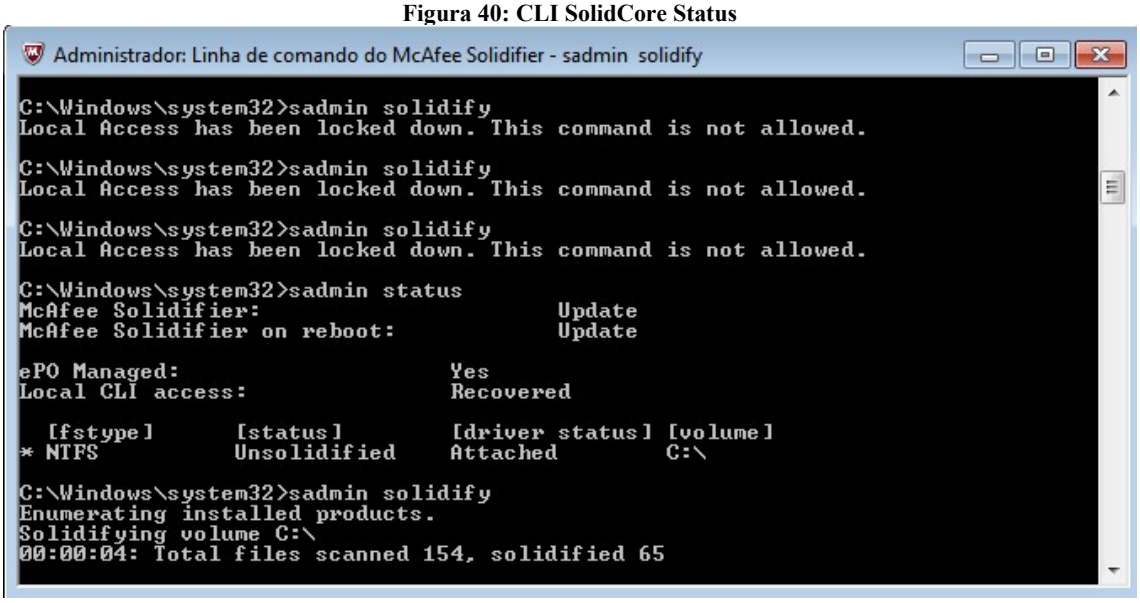
Nome da tarefa	Tipo de tarefa	Status	Programação	Data e hora de início	Herança interrompida
CHANGE CLI	SC: Change Local CLI Acc	Ativada	Executar imediatamente	04/09/15 00:00	Nenhum
ENABLE APP CONTROL	SC: Enable	Ativada	Executar imediatamente	04/09/15 00:00	Nenhum
INSTALL APP CONTROL	Distribuição do produto	Ativada	Executar imediatamente	04/09/15 00:00	Nenhum
SOLIDIFY	SC: Run Commands	Ativada	Diariamente	04/09/15 12:00	Nenhum
UPDATE	SC: Begin Update Mode	Ativada	Executar imediatamente	04/09/15 00:00	Nenhum

Fonte: Elaboração do autor

Com as políticas e tarefas progamadas, o último passo é solidificar a máquina, blindando-a contra qualquer alteração e execução não autorizada.A tarefa *SOLIDIFY* mostrada na figura anterior, realizará esta ação.

Até o presente momento todas as máquinas estão com os Sistemas Operacionais não solidificados, como pode ser visto na figura abaixo o status do volume C:\ (*Unsolidify*).

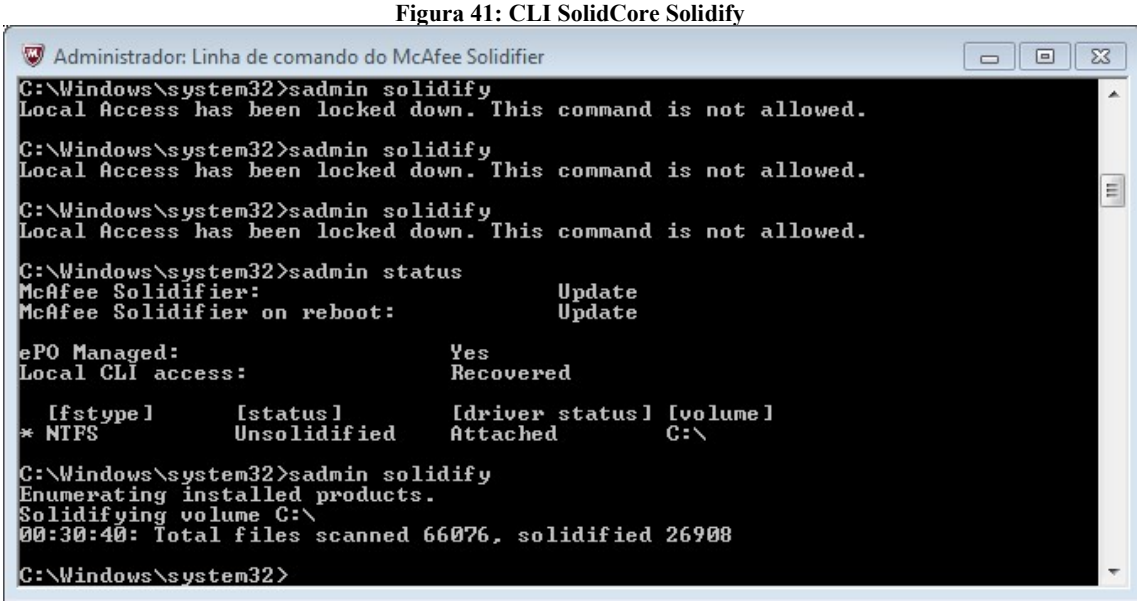
Figura 40: CLI SolidCore Status



Fonte: Elaboração do autor

Ao executar a tarefa, será realizada uma varredura de disco, solidificando-o totalmente.

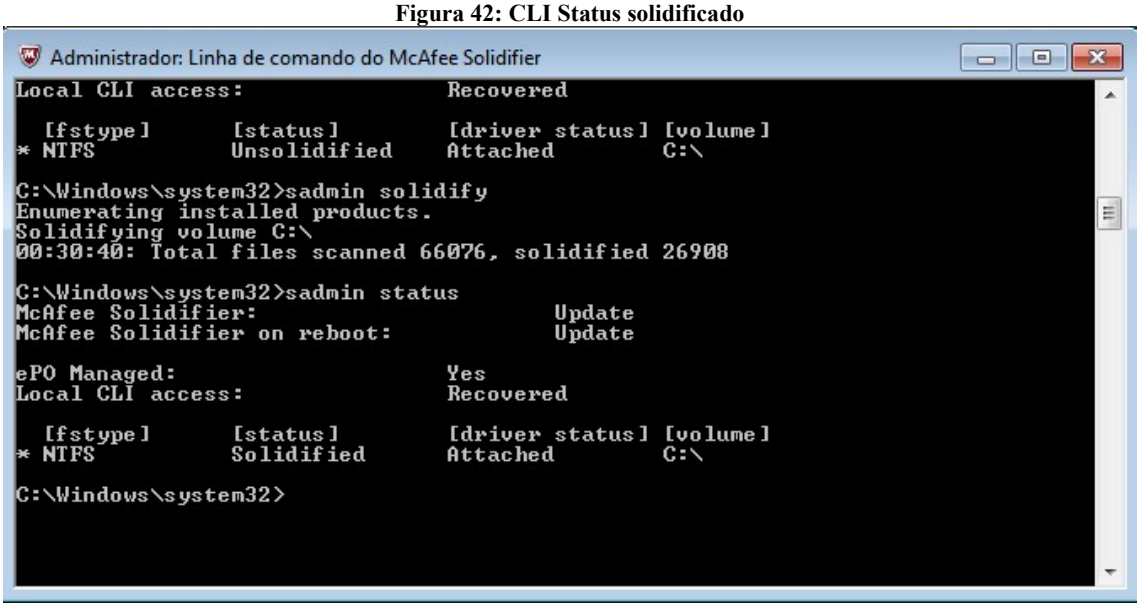
Figura 41: CLI SolidCore Solidify



Fonte: Elaboração do autor

Assim, alterando o status do volume C:\

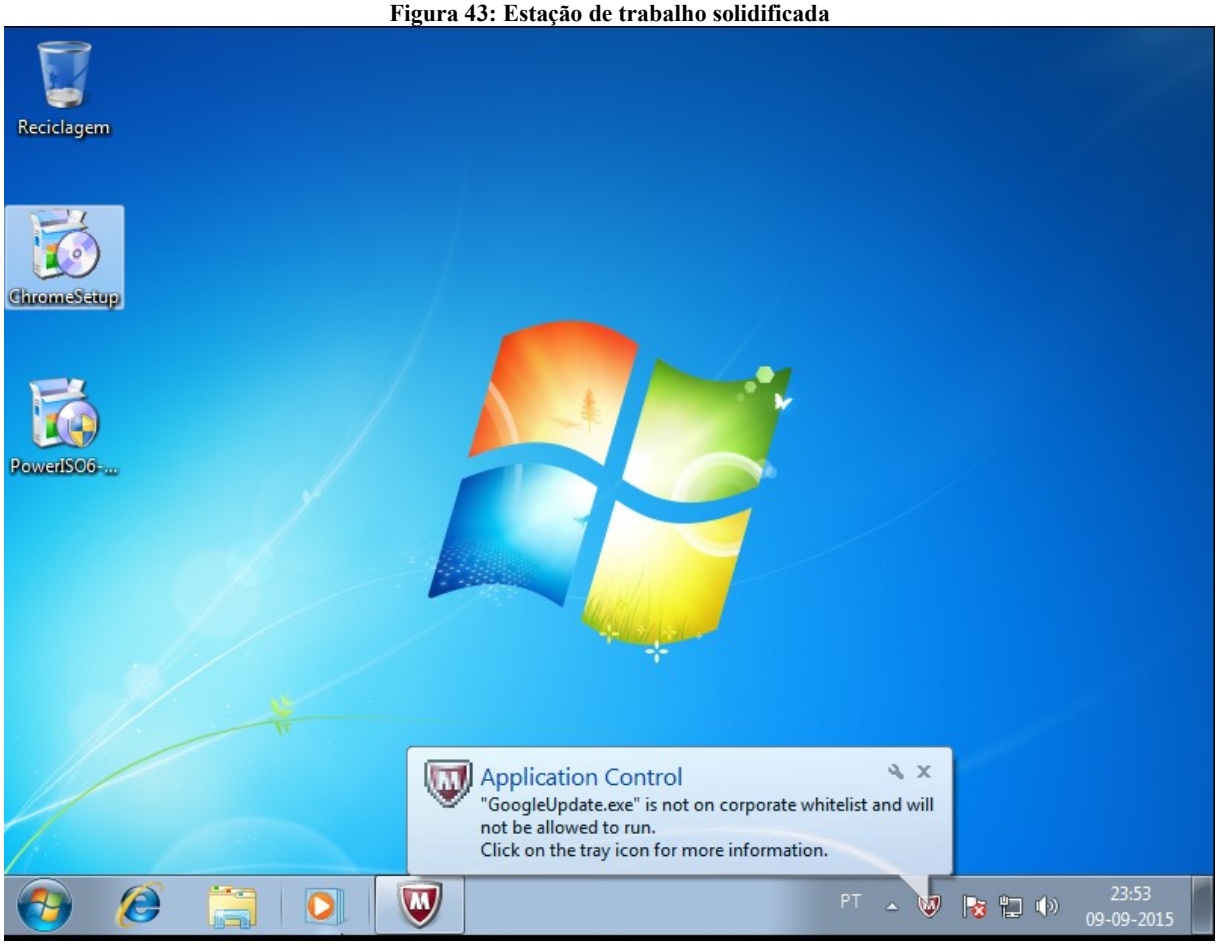
Figura 42: CLI Status solidificado



Fonte: Elaboração do autor

Com a máquina solidificada, é possível ver o resultado e ação da ferramenta na estação de trabalho, quando, ao executar um aplicativo não permitido, o mesmo será imediatamente bloqueado como é possível ver na imagem a seguir.

Figura 43: Estação de trabalho solidificada



Fonte: Elaboração do autor

4 PROJETOS FUTUROS

O projeto inicial demonstrou a solução para implementação do *Hardening* de ambiente Windows no Banco X.

Está em fase de planejamento a expansão desse modelo para o restante dos prédios administrativos e demais agências do Banco X, onde estão localizados o restante dos colaboradores e funcionários de todo o Brasil.

Partindo da necessidade da empresa e da quantidade de usuários afetados por esta solução, com a evolução do nível de maturidade da organização e boa aceitação por parte dos usuários, o sistema de atualizações poderá ser substituído pelo SCCM, que tem como principal foco, diminuir a quantidade de tarefas manuais desenvolvidas pela TI, automatizando atividades corriqueiras e munindo a equipe de ferramentas de ferramentas e recursos para a resolução de problemas de forma mais rápida e eficaz.

De acordo com Batista (2013):

> Com a versão do SCCM 2012 SP1 é possível gerenciar vários tipos de equipamentos, softwares e plataformas. Algumas versões de Linux agora são “gerenciadas” pelo SCCM, dispositivos móveis como celulares e *Tablets* também são gerenciados pela última versão do SCCM, produtos como iPhone, iPad e iPod *Touch*, podem receber a instalação de softwares, além deles produtos como o Windows Phone também são compatíveis com o ambiente e podem receber um certo controle do SCCM, como a necessidade de senha, vínculo com o ExchangeSync, instalação de software entre outros.

Além de atender aos usuários internos, o setor de tecnologia do Banco X, estuda implementações de segurança para serviços *offsite*, melhorando o rendimento de atividades, reposta de atendimentos e melhoria dos serviços prestados. Elaborando um novo nível de maturidade para o *Hardening* já aplicado nas devidas proporções da situação atual.

A solução apresentada poderá ser expandida, atendendo a usuários e clientes, tornando-se uma solução importante, inclusive na área negocial.

CONSIDERAÇÕES FINAIS

Segurança dos dados trafegados em um ambiente bancário é algo bastante discutido nas organizações deste setor hoje em dia. A tendência é as organizações se adequarem a soluções para atender essa necessidade de proteção tão crítica, a blindagem do ambiente contra ameaças torna-se imprescindível para manter a segurança e a conformidade do ambiente (NASCIMENTO, 2014)

Aproveitando a infraestrutura já pronta, as licenças adquiridas junto aos fabricantes e o cronograma reduzido para implantar um projeto de proteção de dados, mostrou-se uma alternativa viável a curto prazo e que atenda a organização em nível nacional. As ferramentas da Microsoft em conjunto com a Mcafee demonstraram atender a essa necessidade.

A implantação do WSUS em conjunto com o DLP e *Application Control*, vieram para trazer o benefício de um ambiente totalmente protegido e monitorado, sendo ideal para a visão de negócio do banco e suprindo algo que, até o presente momento era uma enorme preocupação da área de segurança (MICROSOFT, 2015).

O piloto realizado na AIF/DF trouxe os resultados esperados, superando a aceitação dos usuários a respeito da implantação rígida de um novo modelo de segurança e organização do ambiente. Futuramente esta solução será expandida para o restante da organização do Banco X, elevando o grau de segurança e preservação de dados tão críticos que fazem parte do cotidiano do negócio e seus processos.

REFERÊNCIAS

BATISTA, T. O que é o SCCM?. 2013. Disponível em: http://gestãonati.com.br/o-que-e-sccm/ Acesso em 14 set. 2015.

BRANDAO, R. Introdução a Group Policy (GPO). Disponível em: https://technet.microsoft.com/pt-br/library/Cc668545.aspx. Acesso em: 5 set. 2015

DIÓGENES, Y.; MAUSER, D. Certificação Security+. 2 ed. São Paulo. Nova Terra, 2013.

FINNET. Hardening Windows Server. 2014. Disponível em: http://wiki.finnet.com.br/doku.php?id=infra:procedimentos:padroes:hardening-windows-server. Acesso em 20 ago. 2015.

FREBABAN. Pesquisa FEBRABAN de Tecnologia Bancária. 2012. Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/PesquisaFebrabanTecBanc%E1ria2012.pdf. Acesso em: 20/09/2015.

MCAFEE. McAfee Application Control 6.2.0 – Product Guide. Disponível em: http://www.intel.com/content/dam/www/public/us/en/documents/guides/mcafee-application-control-product-guide.pdf. Acesso em 12 set. 2015.

MCAFEE. McAfee Data Loss Prevention Endpoint 9.4.0 – Product Guide. Disponível em: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24536/en_US/dlp_940_pg_TP000036-a00_en-us.pdf. Acesso em: 10 set. 2015.

MICROSOFT. Auditoria de Segurança. 2010. Disponível em: https://technet.microsoft.com/pt-br/library/cc771395(v=ws.10).aspx Acesso em: 10 set. 2015.

MICROSOFT. Administering Windows Server. 2012. Ed Microsoft Learning. Module 1: Implementing a Group Policy Infrastructure. p. 1-2.

MICROSOFT. Administering Windows Server. 2012. Ed. Microsoft Learning. Module 12: Implementing Update Management. p. 12-2.

MICROSOFT. WINDOWS SERVER UPDATE SERVICES 3.0 SP2 DEPLOYMENT GUIDE. 2015. Disponível em: https://technet.microsoft.com/library/dd939906(WS.10).aspx. Acesso em: 29 ago. 2015.

MICROSOFT. Windos Server Update Services 3.0 SP2. 2015 Disponível em: http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=5216 Acesso em: 29 ago. 2015.

MULLER, E. J. A importância de gerar e manter logs. 2014. Disponível em: http://www.ezequieljuliano.com.br/?p=76. Acesso em: 10 set. 2015.
NASCIMENTO, R. Bancos Investem em Segurança de informação. 2014. Disponível em: http://www.administradores.com.br/artigos/tecnologia/bancos-investem-em-seguranca-de-informacao/76488/. Acesso em: 20/09/2015.

PORTAL EDUCAÇÃO. Introdução a Group Policy. 2008. Disponível em: http://www.portaleducacao.com.br/educacao/artigos/6926/introducao-a-group-policy#ixzz3jPM4FFjP. Acesso em: 5 set. 2015

REIS, F. A.; VERBENA, M. F.; JULIO, E. P. Hardening. 2015. Disponível em: http://www.devmedia.com.br/hardening-artigo-revista-infra-magazine-1/20818#ixzz3lwUbqEVY. Acesso em: 20 ago. 2015.

SILVA, E. G. S. Entenda o que é *Hardening.* 2015. Disponível em: http://www.vivaolinux.com.br/artigo/Entenda-o-que-e-Hardening. Acesso em: 20/09/2015.

TECNOLOGIA DA INFORMAÇÃO. Hardening. 2013. Disponível em: http://blog.segr.com.br/hardening/. Acesso em: 16 ago. 2015.

WIKIPEDIA. Network Time Protocol. 2014. Disponível em: https://pt.wikipedia.org/wiki/Network_Time_Protocol. Acesso em 15 ago. 2015.