UNIVERSIDADE TECNOLOGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
ESPECIALIZAÇÃO EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

JACQUELINE FRANCIELLE DA ROSA

AUTOMATIZANDO PROCESSOS DE ACESSO A REDE EM EMPRESAS DE TELECOM: O CASO DE UMA EMPRESA DE TELECOMUNICAÇÕES

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2013

JACQUELINE FRANCIELLE DA ROSA

AUTOMATIZANDO PROCESSOS DE ACESSO REDE EM EMPRESAS DE TELECOM: O CASO DE UMA EMPRESA DE TELECOMUNICAÇÕES

Trabalho de Monografia apresentada como requisito parcial à obtenção do título de Especialista em Gestão da Tecnologia da Informação e Comunicação, do Programa de Pós-Graduação em Tecnologia, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Christian Carlos Souza Mendes.

CURITIBA

2013

TERMO DE APROVAÇAO

Título da Monografia

AUTOMATIZANDO PROCESSOS DE ACESSO À REDE EM EMPRESAS DE TELECOM: O CASO DE UMA EMPRESA DE TELECOMUNICAÇOES

por

Jacqueline Francielle da Rosa

Esta monografia foi apresentada às 19h30min, do dia 26 de agosto de 2013, como requisito parcial para a obtenção do título de **ESPECIALISTA EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO,** do Programa de Pós-Graduação da Universidade Tecnológica Federal do Paraná. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após a deliberação, a Banca Examinadora considerou o trabalho **APROVADO**

Prof. Dr. Augusto Foronda
(UTFPR)

Prof. Msc. Christian Carlos Souza Mendes
(UTFPR)
Orientador

Prof. Msc. Alexandre Jorge Miziara
Coordenador do Curso

OBS: O DOCUMENTO ORIGINAL COM AS DEVIDAS ASSINATURAS ENCONTRA-SE NA DERAC

RESUMO

ROSA, Jacqueline Francielle da. Automatizando Processos de Acesso a Rede em Empresas de Telecom: O Caso de uma Empresa de Telecomunicações. 2013. 53 f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Atualmente tem-se uma preocupação com relação a acessos a rede corporativa, bem como em definir perfis de acesso no ambiente. Com um alto número de funcionários em empresas de Telecom, é inviável que a criação / bloqueio dos acessos a rede seja efetuada de forma manual. O processo manual para criar / bloquear os acessos a rede corporativa leva em torno de 5 minutos por usuário a ser criado ou bloqueado. O volume de contratações e demissões é considerável, tendo em vista o aquecimento do mercado. Os dados dos últimos 7 meses mostram que há uma média de 1000 demissões por mês e consequentemente 1000 novas contratações, sendo assim, para criar 1000 novos acessos e bloquear 1000 acessos, a equipe responsável necessita aproximadamente de 1 mês para executar a atividade e com a possibilidade de erros no processo. Com a implantação de um sistema de gerenciamento de identidade que gera/ bloqueia automaticamente os logins, bem como os privilégios de acesso dos usuários na rede, há uma redução de tempo de atendimento (SLA) para a criação / bloqueio de logins, minimizando o tempo de ociosidade de novos funcionários, evitando possíveis fraudes, possibilitando a equipe alocada para esta finalidade envolver-se em outros projetos de importância maior e evitar erros nas liberações e bloqueios de acessos.

Palavras-chave: Criação / Bloqueio de acessos. Rede Corporativa. Gerenciamento de Identidade. Empresas de Telecom.

ABSTRACT

ROSA, Jacqueline Francielle da. Automating Processes Network Access for Telecom Companies: The Case of a Telecommunications Company. 2013. 53 f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Currently has a concern with respect to access to the corporate network as well as to define access profiles in the environment. With a high number of employees in companies of Telecom, it is infeasible for the establishment / blocking of access to the network is performed manually. The manual process to create / block the access to the corporate network takes about 5 minutes per user to be created or blocked. The volume of hiring and firing is considerable, considering the heating market. The data of the last seven months show that there is an average of 1,000 layoffs / month and therefore new hires in 1000, so to create 1000 new hits and block access 1000, the team responsible requires approximately one month to run the activity and the possibility of errors in the process. With the implementation of an identity management system that generates / automatically blocks logins and access privileges of users on the network, there is a reduction of service time (SLA) to create / lock logins, minimizing the time idle new employees, avoiding possible scams, enabling staff allocated for this purpose engage in other projects of major importance and avoid errors in releases and locks access.

Keywords: Creation / Lockout hits. Corporate Network. Identity Management. Telecom companies.

LISTA DE FIGURAS E ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas houve um significativo avanço na tecnologia da informação. Processos que são manuais estão cada vez mais perto de serem substituídos por rotinas automáticas que cumprem o mesmo papel de um humano, em menos tempo e com muito menos chances de erros.

Atualmente tem-se uma preocupação com relação a acessos a rede corporativa, bem como em definir perfis de acessos no ambiente. Em empresas de Telecom, o número de funcionários é gigantesco. Efetuar a criação / bloqueio de logins de forma manual aonde o volume mensal chega a mais de 1000 solicitações tanto de criação como de bloqueio é praticamente inviável.

A partir do momento em que um novo colaborador ingressa na companhia, a equipe de RH é responsável por efetuar o cadastro deste funcionário nos sistemas de folha de pagamento e benefícios, a partir deste ponto entra o processo manual para criar / bloquear os acessos a rede corporativa, que leva em torno de 5 minutos por usuário a ser criado ou bloqueado.

O volume de contratações e demissões é considerável, tendo em vista o aquecimento do mercado. Os dados dos últimos 7 meses mostram que há uma média de 1000 demissões / mês e consequentemente 1000 novas contratações, sendo assim, para criar 1000 novos acessos e bloquear 1000 acessos, a empresa necessita dispensar um tempo considerável para executar a atividade e com a possibilidade de erros no processo.

Com a implantação de um sistema corporativo de gerenciamento de identidade que gera / bloqueia automaticamente os logins, bem como os privilégios de acesso dos usuários na rede há um ganho em tempo e menores quantidades de solicitações junto ao help desk associadas à senha ou login. Desta forma, a equipe alocada para esta finalidade tem a oportunidade de se envolver em outros projetos de importância maior, evitando fraudes e minimizando erros nas liberações e bloqueios de acessos.

1.1 CONSIDERAÇÕES INICIAIS

Principais fatores que devem ser considerados para automatizar o processo de criação / bloqueio de logins na rede corporativa de uma empresa de Telecom:

- Quantidade elevada de solicitações de criação de novos acessos;
- Quantidade elevada de solicitações de bloqueio de colaboradores desligados;
- Incidência de erros ocorridos durante a execução do processo;
- Tempo de espera do novo colaborador para conclusão da criação do acesso;
- Aumento da segurança da informação com relação aos bloqueios de usuários desligados.

1.2 JUSTIFICATIVA

Principais benefícios que podem ser alcançados com a automatização do processo:

- Autonomia tecnológica;
- Redução de solicitações via help desk associadas à criação / bloqueio de logins;
- Redução de falhas e tempo de espera para a conclusão da criação de novo login no ambiente corporativo;
- Redução de custos com funcionário ocioso no tempo de espera para início de atividades com o login de rede.
- Alocar os analistas envolvidos no processo de criação / bloqueio de logins em projetos de maior importância.

1.3 PROBLEMA

A importância da automatização dos processos de criação / bloqueio de logins de acesso à rede corporativa.

1.3.1 Delimitação do Problema

Qual a contribuição da automatização dos processos de criação / bloqueio de logins de rede, bem como definir perfis de acesso no ambiente, utilizando-se de tecnologias da informação?

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Identificar os benefícios da automatização dos processos de criação e bloqueio de logins de rede no ambiente corporativo de empresa no ramo de Telecom, analisando ferramentas de Gerenciamento de Identidade.

1.4.2 Objetivos Específicos

- Avaliar ferramentas que possibilitem automatizar o processo manual de criação / bloqueio de logins;
- Avaliar os impactos e as contribuições da tecnologia de ferramentas de Gerenciamento de Identidade no processo de criação e bloqueio de logins de rede;
- Identificar e promover a autonomia tecnológica;
- Reduzir falhas humanas durante o desenvolvimento do processo de criação / bloqueio de logins;
- Reduzir o tempo de espera para a conclusão da criação de novo login no ambiente corporativo;
- Reduzir custos com funcionário ocioso no tempo de espera para início de atividades com o login de rede.

1.5 JUSTIFICATIVAS

Com a implantação de um sistema corporativo de gerenciamento de identidade que gera / bloqueia automaticamente os logins, bem como os privilégios de acesso dos usuários na rede é possível gerar um ganho em tempo, reduzindo a quantidade de solicitações de correções junto ao help desk associadas à senha ou login, além de estar minimizando a ociosidade de um novo colaborador.

Desta forma, a equipe alocada para finalidade de criar / bloquear logins tem a oportunidade de se envolver em outros projetos de importância maior minimizando erros nas liberações e bloqueios de acessos, contribuindo de maneira mais efetiva na companhia.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 AUTOMATIZAÇÃO DE PROCESSOS

A automatização de processos permite aos negócios controlar o desenvolvimento dos processos de diferentes aplicações, pessoas e sistemas para eliminar ineficiências, otimizar custos, garantir o cumprimento e impulsionar a produtividade.

Uma solução de automatização de processos traz absoluta flexibilidade, incluindo tarefas especiais, a capacidade para dirigir as complexidades do fluxo de trabalho e a implementação de políticas de gestão de trabalho.

Para Marques, (2007, pg. 2),

> “a automatização de processos é uma designação abrangente que procura sintetizar a capacidade de definir e otimizar os processos de negócio e em seguida executá-los sobre as arquiteturas informáticas ... é importante referir que a designação de processo de negócio não se limita à execução por computadores de atividades automáticas mas à visão mais abrangente de um processo de negócio que para além das atividades totalmente automáticas, realizadas por aplicações, bases de dados, etc., tem ampla intervenção de pessoas normalmente colaboradores da empresa, mas por vezes clientes ou parceiros”.

Para Capiotti, (2012),

> “a automatização de processos procura definir e otimizar os processos de negócio para, em seguida, executá-los sobre uma arquitetura de sistemas informatizada. Esta automação não está limitada à mera execução de atividades automáticas por computadores; vai além, mantendo uma ampla intervenção humana e a participação dos diferentes participantes relacionados, como colaboradores, clientes e parceiros”.

Antes de se pensar em automatizar é necessário analisar e representar minuciosamente as atividades realizadas durante o processo de criação e bloqueio de logins de rede. A partir deste ponto pode-se classificar, melhorar e otimizar as atividades bem como suas interligações e interações. Assim são geradas evidencias de que a possibilidade de executar várias partes ou até mesmo o processo por completo através de sistemas informáticos melhora a eficiência e a eficácia do processo como um todo.

Este ponto de partida é denominado Arquitetura de Processos.

Para Dawis, (2001, pg. 1554),

> **“**arquitetura de processos é a especificação da estrutura geral de um sistema de processos e um conceito aplicável a diversos campos tais como

> informática, gestão de processos de negócio, gestão estratégica etc. Processos são definidos como um fluxo de atividades que utilizam recursos (pessoal, informações, energia etc.) para transformar as entradas (insumos) em saídas (produtos)".

Para Marques, (2007, pg. 4),

> "em poucas palavras, a arquitetura de processos é definida tendo como ponto de partida a percepção de valor por parte dos clientes, e de seguida é analisada e optimizada em função dos colaboradores, das respectivas estruturas orgânicas e dos sistemas envolvidos na sua automação".

Sendo assim, o resultado da arquitetura de processos é o conjunto de representações e descrições dos processos.

A preocupação com a produtividade, com as melhores práticas, com a redução do risco operacional e com a qualidade, nos dias de hoje, fazem com que a empresa adote os sistemas de informação para ajudar nestes pontos.

Com os meios informáticos é possível obter dados de quanto tempo o processo leva para concluir e se ocorrer uma pausa, permite saber por que o sistema parou. Automatizando o processo consegue-se extrair indicadores para medir e então progredir.

2.1.1 A Importância da Automatização de Processos

Com o avanço tecnológico tão acentuado nos dias de hoje, os gestores de uma companhia de Telecom, tem cada vez mais oportunidades de aplicar a automatização de processos, pois compreendem a importância de gerir seus processos e os benefícios que a automatização pode gerar.

Visibilidade, identificação de oportunidades de melhorias e otimização de recursos são alguns resultados observados. Porém, para que esses perpetuem no decorrer do tempo, e para que a gestão se aproxime ainda mais do operacional e se propague por toda a empresa é preciso sustentação.

A automatização de processos é fundamental para os negócios, pois controla o desenvolvimento de diferentes processos, sistemas e pessoas. Ajuda a eliminar deficiências, reduzir custos e a impulsionar a produtividade.

É responsável por incluir tarefas especiais e está diretamente relacionada a flexibilidade, a capacidade de lidar com as complexidades do fluxo de trabalho, bem como, a implementação de políticas de gestão de trabalho.

Resumindo, a automatização de processos, simplifica as tarefas humanas em etapas por meio de conhecimento especializado, permitindo que as empresas captem as informações dos seus processos de negócio aperfeiçoando as atividades constantemente. Percebe-se então que a automatização dos processos é importante, pois sustenta a Gestão por Processos e possibilita, além da execução, controle, monitoramento de indicadores e constante otimização, além de gerar confiabilidade e qualidade no serviço.

2.1.2 Vantagens da Automatização de Processos

As vantagens de automatizar os processos são inúmeras e na atualidade já tem uma significativa aceitação nas preocupações da gestão das empresas.

Para Sganderla (2013), os benefícios típicos da automatização aparecem quando o processo de negócio:

> - "Envolve mais de uma área da empresa (melhoria da comunicação);
> - Permite extrair indicadores que demonstrem o desempenho do processo (melhoria do controle);
> - Deve ser controlado para que sua execução siga integralmente o fluxo modelado;
> - Possibilita apresentar informações de tempo do processo que possam apoiar as decisões que levarão à sua evolução (quanto tempo o processo leva hoje e quais atividades devem sofrer alguma melhoria para que esse tempo possa ser reduzido)".

Conforme a figura 1, os benefícios da automatização dos processos estão divididos em seis partes:

- Automatizar tarefas repetitivas e acelerar os tempos dos ciclos produtivos;
- Gestão das exceções aos processos automatizados;
- Monitorizar o pessoal e a performance dos processos;
- Capacidade de visualizar, simular e retirar problemas a processos de negócio;
- Alterar regras de negócio da empresa sem intervenção das TIC;
- Outros.

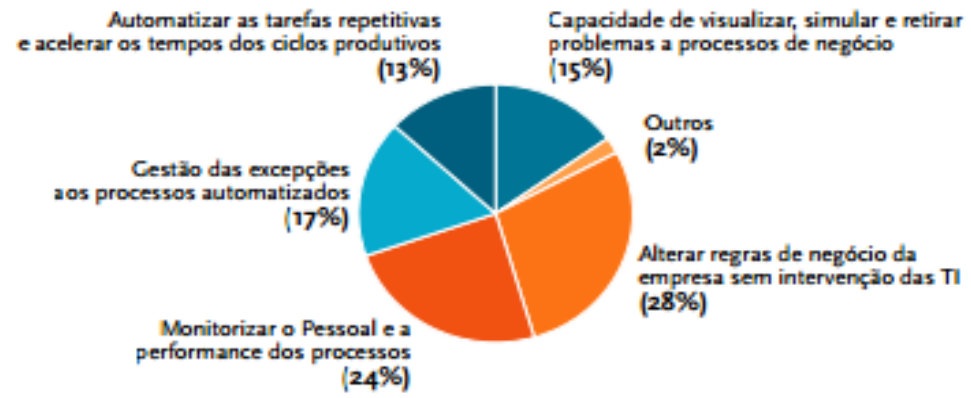


Figura 1. Principais benefícios da automatização de processo

Fonte: Automatização de Processos. Página 03 - http://www.link.pt/upl/%7Bd6dfd44a-3c8a-43ec-9276-9a1bb4baa4f9%7D.pdf

Neste estudo de caso, um dos principais fatores para a automatização dos processos de criação / bloqueio de logins na rede corporativa é o tempo de duração da execução do processo como um todo.

Para Sganderla, (2012), “para se estimar o tempo envolvido na realização de um processo, é necessário compreender os conceitos de: duração, execução e trabalho”.

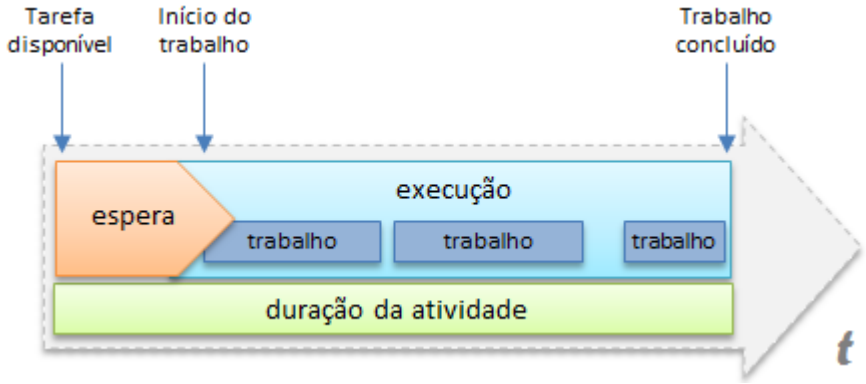


Figura 2. Execução de processo

Fonte: http://blog.iprocess.com.br/tag/beneficios-da-automacao-de-processos/

O trabalho ou esforço é o tempo que o analista de suporte a rede, efetivamente leva para criar ou bloquear um login.

A execução é o tempo dispendido desde o início da criação e ou bloqueio de login até a sua conclusão, incluindo neste tempo também, outras atividades que fazem parte do processo, como a solicitação de criação ou do bloqueio de login.

A duração é o tempo calculado desde o momento em que a tarefa esteve disponível para o analista responsável por executar a criação e ou bloqueio do login.

Ao analisar a execução do processo, deve-se conhecer o tempo de trabalho, execução e duração de cada atividade envolvida.

Em processos manuais como é o caso, a duração também é afetada pelo *handoff*, que é a espera dispendida no transporte das informações do processo entre os analistas responsáveis pela execução das criações e ou bloqueios de logins.

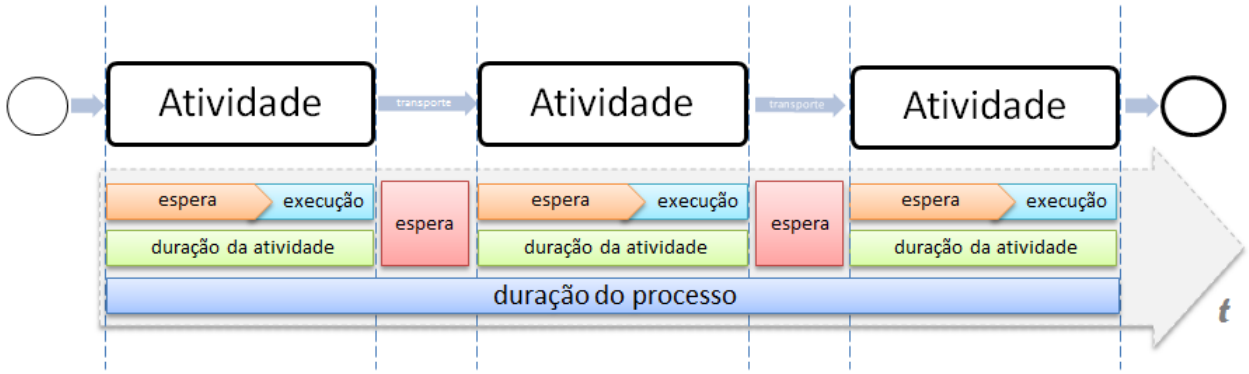


Figura 3. Tempo de espera durante a execução

Fonte: http://blog.iprocess.com.br/tag/beneficios-da-automacao-de-processos/

Para Sganderla (2012), há dois benefícios comumente identificados na automatização relacionados ao tempo de execução do processo:

- "Eliminação do tempo de *handoff*, já que o motor do processo disponibiliza as informações ao próximo participante imediatamente após a conclusão da atividade anterior;
- Eliminação do tempo de espera em atividades executadas pelo sistema (como serviços de busca ou gravação de informações, por exemplo), já que a execução das mesmas é realizada imediatamente quando a atividade é disponibilizada".

2.2 SEGURANÇA DA INFORMAÇÃO

Durante a automatização do processo de criação / bloqueio de logins na rede corporativa, há a preocupação com a questão da segurança da informação. É obrigatório garantir que as políticas de segurança da informação serão aplicadas corretamente a fim de evitarem-se problemas.

O controle de acesso lógico, definido na política de segurança da informação, tem o objetivo de proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

Os controles de acesso lógico são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou por outros programas de computador. (Tribunal de Contas da União, 2007, pg. 9).

A proteção aos recursos computacionais está mapeada de acordo com as necessidades de acesso de cada usuário, enquanto que a identificação e autenticação do usuário são efetuadas normalmente por meio do login (ID) e pela senha durante o processo de logon no sistema.

Objetivos do controle:

- Apenas usuários autorizados tenham acesso aos recursos;
- Os usuários tenham acesso aos recursos necessários a execução de suas tarefas;
- O acesso a recursos críticos seja monitorado e restrito;
- Os usuários sejam impedidos de executar transações incompatíveis com sua função ou responsabilidades.

Na prática, para analistas de TI, o controle de acesso lógico resume-se em:

- Conjunto de funções de identificação e autenticação de usuários;
- Alocação, gerência e monitoramento de privilégios;
- Limitação, monitoramento e bloqueio de acessos;
- Prevenção de acessos não autorizados.

Aplicando estes métodos é garantida a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela organização.

Neste controle, o usuário é peça fundamental. A utilização de senhas fracas ou até mesmo compartilhadas, ou descuido na proteção das informações podem acarretar prejuízos financeiros a companhia.

Além destes controles, a política de senhas está embutida no processo e deve garantir que a escolha da senha de acesso à rede corporativa siga o padrão para gerar uma senha forte.

Para a escolha de uma senha forte, é necessário considerar:

- Letras maiúsculas e minúsculas, números e caracteres especiais, embaralhados;
- Composta por no mínimo 07 caracteres, ou mais;
- Efetuar a troca da senha periodicamente.

3 METODOLOGIA DA PESQUISA PARA ESTUDO DE CASO

O projeto fundamenta-se em pesquisa bibliográfica com observações do cotidiano da equipe responsável pelo controle de acessos a rede corporativa, com pesquisas qualitativa, quantitativa e exploratória para coleta e análise de dados do ambiente corporativo de uma empresa de Telecom.

Articulando e confrontando as informações adquiridas ao longo do projeto com os conhecimentos teóricos da literatura pesquisada em livros, artigos científicos, revistas especializadas, documentos oficiais, revistas eletrônicas entre outros para que possibilitem uma interação entre estudo e análise do objeto de estudo.

A principal atividade da equipe é criar logins de acesso a rede corporativa, aplicando em cada login novo as policies de acesso condizentes com o cargo do funcionário, bem como, as atividades diárias.

Em uma segunda fase do processo, efetuar o bloqueio das contas de usuários desligados da empresa, removendo todos os acessos liberados no momento do ingresso do funcionário na companhia.

Este trabalho é efetuado manualmente pela equipe, e cada criação de novo login, ou até mesmo bloqueio do acesso, leva em média 5 minutos, por usuário, para conclusão da atividade.

Além do tempo despendido para efetuar as criações e bloqueios manualmente, há o risco da ocorrência de erros durante o processo. Tarefas repetitivas estão sujeitas a falhas, seja por excesso de confiança do analista que esta desenvolvendo a atividade, ou até mesmo, por pressões sofridas com relação ao prazo de entrega (SLA). Sendo assim, há também uma quantidade de retrabalho, já que o usuário final depende que o login esteja funcionando corretamente para que possa desempenhar suas atividades cotidianas normalmente.

Através de relatórios de quantidade de solicitações de criação / bloqueio de acessos, solicitações de correções de erros e também de um relatório de eficiência deste serviço é possível analisar a viabilidade da automatização de ambos os processos. Além disso, com base no cotidiano da equipe, pode-se avaliar o esforço bem como a qualidade do serviço prestado. Desta forma, é reduzido o tempo de espera na criação de um novo acesso, bem como no bloqueio de acessos de usuários desligados evitando acessos indevidos e minimizando a ocorrência de erros e retrabalho durante ambos os processos.

O gráfico 1 mostra a demanda recebida para criação de novos logins de rede nos meses de Janeiro a Julho do ano de 2013.

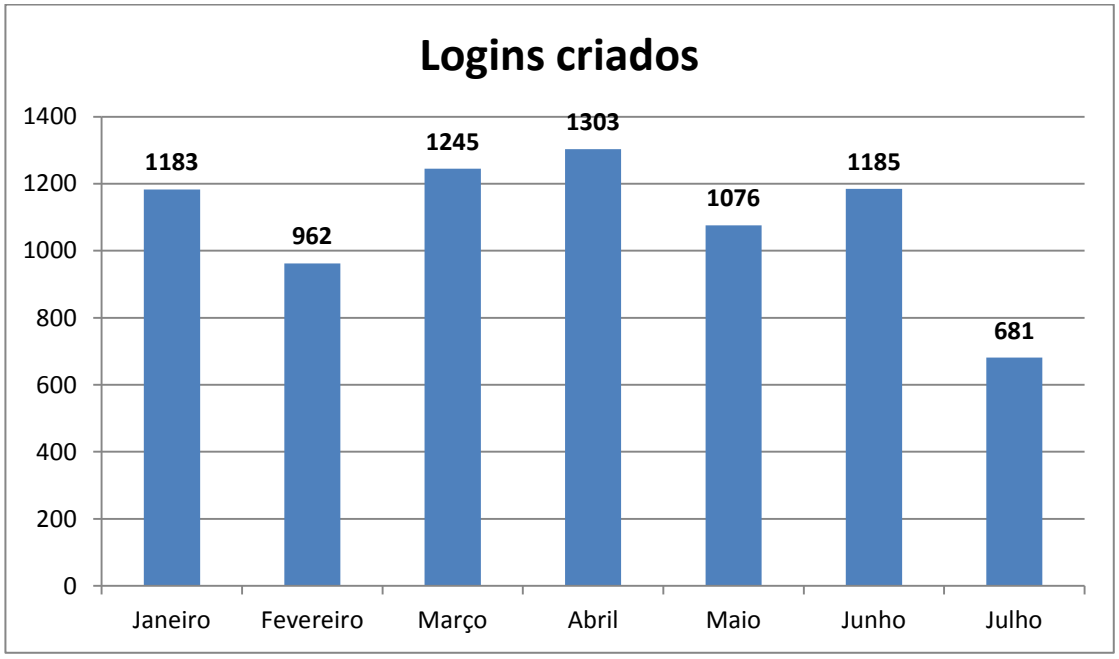


Gráfico 1. Logins criados

Fonte: A autora

A demanda é considerável, levando em conta que o processo é todo manual e o SLA para atendimento de cada solicitação é de apenas 4 horas. Analisando as solicitações do mês de Janeiro, 1.183 solicitações, considerando que o tempo de atendimento de cada uma é de aproximadamente 5 minutos, teríamos um total de 5.915 minutos, ou seja, são necessárias 98,58 horas, aproximadamente 2 semanas para atendimento da demanda completa. Claro que cada solicitação é efetuada em data e hora diferente uma da outra, mas há a incidência de picos de solicitações no inicio e fim do mês, devido ao fato de conciliar as contratações de acordo com o fechamento da folha de pagamento.

Além das solicitações de criação de novos logins a equipe recebe em paralelo as solicitações de bloqueio dos logins de colaboradores que foram desligados.

No gráfico 2 observa-se que praticamente na mesma quantidade em que se contratam novos funcionários, também desligamentos são efetuados.

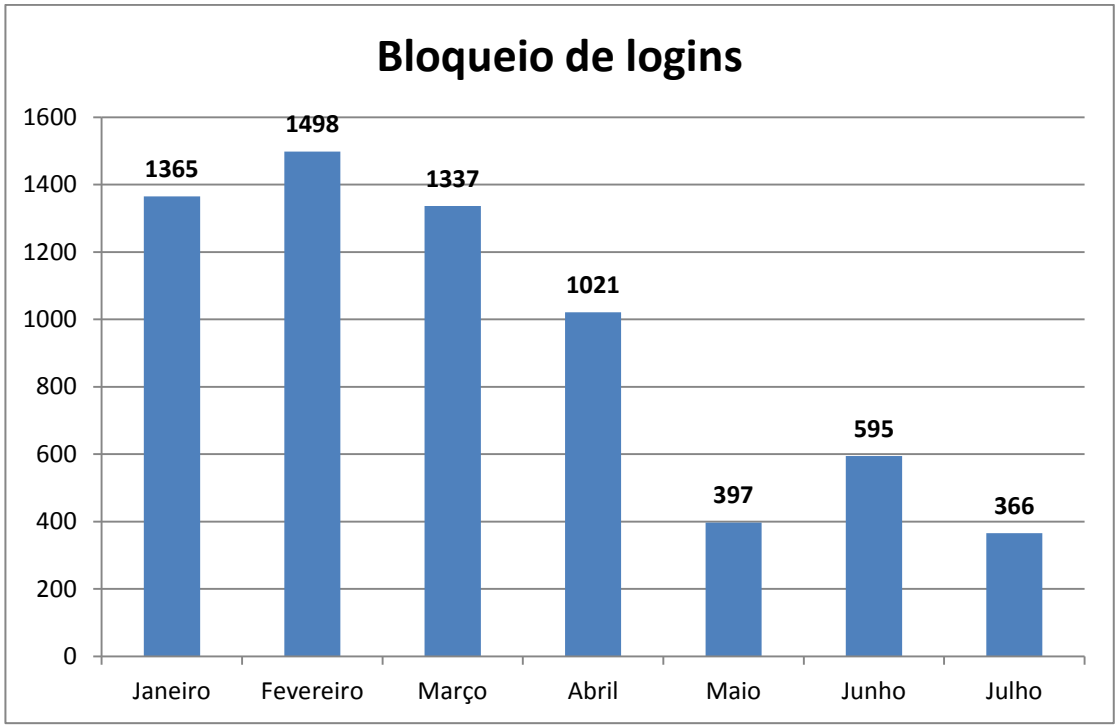


Gráfico 2. Bloqueio de logins

Fonte: A autora

Da mesma forma que as solicitações de logins possuem um prazo para atendimento, os bloqueios também possuem SLA de 4 horas. O SLA é curto, já que a principal preocupação da empresa é desativar todos os acessos do colaborador desligado a fim de evitar possíveis ações mal intencionadas por parte deste ex-funcionário.

Por se tratar de uma atividade manual, na qual todos os analistas envolvidos, desde o analista de RH até o analista que efetivamente irá criar o login na rede, devem ter o máximo de atenção para concluir com êxito, e levando em conta que há certa pressão devido ao prazo para atendimento ser curto, a execução desta tarefa repetitiva, quando desempenhadas por pessoas, estão suscetíveis a erros.

Analisando o dia-a-dia da equipe responsável por criar / bloquear logins de rede, é perceptível a incidência de solicitações para corrigir erros ocasionados por excesso de confiança, pressão, e em alguns casos falta de atenção.

Os problemas mais comuns que ocorrem com relação à criação de logins são:

- Dados dos colaboradores inseridos incorretamente nos sistemas de RH e replicados para a Intranet, e-mail e login de rede. Ex: Nome – Colaborador cadastrado com o nome do pai ou do filho / erros de grafia;
- Inexistência de dados, tais como, cargo, gestor, centro de custo, etc;

- Existência de outro login de rede associado ao mesmo colaborador (terceiro, estagiário, temporário);
- Colaboradores homônimos;
- Demissão Incorreta ou indevida.

O gráfico 3, mostra que no mesmo período de Janeiro a Julho do ano de 2013 a quantidade de problemas com os logins criados é alta.

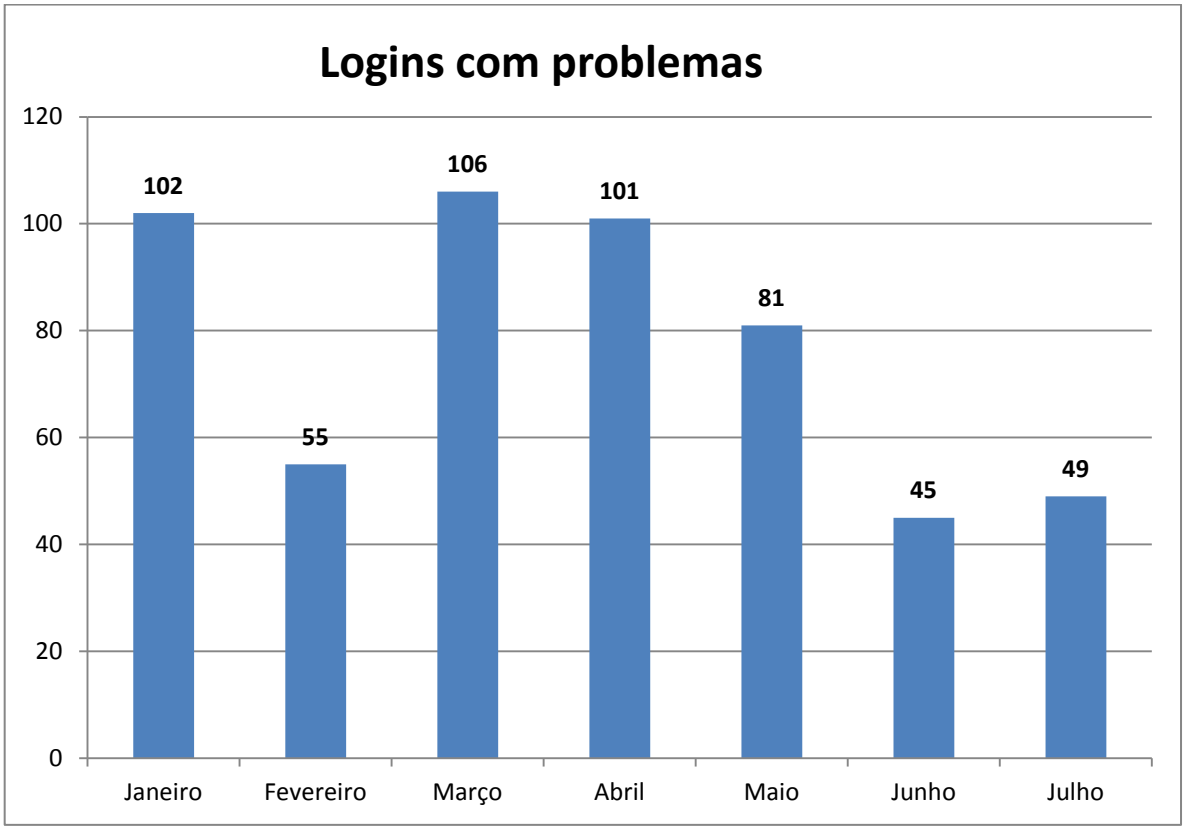


Gráfico 3. Logins com problemas

Fonte: A autora

Se comparado com o total de criações, aproximadamente 10% do total apresenta erro, gerando retrabalho e ociosidade para o usuário do login.

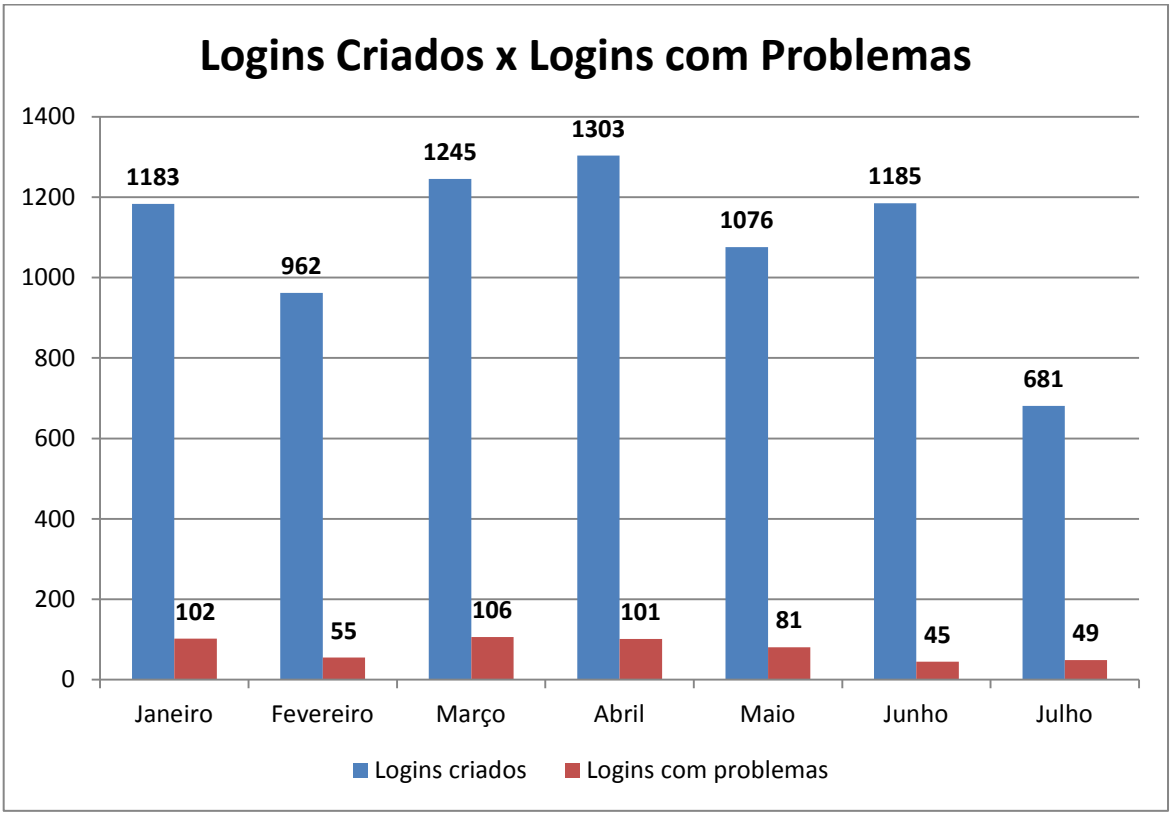


Gráfico 4. Relação entre Logins criados X Logins com problemas

Fonte: A autora

Além dos dados apresentados e com base no dia-a-dia da equipe que efetua as criações de logins, é possível identificar que a quantidade de reclamações que são recebidas, sejam através de telefonemas no help desk, ou até mesmo o contato direto com o gestor imediato, são inúmeras. Estas constantes reclamações demonstram a insatisfação do cliente interno com relação ao processo para se obter ou até mesmo corrigir um login.

4 MAPEAMENTO DO PROCESSO DE CRIAÇÃO/BLOQUEIO DE LOGINS EM EMPRESAS DE TELECOM

Em empresas de Telecom há um grande numero de funcionários e consequentemente o volume de admissões e demissões é alto. Um dos principais setores onde nota-se uma rotatividade constante é o Call Center. Normalmente este setor não exige uma alta qualificação dos funcionários como pré-requisito para contratações, sendo assim, é comum que o setor proporcione muitas vezes o primeiro emprego.

A rotatividade no setor deve-se muitas vezes a fatores organizacionais como a insatisfação dos funcionários quanto à questão salarial e benefícios, supervisores e gestores, pressão por metas estabelecidas pela empresa, horário de trabalho e possibilidade de crescimento.

Devido ao entra e sai de pessoal, a equipe responsável por gerenciar os usuários de rede recebe diariamente uma quantidade considerável de solicitações para criar novos usuários na rede e também bloquear os usuários desligados. Em períodos como inicio e fim do mês o numero de solicitações é ainda maior.

O processo de criação de um login na rede corporativa quando efetuado manualmente exige tempo além de muita atenção. Normalmente neste processo é definido o perfil de acesso que o usuário em questão deve ter na rede corporativa da empresa.

A existência de políticas de acesso na rede são de suma importância para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e de seus recursos associados.

Cada departamento da Companhia tem perfil de acesso diferenciado, condizente com o cargo e a atividade a ser desenvolvida, assim, acessos indevidos não são liberados protegendo o ambiente de rede de usuários mal intencionados. Desta forma, a equipe que gerencia os usuários de rede deve ter mapeado todos os acessos de rede pertinentes a cada departamento para criar o login.

4.1 SISTEMA TRADICIONAL

No ato da contratação de um novo colaborador, a primeira ação a ser tomada é efetuar o registro do mesmo no RH da empresa. Os dados do funcionário são imputados nos sistemas de controle de funcionários, normalmente, no módulo de folha de pagamento. A partir deste ponto é gerada uma matricula única que identifica o funcionário.

O próximo passo é incluir os principais dados do funcionário no módulo Colaboradores da intranet local. Este módulo permite aos colaboradores da empresa através de um campo de busca, visualizar dados de todos os funcionários ativos na companhia. Os dados apresentados nesse módulo são:

- Nome completo;
- E-mail corporativo;
- Telefone corporativo;
- Cargo;
- Departamento;
- Gestor Imediato;
- Localidade – Andar.

Concluída esta primeira etapa, a equipe responsável por criar o acesso do novo colaborador na rede corporativa tem condições de criar um perfil para este usuário.

O processo para criação deste novo login é totalmente manual. De posse da matricula do novo colaborador é gerada uma identificação (login) e senha que permitem o acesso ás informações e programas dentro de sua autorização.

Este login é criado em um sistema de serviços de diretórios capaz de autenticar e autorizar um usuário de computador acessar a rede corporativa, neste caso, o sistema é Active Directory.

No login é criado o endereço de e-mail e caixa postal do usuário, além de serem aplicados os acessos default pertinentes á função exercida, tais como:

- Policies de segurança;
- Bats para configurar drives de rede;

- Grupos que liberam acesso a Intranet;
- Grupos que bloqueiam acesso administrativo na estação de trabalho;
- Grupos que liberam acessos a aplicações internas;
- Entre outros.

Finalizada a criação do login, o gestor imediato do novo colaborador é sinalizado através de e-mail. Neste e-mail segue a informação de que a criação do login foi concluída e orientações de como proceder para efetuar o primeiro acesso a rede corporativa.

Em sua maioria, o acesso á rede é efetuado através de desktops da corporação dentro da empresa, neste caso a validação do acesso ocorre somente por autenticação de dois fatores, login e senha. Nos casos onde há a utilização de notebooks a validação é efetuada por autenticação de três fatores, sendo, login, senha e impressão digital.

O primeiro caso aplica-se a usuários de baixo escalão do organograma da empresa, operadores, analistas, supervisores. O segundo caso, aplica-se ao alto escalão do organograma, normalmente, coordenadores, gerentes, diretores, vice-presidentes, presidente.

Já no processo de bloqueio de um login de acesso rede corporativa deve-se desfazer todo o procedimento executado durante a criação do login.

O gestor imediato solicita ao RH o desligamento do funcionário. A partir desta premissa, as seguintes ações são tomadas:

- A conta é desabilitada;
- A caixa postal é desassociada;
- A BAT que configura drives de rede é removida;
- Os grupos que liberam ou bloqueiam acessos na rede são removidos;
- É inserida na descrição do login a data de bloqueio;
- O login é movido para um diretório de usuários desativados onde será excluído em definitivo da rede em 30 dias.

Neste ultimo item, conservar o login por 30 dias na rede em um diretório de contas desativadas é procedimento normal, tendo em vista que demissões incorretas podem ocorrer.

Pelo fato de ambos os processos serem efetuados de forma manual e devido à grande quantidade de solicitações recebidas, há certa demora na conclusão de cada processo, além de haver a possibilidade de falhas humanas, sobrecarregando a equipe responsável pela rede com esta atividade.

Hoje as empresas tem urgência em agilizar os processos de criação e bloqueio de acesso a rede, pois no primeiro caso, criação de acesso, há urgência em que o funcionário recém contratado comece a produzir e gerar lucros, no segundo caso, bloqueio, há urgência em bloquear o acesso devido a questões de segurança das informações contidas na rede.

4.1.1 Funcionamento

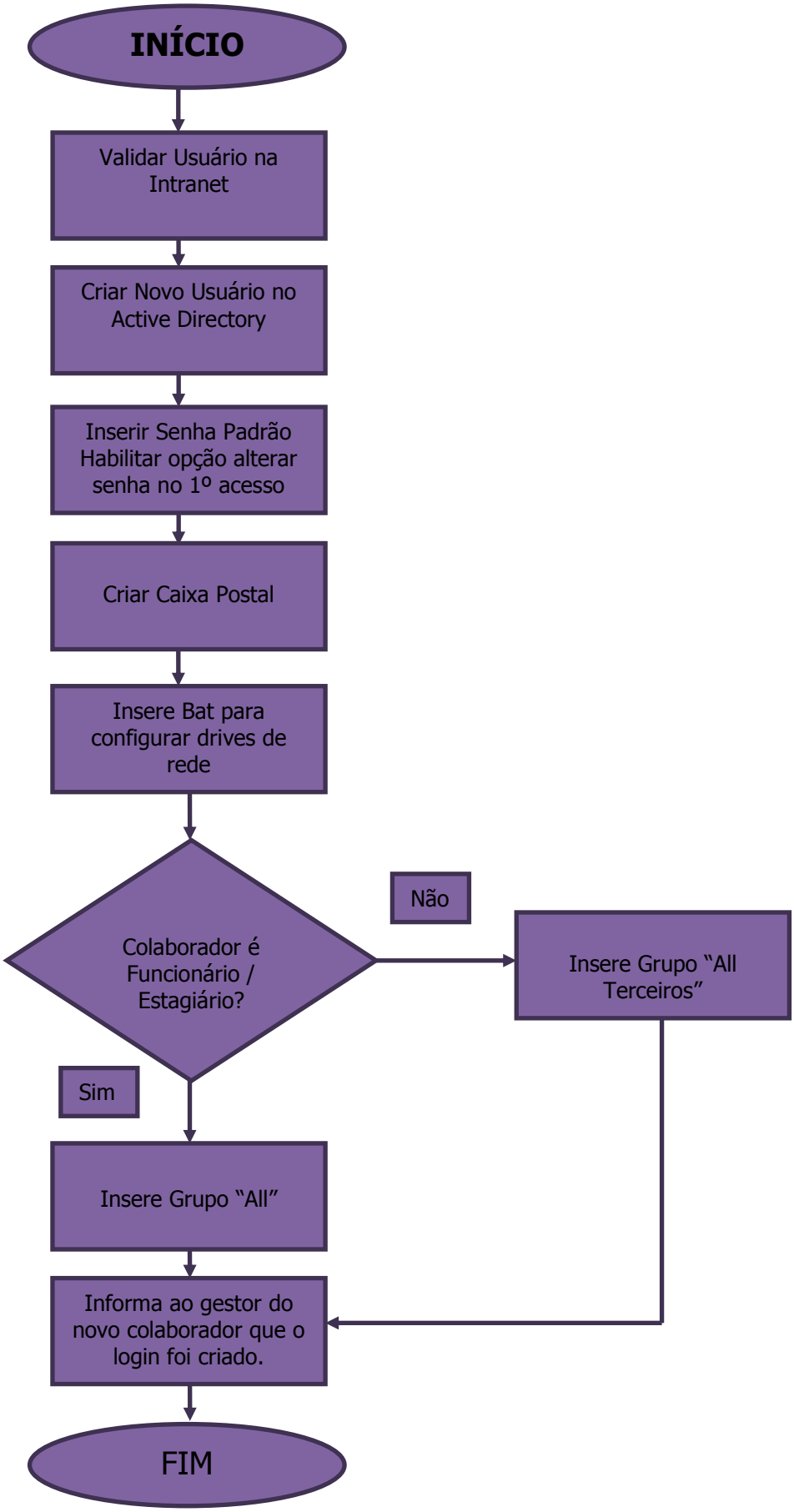
Todo o processo para a criação de login, descrito no tópico acima leva em média 4 dias úteis para a conclusão e só é iniciado no primeiro dia de trabalho do novo colaborador.

Levando em consideração de que o colaborador precisa produzir resultados positivos para a empresa, ficar aproximadamente 4 dias ocioso é perca de dinheiro e recurso.

Resumindo todo o processo desde seu início:

- RH Cadastra novo usuário no sistema de folha de pagamento;
- Cadastra no modulo “Colaboradores” da Intranet;
- Equipe responsável por criar logins na rede, valida usuário na Intranet;
- Cria usuário no Active Directory (AD);
- Insere senha padrão e habilita opção para alterar a senha no primeiro login;
- Cria caixa postal;
- Insere BAT para configurar drives de rede;
- Valida tipo do usuário e insere grupo;
    - Se usuário é colaborador ou estagiário, insere grupo “All”
    - Se usuário é terceiro, insere grupo “All-Terceiros”;
- Envia e-mail ao gestor do colaborador informando login e senha criados.

O fluxograma 1 exemplifica o processo manual para criação de um novo login na rede a partir do ponto em que a equipe de RH já concluiu o cadastro do novo colaborador nos sistemas de folha de pagamento:



Fluxograma 1. Sistema manual de criação

Fonte: A autora

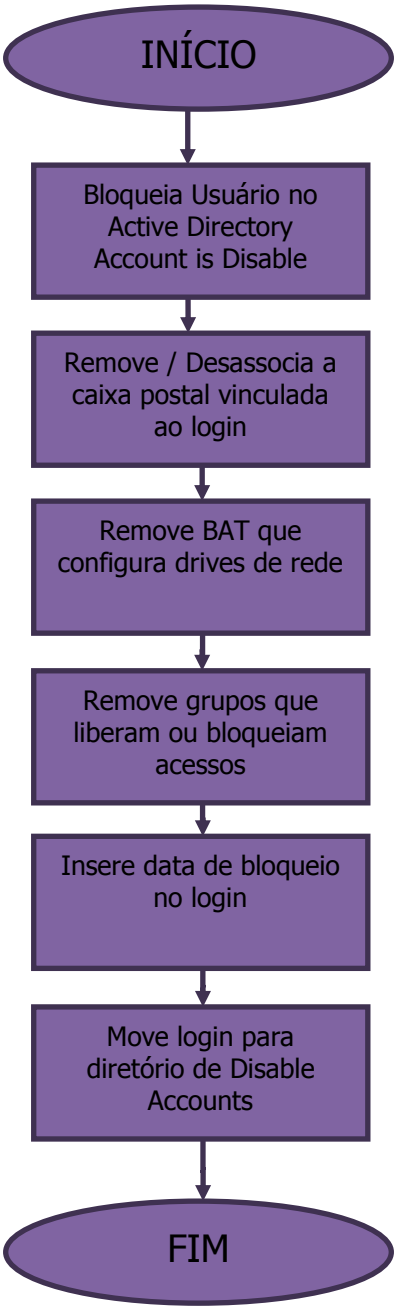
Já no processo de bloqueio de logins na rede, o procedimento é o contrário. Toda ação tomada durante a criação do login deve ser desfeita e o login do funcionário desligado deve ser movido para um local especifico no qual no prazo de 30 dias será removido em definitivo dos sistemas.

Tem-se como procedimento bloquear o login e deixá-lo ainda nos sistemas no prazo de 30 dias, pelo fato de que em alguns casos, o funcionário desligado, poderá recorrer a métodos judiciais que comprometam a saída em definitivo da empresa. Um exemplo típico de situações como esta é se o funcionário desligado estiver gestante ou até mesmo com a justificativa de atestado médico. Outro fato que pode ocorrer é o equívoco no momento de desligar um colaborador, ao invés de desligar X, desliga-se o Y. Nestes casos o login do funcionário pode ser reativado e o colaborador retornará as suas atividades normalmente.

Resumindo o processo de bloqueio de login:

- Gestor solicita ao RH o desligamento do funcionário;
- RH delimita o login nos sistemas de RH;
- RH envia solicitação de bloqueio na rede;
- Equipe responsável por bloquear logins executa o bloqueio:
    - Desabilitando a conta;
    - Desassociando a caixa postal;
    - Removendo a bat que configura drives de rede;
    - Removendo os grupos que liberam ou bloqueiam acessos na rede;
    - Insere data de bloqueio;
    - Move o login para um diretório de usuários desativados onde será excluído em definitivo da rede em 30 dias.

O fluxograma 2 exemplifica o processo manual para o bloqueio de um login na rede a partir do ponto em que a equipe de RH já concluiu a delimitação do colaborador nos sistemas de folha de pagamento:



Fluxograma 2. Sistema manual de bloqueio

Fonte: A autora

Finalizado o bloqueio do usuário na rede, 30 dias após, este login é removido em definitivo do sistema. Neste caso, a equipe responsável por esta atividade efetua todos os meses no primeiro dia útil do mês vigente a limpeza no diretório de contas desativadas.

4.1.2 Proposta para a automatização do processo

Com base na descrição do funcionamento dos processos de criação e bloqueio de logins, além da analise efetuada através dos números de solicitações recebidas que são apresentados nos gráficos anteriores, é possível avaliar a possibilidade de automatizar o processo.

4.1.2.1 Necessidade

Com um alto número de funcionários, em empresas de telecomunicações, é inviável que a criação / bloqueio dos acessos a rede seja efetuada de forma manual.

A partir do momento em que o novo colaborador já esta cadastrado nos sistemas do RH e devidamente incluído no módulo Colaboradores da Intranet, o processo manual para criar / bloquear os acessos á rede corporativa leva em torno de 5 minutos por usuário a ser criado ou bloqueado.

Geralmente no inicio do mês o volume de contratações é elevado, este fato pode ocasionar atrasos nas criações além de aumentar a incidência de erros durante execução do procedimento.

Para reduzir atrasos e erros durante a criação de um novo usuário, aplica-se a automatização do processo, ou seja, implantar um sistema que efetue as criações/bloqueios destes usuários de forma automática com o mínimo de intervenção humana.

A avaliação de ferramentas que executem estes processos é fundamental para obter-se sucesso na operação. Todos os pré-requisitos da ferramenta a ser implantada para solução do caso devem ser atendidos, tais como:

- Função Single Sign On, permitindo que o usuário final utilize a mesma senha de acesso à rede corporativa nos demais sistemas necessários para o desenvolvimento das atividades rotineiras;
- Possibilidade de customização, sendo possível incluir novas automatizações de criações de acessos a outros sistemas;
- Gerenciamento de identidade de usuários;
- Gerenciamento dos privilégios de acesso de usuários durante a vida útil;
- Eliminação de erros manuais;

- Redução de custos;
- Redução do tempo de espera para a conclusão da criação de um novo acesso / bloqueio do mesmo.

4.1.2.2 Funcionamento

A idéia principal neste ponto é automatizar o processo para que o mesmo necessite o mínimo de intervenção humana, neste caso que a única intervenção seja executada pela equipe RH no ato em que um novo colaborador é contratado. A partir deste ponto a ferramenta deve replicar os dados para a intranet no portal de colaboradores e replicar para o *Active Directory*.

4.1.2.3 Funcionamento do sistema proposto

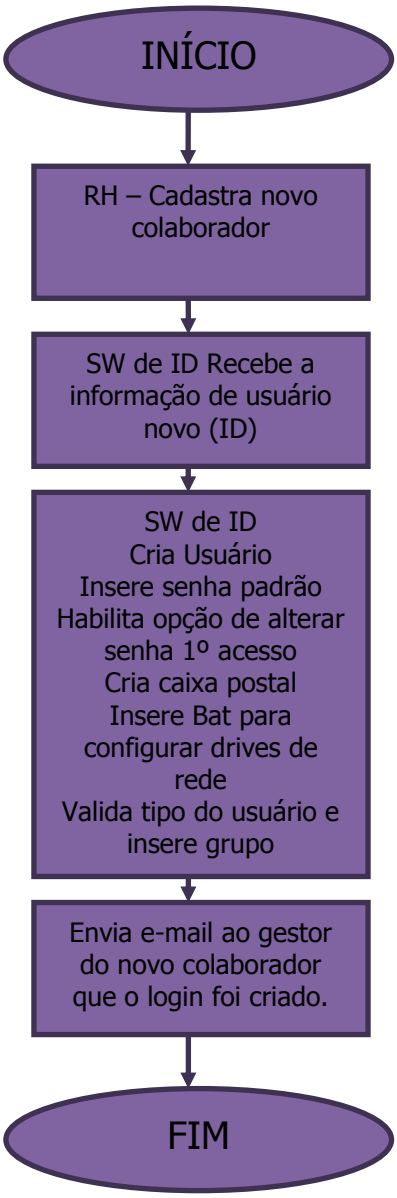
No primeiro momento para a criação de um novo login, é necessário que sejam inseridos os dados do novo colaborador. Esta fase do processo é efetuada de forma manual pela equipe de RH que estará cadastrando o novo colaborador nos sistemas de cadastro de funcionários e folha de pagamento.

Assim que os dados estiverem inseridos no sistema, a ferramenta de controle de identidade estará replicando as informações para a intranet, no portal de colaboradores e posteriormente para o *Active Directory*.

Resumindo o processo de criação de login na rede de forma automática:

- RH Cadastra novo usuário no sistema de folha de pagamento;
- Dados são replicados para a intranet, no portal de colaboradores;
- Software de controle de Identidades recebe a informação de usuário novo (ID) inicia o processo de criação do login na rede;
  - Cria Usuário;
  - Insere senha padrão;
  - Habilita opção de alterar senha 1º acesso;
  - Cria caixa postal;
  - Insere Bat para configurar drives de rede;
  - Valida tipo do usuário e insere grupo;
- Concluída a criação, dispara-se o e-mail para o gestor imediato do novo colaborador com a informação de login e senha.

O fluxograma 3 mostra o fluxo do processo de criação de login na rede de forma automática, eliminando ou até mesmo minimizando atrasos, erros no processo e interferência humana.



Fluxograma 3. Criação de login automatizado

Fonte: A autora

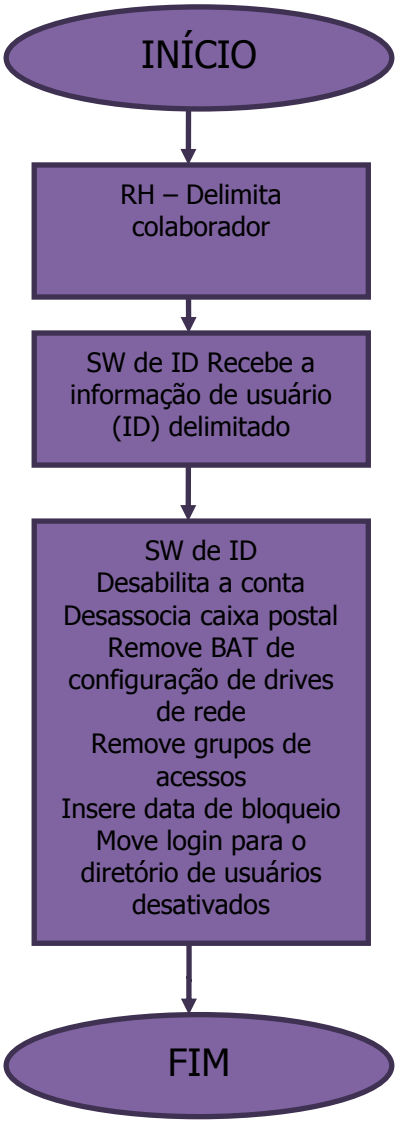
No caso do bloqueio de login de acesso a rede, assim que o gestor imediato solicitar ao RH o desligamento de um funcionário, a única intervenção manual por parte da equipe de RH é delimitar o usuário nos sistemas de folha de pagamento, marcando apenas um *flag*.

A partir do momento em que o *flag* de demissão esta marcado, esta ação é replicada para a ferramenta removendo o usuário da Intranet, no portal de colaboradores, e efetuando o bloqueio no *Active Directory*.

Resumindo o processo de bloqueio de login de rede de forma automática:

- RH delimita usuário no sistema de folha de pagamento;
- Informação é replicada para a intranet, no portal de colaboradores, removendo o usuário;
- Software de controle de Identidades recebe a informação de usuário (ID) delimitado e inicia o processo de bloqueio do login na rede;
    - Desabilitando a conta;
    - Desassociando a caixa postal;
    - Removendo a bat que configura drives de rede;
    - Removendo os grupos que liberam ou bloqueiam acessos na rede;
    - Insere data de bloqueio;
    - Move o login para um diretório de usuários desativados onde será excluído em definitivo da rede em 30 dias.

O fluxograma 4 mostra o fluxo do processo de bloqueio de login de forma automática, minimizando a interferência humana e aumentando a segurança das informações da empresa, bloqueando o acesso a rede do usuário no momento em que ele é desligado.



Fluxograma 4. Bloqueio de login automatizado

Fonte: A autora

5 ANÁLISE DE FERRAMENTAS DISPONÍVEIS NO MERCADO

Com base nas necessidades descritas nos tópicos anteriores, foram avaliadas duas ferramentas para a automatização dos processos de criação e bloqueio de logins de rede.

As ferramentas que mais se adéquam a necessidade são:

- *OIM – Oracle Identity Manager com Oracle Access Manager*
- *IBM Security Identity Manager* com *IBM Security Access Manager for Enterprise Single Sign-On*

Comparando as ferramentas:

Especificações		
Funcionalidades	**Oracle**	**IBM**
Automatiza o provisionamento de contas	Sim	Sim
Automatiza o desaprovisionamento de contas	Sim	Não
Auto-atendimento	Sim	Sim
Controle de Acesso Baseado em Função	Sim	Sim
Política de Negação	Sim	Não
Recuperação e Reversão de Dados	Sim	Sim
Rastreamento do Status da Solicitação	Sim	Não

Gerenciamento de Senhas por parte do Usuário	Sim	Sim
Sincronização de Senha com *Active Directory*	Sim	Não
Política de Senha	Sim (mais de uma)	Sim (uma apenas)
Inclusão de Dispositivos Móveis para acesso	Não	Sim
Logs de acesso	Sim	Sim
Re-conciliação de Identidade	Sim	Sim
Re-certificação	Sim	Sim parcialmente
Gestão de Contas Genéricas	Sim	Sim
Customização	Sim	Sim com restrições

Quadro 1. Comparação das ferramentas

Fonte: A autora

5.1 *OIM – ORACLE IDENTITY MANAGER*

De acordo com as informações contidas no site da Oracle:

Oracle Identity Manager é um sistema de gerenciamento de identidade corporativa poderosa e flexível que gere automaticamente os privilégios de acesso dos usuários dentro dos recursos de TI da empresa. Sua arquitetura flexível lida facilmente com os requisitos de negócio de TI e mais intransigente e rigorosa - sem a necessidade de mudanças na infra-estrutura, políticas e procedimentos existentes.

Oracle Identity Manager é projetado para gerenciar os privilégios de acesso do usuário através de todos os recursos de uma empresa, ao longo de todo o ciclo de vida de gerenciamento de identidade - desde a criação inicial de privilégios de acesso para adaptar dinamicamente às mudanças nos requisitos de negócios.

É um produto de gerenciamento de identidade que automatiza o provisionamento de usuários, administração de identidade e gerenciamento de senhas, integrados em um mecanismo de fluxo de trabalho completo.

Automatizando o provisionamento de identidade do usuário é possível reduzir a Tecnologia da Informação (TI) custos administrativos e melhorar a segurança, além de desempenhar um papel importante no cumprimento da regulamentação. As principais características do *Oracle Identity Manager* incluem o gerenciamento de senhas, fluxo de trabalho e gerenciamento de políticas, reconciliação identidade, informação e auditoria, e extensibilidade por meio de adaptadores.

As características do Gerenciador de Identidades podem ser divididas nas seguintes categorias:

- *Self-Service* e Administração delegada: Com a implantação de características de auto-atendimento e delegar funções administrativas, uma organização pode aumentar a produtividade do usuário, satisfação do usuário, e eficiência operacional.

    - *Profile Management*: Os usuários podem visualizar e editar seus próprios perfis usando a interface do *Oracle Identity Manager self-service*. Isso reduz a sobrecarga administrativa e fornece aos usuários o controle sobre seus perfis de identidade.

- Pedido de Gestão: A interface de auto-serviço também permite que os usuários criem solicitações de aprovisionamento por recursos com direitos de granulação fina. Aprovadores de negócios, como líderes de equipe, gerentes de linha e chefes de departamento, podem usar a mesma interface baseada na Web para examinar e aprovar as solicitações de entrada. Isso ajuda as organizações em reduzir o esforço e custo.
- Configurável Proxy usuário: O *Oracle Identity Manager* apresenta uma estrutura de segurança altamente flexível que suporta delegação da maioria das funções administrativas a qualquer grupo ou usuário. Ao mover pontos de administração mais próximo do usuário quanto possível, uma organização pode alcançar um controle mais rígido e melhor segurança, aumentando a produtividade ao mesmo tempo.

- Fluxo de Trabalho e Política: O uso de fluxo de trabalho e política de automatizar processos de negócios e de TI pode levar a melhoria da eficiência operacional, segurança, conformidade e controle de mais custo-efetiva. *Oracle Identity Manager* fornece os seguintes recursos nesta categoria:
  - Gestão de Políticas: Permite o provisionamento automatizado com base em políticas de recursos com direitos de granulação fina. Para qualquer conjunto de usuários, os administradores podem especificar níveis de acesso para cada recurso a ser provisionado, concedendo a cada usuário apenas o nível exato de acesso necessário para concluir o trabalho. Essas políticas podem ser impulsionadas por papéis de usuário ou atributos, permitindo a implementação de controles de acesso baseado em função. A mistura eficaz de políticas baseadas em função e baseada em atributos é a chave para uma solução escalável e gerenciável destes provisionamentos na organização. Além de uma política de provisionamento automatizado, o *Oracle Identity Manager* também suporta uma política de negação. A política de negação é usada para negar explicitamente o acesso do usuário a recursos específicos, reforçando, assim, as políticas de segurança e governança, como a segregação de funções.

- *Workflow Management*: *Oracle Identity Manager* suporta a separação de aprovação e fluxos de trabalho de provisionamento. Um *workflow* de aprovação permite a organização modelar seus processos de aprovação preferenciais de gestão dos pedidos de acesso aos recursos. Um fluxo de trabalho de provisionamento permite uma organização de TI automatizar tarefas de provisionamento de recursos os procedimentos mais complexos de aprovisionamento. A separação destes dois fluxos de trabalho permite aos negócios e a TI designar proprietários para gerenciar o trabalho de forma eficiente com interferências mínimas entre processos. Além de alavancar os fluxos de trabalho existentes em sistemas já implantados, como um help desk e HRMS, na organização. *Oracle Identity Manager* fornece o Visualizador de fluxo de trabalho que permite aos usuários de negócios, administradores e auditores visualizar e editar sequências de tarefas e dependências para compreender o fluxo do processo e do *Designer* de *Workflow* para editar e gerir o fluxo do processo.

- Tratamento de erros dinâmico: O tratamento de erros dinâmico do Oracle Identity Manager permite tratar exceções que ocorrem durante o provisionamento. Problemas frequentes, por exemplo, a ausência de recursos, não aborta a transação de provisionamento ou falha. A lógica de negócios definida dentro do fluxo de trabalho de provisionamento é personalizada de forma que seja à prova de falhas.

- Desconfigurações garantidas: Quando o acesso de um usuário não é mais necessário ou válido em uma organização, o *Oracle Identity Manager* revoga o acesso por demanda ou automaticamente, como ditado por papel ou políticas de acesso baseadas em atributos. Isso garante que o acesso de um usuário seja imediatamente encerrado quando ele é mais necessário. Isto é feito para minimizar os riscos de segurança e prevenir acessos indevidos aos recursos dispendiosos, tais como serviços de dados.

- Integridade da transação: *Oracle Identity Manager* fornece o alto nível de integridade da transação exigido por outros sistemas de organização de missão crítica. Possui a opção de reversão e capacidade de

recuperação. Quando uma transação de provisionamento falhar ou for interrompida, o sistema é capaz de recuperar e reverter para o último estado bem sucedido ou redirecionar para um caminho diferente, de acordo com regras pré-definidas.

- *Real-Time Request* Rastreamento: Para manter um melhor controle e proporcionar melhor visibilidade em todos os processos de provisionamento, o *Oracle Identity Manager* permite os usuários e administradores rastrear o status da solicitação em tempo real, a qualquer momento durante uma transação de provisionamento.

- Gerenciamento de senha: Gerenciamento de senhas é uma das questões mais importantes nas organizações hoje em dia. A implementação de uma solução de gerenciamento de senha reduz o custo e despesas gerais relativos à criação de bilhetes ou ligações para help desk. Os recursos de gerenciamento de senha do *Oracle Identity Manager* visam ajudar as organizações nesta área.

  - Gerenciamento de senha *Self-Service*: Os usuários podem gerenciar suas próprias senhas através de recursos de auto-atendimento do *Oracle Identity Manager*. No caso de um usuário esquecer a senha, o *Oracle Identity Manager* pode apresentar perguntas de personalizáveis para permitir a verificação da identidade de auto-atendimento e recuperação de senha. A grande maioria das chamadas ao help desk estão relacionadas com a redefinição de senha e bloqueio. Ao reduzir a quantidade de chamadas de help desk, este recurso de auto-atendimento reduz os custos.

  - Gestão de Políticas *Advanced Password*: A maioria das melhores práticas é suportada fora da caixa e são configuráveis através de uma interface de usuário intuitiva. Requisitos de complexidade de senha suportados incluem: comprimento senha alfanumérica e uso de caracteres especiais, maiúsculas e minúsculas uso, total ou parcial, a exclusão do nome do usuário, a idade mínima da senha, senhas e históricos. *Oracle Identity Manager* permite definir políticas de senhas complexas que ultrapassam os requisitos de senha do *Microsoft Active Directory*. Além disso, o *Oracle*

Identity Manager permite a aplicação de várias políticas para cada recurso. Por exemplo, os usuários com menos privilégios podem ser submetidos a uma política de senha mais displicente, enquanto que os administradores privilegiados podem ser submetidos a uma política mais rigorosa.

- Sincronização de Senha: *Oracle Identity Manager* pode sincronizar ou mapear senhas entre recursos gerenciados e reforçar as diferenças de políticas de senhas entre esses recursos. Além disso, se uma organização está usando o recurso de redefinição de senha baseada em *desktop* do *Microsoft Windows*, o *Active Directory* (AD) conector do *Oracle Identity Manager* pode interceptar alterações de senha no servidor AD e, posteriormente, propagar essas alterações para outros recursos geridos de acordo com políticas. Semelhante capacidade de sincronização de senha bidirecional é apresentada na maioria dos conectores do Gerenciador de Identidade, para servidores de diretório e *mainframes*.

- Auditoria e *Compliance Management*: Gerenciamento de identidade é um componente-chave em qualquer solução de conformidade de auditoria de uma organização. *Oracle Identity Manager* minimiza o risco e reduz o custo no cumprimento das regras de governança interna e externa e auditorias de segurança.

  - Reconciliação identidade: Reconciliação é um dos importantes recursos do *Oracle Identity Manager*. Se o *Oracle Identity Manager* detecta quaisquer contas ou alterações aos privilégios de acesso do usuário efetuadas além de seu controle, então o mecanismo de reconciliação pode imediatamente toma as medidas corretivas, como desfazer a alteração ou notificar o administrador. *Oracle Identity Manager* também ajuda a detectar e mapear as contas existentes em recursos de destino. Isso ajuda na criação de uma identidade em toda a organização e perfil de acesso para cada funcionário, sócio, cliente ou usuário.

  - Gestão de Contas a *Rogue* e *Orphan*: A *desonestosconta* é uma conta criada "fora do processo", ou fora do controle do sistema de provisionamento. Uma conta órfã é uma conta operacional sem um

usuário válido. Estas contas representam sérios riscos de segurança á organização. *Oracle Identity Manager* pode monitorar *desonestosconta* e contas órfãs continuamente. Através da combinação de políticas de negação de acesso, fluxos de trabalho e de reconciliação, uma organização pode executar as ações corretivas necessárias quando tais contas são descobertas, de acordo com as políticas de segurança e governança. *Oracle Identity Manager* também pode gerenciar o ciclo de vida das contas de administrador. Estas contas têm necessidades especiais no ciclo de vida que vão além do ciclo de vida de um usuário comum. A gestão adequada das contas de serviço pode ajudar a eliminar a fonte de contas órfãs potenciais.

- Relatórios abrangentes e Auditoria: *Oracle Identity Manager* possui *logs* do estado atual do ambiente de provisionamento. Alguns dos dados de identidade capturados pelo *Oracle Identity Manager* incluem a identidade do usuário, tipo de perfil, grupo de usuários, logs de acesso, acesso aos recursos do usuário e histórico direito de granulação fina. *Oracle Identity Manager* também capta dados gerados pelo seu fluxo de trabalho, a política, e funções de reconciliação. Ao combinar esses dados, juntamente com dados de identidade, a organização tem todos os dados necessários para enfrentar auditoria de acesso em qualquer login de usuário.

- Atestação: Também conhecido como re-certificação, é uma parte fundamental de conformidade com as melhores práticas de segurança e é altamente recomendado. A organização normalmente atende a esses requisitos de certificação principalmente através de processos manuais baseados em relatórios de planilhas e e-mails. Estes processos manuais tendem a ser fragmentados, é difícil e caro para gerir e têm pouca integridade dos dados e auditoria. *Oracle Identity Manager* oferece um recurso de atestado que pode ser implantado rapidamente para permitir um processo de atestado de toda a organização gerando um relatório automático de entrega e notificação. Os administradores podem analisar os relatórios de acesso de granulação fina dentro de uma interface interativa que permite refinar a busca certificar, rejeitar, recusar, e delegar ações. Todos os dados do relatório e ações do administrador

são gravados para as necessidades futuras de auditoria. As ações do administrador podem, opcionalmente, desencadear uma ação corretiva, configurando o mecanismo de fluxo de trabalho do *Oracle Identity Manager*.

- Soluções de Integração: A arquitetura de integração escalável e flexível é fundamental para o êxito da implantação de soluções de provisionamento na organização. *Oracle Identity Manager* oferece uma arquitetura de integração comprovada e conectores pré-configurados para implementações rápidas e de baixo custo.
    - Adaptador de Fábrica: Integrar a maioria dos sistemas de provisionamento de recursos gerenciados não é fácil. A conexão com sistemas próprios pode ser difícil. O adaptador de fábrica elimina a complexidade associada à criação e manutenção dessas conexões. Esta ferramenta de geração de código permite criar classes Java. O Adaptador *Factory* fornece rápida integração com sistemas comerciais ou personalizados. Os usuários podem criar ou modificar integrações usando a interface gráfica do usuário do adaptador de fábrica, sem programação ou scripting. Quando os conectores são criados, o repositório do *Oracle Identity Manager* mantém suas definições, a criação de vistas de auto-documentação.
    - Conectores predefinidos: *Oracle Identity Manager* oferece uma extensa biblioteca de conectores pré-definidos para aplicações comerciais e outros sistemas de reconhecimento de identidade que são amplamente utilizados. Ao usar esses conectores, uma organização pode obter uma vantagem sobre a integração de aplicativos. Cada conector suporta uma ampla gama de funções de gerenciamento de identidade. Esses conectores usam a tecnologia de integração mais adequada e recomendada para o recurso de destino, seja ele proprietário ou baseada em padrões abertos. Esses conectores permitem a integração *out-of-the-box* entre um conjunto de sistemas de destino heterogêneos e *Oracle Identity Manager*, tendo em vista que os conectores fornecem um conjunto de componentes que foram originalmente desenvolvidos usando o adaptador *Factory*, possibilitando a customização com o adaptador de

fábrica atendendo as necessidades específicas de integração de cada organização.

- Conectores tecnologia genérica: Caso não sejam necessários os recursos de personalização do adaptador de fábrica para criar um conector personalizado, é possível utilizar o recurso Conector Tecnologia genérico do *Oracle Identity Manager* para criar o conector.

5.1.1 *Oracle Access Manager*

O módulo *Oracle Access Manager* (também conhecido como *Access Manager*) é a base da nova plataforma *Access Management Oracle*.

Access Manager fornece a funcionalidade principal da *Web Single Sign On* (SSO), autenticação, autorização, administração política centralizada e gerenciamento de usuários, gerenciamento de sessões em tempo real e de auditoria.

Principais recursos do *Access Manager* incluem:

- Simplificado *Web Single Sign On* (SSO)
- Autenticação e Autorização
- Política de Administração Centralizada
- Gerenciamento de Sessão avançada
- Agente de Gerenciamento simplificado
- Gerenciamento de senha Nativa
- Autenticação Nativa do *Windows*
- Auditoria abrangente e *Logging*

5.2 *IBM SECURITY IDENTITY MANAGER*

De acordo com as informações contidas no site da IBM:

O IBM *Tivoli Identity Manager* é uma solução de fornecimento de usuário baseada em política automatizada que gerencia funções de usuário, identidades e direitos de acesso na infraestrutura de TI. Este *software* de gerenciamento de

identidade seguro é fácil de implementar e usar. Ele ajuda as organizações menores a estarem em conformidade com os regulamentos, gerenciarem riscos e ativarem a colaboração segura.

O *Tivoli Identity Manager* economiza dinheiro e melhora a produtividade por meio de automação, autoatendimento do usuário e outras inovações

.

- Gerencia funções, contas e direitos de acesso automaticamente em todo o ciclo de vida, desde a implementação até o término. Isso reduz os custos de adicionais e elimina erros manuais.
- Acelera a implementação de novos aplicativos e usuários por políticas e modelos pré-configurados. O software fornece aos novos usuários recursos necessários em apenas minutos em vez de dias.
- Fornece interfaces de auto-atendimento para que os usuários possam modificar senhas e informações pessoais sozinhos. Isso reduz os custos de help desk e aumenta a produtividade da equipe de TI.
- Estabelece a separação de obrigações para fortalecer a segurança e a conformidade. Ele associa os requisitos que evitam conflitos de negócios com as funções e políticas de fornecimento que controlam direitos de acesso de usuário.
- Corrige e remove direitos de acesso não conformes por meio de fluxos de trabalho de retificação periódica ou acessar políticas de controle baseadas em funções. Este recurso poderoso fornece detalhes granulares de apoio à auditoria para demonstrar a conformidade.

5.2.1 *IBM Security Access Manager for Enterprise Single Sign-On*

De acordo com as informações contidas no site da IBM:

O IBM *Tivoli Access Manager* para Conexão Única Corporativa permite que os usuários acessem todos os seus aplicativos com uma única senha. Essa solução oferece suporte para aplicativos *Microsoft Windows*, da *Web*, Java, Telnet, de *mainframe* e aplicativos internos. Simplifica o gerenciamento de senha, protege as informações com autenticação forte e ajuda a proteger os quiosques e as estações de trabalho compartilhadas.

O *Tivoli Access Manager* para Conexão Única Corporativa ajuda a reduzir os custos, reforçar a segurança, melhorar a produtividade e atender aos requisitos de conformidade.

- Reduz os custos do help desk associados à senha ao diminuir o número de chamados de reconfiguração de senha. Quando os funcionários esquecem sua senha, eles podem reconfigurá-la usando um processo simples de pergunta e resposta.
- Permite senhas fortes para reforçar a segurança e atender aos regulamentos. O software fornece *tokens* USB inteligentes, *smart cards*, *tokens* com senha descartável e dispositivos biométricos de impressão digital. Também é possível usar os dispositivos de identificação existentes como crachás e telefones celulares.
- Melhora a produtividade e simplifica a experiência do usuário. Os usuários podem automatizar todo o fluxo de trabalho de acesso como login no aplicativo, mapeamento de unidades, ativação de aplicativo, conexão única, navegação para as telas preferenciais, logins com diversas etapas, entre outros.
- Registra e grava no *log*, de forma central e transparente, todas as atividades de login do usuário para facilitar o cumprimento dos regulamentos de privacidade e segurança. Além disso, fornece relatórios flexíveis para atender suas necessidades de conformidade.
- Fornece desconexão única em todos os aplicativos e configura políticas de proteção da área de trabalho para evitar acessos não autorizados aos aplicativos confidenciais. Se um usuário sair de uma estação de trabalho sem efetuar *logout*, o *software* pode impingir políticas de tempo limite de inatividade como bloqueios de tela configuráveis, políticas de *logout* do aplicativo, *logoffs* normais, entre outros.

6 IMPLANTAÇÃO DO SISTEMA AUTOMATIZADO EM UMA EMPRESA DE TELECOMUNICAÇÕES

O quadro 1, comparativo entre os *softwares* da *Oracle* e da IBM apresentado no tópico 5 deste documento, é de grande valia no momento da escolha de qual ferramenta atende melhor a necessidade da companhia de Telecom.

Avaliadas todas as funcionalidades apresentadas por cada uma das ferramentas é nítido que a ferramenta da *Oracle* oferece muito mais recursos do que a IBM. Sendo assim, opta-se escolher a ferramenta da *Oracle* para ser implantada, tendo em vista a riqueza de funcionalidades oferecidas, além da possibilidade de customização e implementação de aplicativos próprios da Companhia para provisionamento de contas futuramente.

Analisados todos os pontos positivos e também os negativos das ferramentas e efetuada a escolha da que mais se adequa para automatizar a criação e bloqueio de logins na rede corporativa, o próximo passo é partir para a implantação do novo método.

A primeira fase compreende a definição da metodologia de implantação, inclusive com o organograma das equipes e matriz de responsabilidades. Posteriormente já com o mapeamento do processo de criação e bloqueio de logins avaliam-se quais os níveis de parametrização e customização são necessários para a efetiva instalação do software, além de determinar o tempo gasto para cada etapa do projeto.

Definidas as configurações, parametrizações e customizações o *software* é implantado inicialmente para uma fase de testes em ambiente de homologação a fim de avaliar se todo o processo esta sendo executado conforme o previsto.

Em um primeiro momento ocorre somente a implantação da automatização para a criação de logins novos na rede. Esta fase de homologação da ferramenta é importante para que sejam avaliadas todas as falhas que podem ocorrer durante a execução do processo automático. Desta forma é possível avaliar a eficácia e eficiência do método.

Durante a fase de testes, os analistas da equipe responsável por criar logins na rede avaliam cada login criado pela rotina automática certificando-se que o processo esta sendo executado de maneira correta e apontando as falhas ocorridas para reportar a equipe de implantação efetuar as devidas correções. As solicitações

de criação de logins ainda são encaminhadas para a equipe apenas para conferência e caso o processo tenha ocorrido conforme o previsto é realizado o fechamento da solicitação

Concluída a etapa de testes, a ferramenta é disponibilizada em ambiente de produção. Neste ponto, o envio de solicitações de criação de logins a equipe responsável é eliminado. As solicitações existem, mas a ferramenta gera a solicitação, executa e efetua o fechamento da mesma encaminhando ao gestor imediato do login criado a notificação via e-mail com as informações de login e senha.

6.1 ANÁLISE COMPARATIVA DOS RESULTADOS

Conforme informado anteriormente, no primeiro momento houve apenas a implantação do sistema automático para criação de logins na rede. Com esta automatização eliminou-se o envio de solicitações para criação manual de novos logins, reduzindo a demanda de atendimento da equipe responsável por criar / bloquear logins na rede numa média de 1000 solicitações por mês.

Além da redução deste número, é perceptível a atenuação das solicitações de correções de logins com problemas tais como:

- Inexistência de dados, tais como, cargo, gestor, centro de custo, etc;
  - Neste caso a falta de dados impede a criação do login, tendo em vista que a ferramenta só efetua a criação, caso todos os dados necessários estejam inseridos.
- Existência de outro login de rede associado ao mesmo colaborador (terceiro, estagiário, temporário);
  - Validação por parte da ferramenta no campo CPF.
- Colaboradores homônimos;
  - Validação por parte da ferramenta no campo CPF.

Neste caso, houve a redução de 3 problemas dos 5 problemas mais comuns que ocorrem durante a criação de logins de maneira manual. Isso representa aproximadamente a redução de 70% de solicitações de correções de logins que a equipe recebe mensalmente.

Analisando também a rotina de trabalho da equipe de help desk, é perceptível a redução significativa das ligações relacionadas a problemas com senhas de acesso a rede. Antes da implantação da ferramenta, eram recebidas ligações relacionadas a problemas com senhas diariamente, e após a implantação, a equipe recebe ligações com este tipo de problema numa média de dia sim e dia não.

Através destas informações, tanto da redução do volume de solicitações de criação de novos logins na rede e solicitações de correções de problemas com logins, também da contração de ligações geradas no help desk com problemas de senhas, verifica-se que o cliente interno esta sendo bem atendido com relação ao acesso necessário para inicio das atividades na empresa de maneira rápida e eficaz.

Assim que a implantação da automatização do processo de bloqueio de logins ocorrer, a equipe responsável por criar / bloquear logins terá uma redução ainda mais significativa do volume de solicitações recebidas e conseqüentemente a segurança das informações contidas na rede será maximizada.

7 CONSIDERAÇÕES FINAIS

Com a implantação do sistema automático para criação de logins de acesso a rede corporativa, a empresa como um todo obteve ganhos na redução do tempo de atendimento (SLA) para a criação de novos logins na rede, minimizando o tempo de ociosidade de novos funcionários, gerando lucros com o inicio antecipado das atividades do novo colaborador.

Além deste beneficio, ao analisar os relatórios de solicitações de novos acessos na rede, é perceptível a redução de carga de trabalho manual encaminhada para a equipe responsável por efetuar a criação destes novos acessos na rede corporativa. Automaticamente, alguns dos problemas mais comuns com relação à criação de logins, são reduzidos, tais como, inexistência de dados, existência de outro login de rede associado ao mesmo colaborador (terceiro, estagiário, temporário) e colaboradores homônimos.

Os erros manuais são eliminados, além de evitar possíveis fraudes. Desta maneira, possibilita a equipe envolver-se em projetos de maior importância na companhia.

Num futuro próximo, implantando também a automatização do processo de bloqueio de logins, a redução da carga de trabalho manual encaminhada à equipe responsável por criar / bloquear logins na rede será ainda maior com isso, maximizando a segurança das informações contidas na rede.

8 POSSÍVEIS TRABALHOS FUTUROS

- Automatização do processo de bloqueio de logins de rede.
- Automatização do processo de criação/bloqueio de acesso em ferramentas utilizadas em Companhias de Telecom.

9 REFERENCIAS BIBLIOGRÁFICAS

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação / Tribunal de Contas da União.** – 2. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 22 abr. 2013.

CAPIOTTI, Paulo. **Benefícios da Automação de Processos.** Blog IPROCESS – 25 de junho de 2012. Disponível em: <http://blog.iprocess.com.br/2012/06/beneficios-da-automacao-de-processos/>. Acesso em: 10 jun. 2013.

DAWIS, E. P., J. F. Dawis, Wei-Pin Koo (2001). **Architecture of Computer-based Systems using Dualistic Petri Nets. Systems, Man, and Cybernetics**, 2001 IEEE International Conference on Volume 3, 2001 Page(s):1554 - 1558 vol.3

MARQUES, José Alves. Automatização de Processos. **Cadernos LINK** – Entrevista. Junho, 2007. Disponível em: <http://www.link.pt/upl/%7Bd6dfd44a-3c8a-43ec-9276-9a1bb4baa4f9%7D.pdf>. Acesso em: 22 abr. 2013.

SGANDERLA, Kelly. **Estudo de Caso: Automatizar o processo (ou não)? Eis a questão!.** Blog IPROCESS – 04 de fevereiro de 2013. Disponível em: <http://blog.iprocess.com.br/tag/beneficios-da-automacao-de-processos/>. Acesso em: 22 abr. 2013.

SGANDERLA, Kelly. **Estimando a duração de processos.** Blog IPROCESS – 10 de Setembro de 2012. Disponível em: <http://blog.iprocess.com.br/tag/beneficios-da-automacao-de-processos/>. Acesso em: 22 abr. 2013.

Site da Oracle. **Produtos Oracle.** Disponível em: <http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-090417.html>. Acesso em: 10 jun. 2013.

Site da Oracle. **Documentos Oracle.** Disponível em: <http://docs.oracle.com/cd/E10391_01/doc.910/e10374/idntmngr.htm#CFABGIIE> <http://docs.oracle.com/cd/E10391_01/doc.910/e10374/toc.htm>. Acesso em: 10 jun. 2013.

Site da IBM. Produtos IBM. Disponível em: <http://www-03.ibm.com/software/products/br/pt/access-mgr-esso> <http://www-03.ibm.com/software/products/br/pt/identity-manager>. Acesso em: 10 jun. 2013