# GERENCIANDO PRIVILÉGIOS EM TECNOLOGIA DA INFORMAÇÃO

## IMPLEMENTANDO A POLÍTICA DE PRIVILÉGIO MÍNIMO

JOHN MUTCH e BRIAN ANDERSON

Novatec

Editor: Rubens Prates
Tradução: Eduardo Kraszczuk
Revisão gramatical: Alessandro Thomé/Giacomo Leone Neto
Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-300-0

Histórico de impressões:

Junho/2012 Primeira edição

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Fax: +55 11 2950-8869
E-mail: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec

**Dados Internacionais de Catalogação na Publicação (CIP)**
**(Câmara Brasileira do Livro, SP, Brasil)**

Mutch, John
Gerenciando privilégios em tecnologia da informação : implementando a política de privilégio mínimo / John Mutch e Brian Anderson ; [tradução Eduardo Kraszczuk]. -- São Paulo : Novatec Editora ; NEW York, EUA : Apress Inc, 2012.

Título original: Preventing good people from doing bad things : implementing least privilege.
ISBN 978-85-7522-300-0

1. Computadores - Medidas de segurança 2. Hackers 3. Proteção de dados 4. Redes de computadores - Medidas de segurança I. Anderson, Brian. II. Título.

12-07155 CDD-005.8

Índices para catálogo sistemático:

1. Dados : Segurança : Computadores 005.8
2. Segurança de dados : Computadores 005.8

CAPÍTULO 1

# A única constante em TI é a mudança

*"A única constante é a mudança, mudança contínua, mudança inevitável, que é o fator dominante da sociedade atual. Não se pode mais tomar nenhuma decisão sensata sem levar em conta não só o mundo como ele é, mas o mundo como ele será."*

– Isaac Asimov, autor e professor

As melhores práticas na segurança de TI corporativa devem reconhecer a intersecção entre tecnologia, processos e pessoas. Ainda assim, muitas vezes o foco se direciona à tecnologia e aos processos, enquanto parte da equação sobre as pessoas é ignorada.

Não que as empresas nunca tenham reconhecido os melhores softwares de segurança ou desenvolvido políticas robustas o bastante para executá-los, só que elas muitas vezes ignoraram o elo mais fraco da sua implementação: a natureza humana. Isso é especialmente verdade quando se tratam de contas privilegiadas em servidores físicos e virtuais, desktops e ambientes de nuvem.

Vamos cobrir extensivamente as implicações do mau uso desse privilégio no próximo capítulo, mas uma coisa que precisamos reconhecer primeiro é a elusividade da natureza humana e as implicações da única constante verdadeira de negócios, que tudo pode mudar, e geralmente o faz.

- Por que parece que sempre que um buraco na segurança é fechado, outro aparece?
- Por que algumas auditorias (e auditores) permitem algumas práticas, tecnologias e políticas, e outras não?
- Por que parece que a maioria dos executivos sofre de desordem bipolar (por exemplo, esperando segurança estrita na época da auditoria, mas exige cumprimento mais relaxado em outras épocas para maior produtividade)?

## Ameaças internas *versus* externas

As políticas de segurança são a primeira linha de defesa de um ambiente de TI. Sem elas um empreendimento poderia entrar em guerra facilmente. Não só haveria batalhas entre as diferentes organizações de suporte, mas os administradores também se veriam lutando contra hackers (interna ou externamente). Não haveria políticas quanto ao mau uso de privilégios – somente um desejo brutal de modificar, roubar ou destruir dados acidentalmente.

Dessa forma, outra mudança significativa que as organizações enfrentam hoje é a natureza das ameaças à segurança da informação. Foram-se os dias em que a única preocupação era manter os bandidos do lado de fora dos nossos firewalls e as ameaças externas eram a principal preocupação. Naqueles dias a segurança de TI era voltada quase que exclusivamente a proteger os ativos de informação da empresa contra qualquer forma de ameaça externa. Esse panorama mudou significativamente desde então. Hoje as pesquisas mostram que cumprimento de padrões e continuidade dos negócios são os principais motivadores da segurança de TI, e o foco mudou para o como lidar com o potencial de uma quebra interna de segurança. A figura 1.1 demonstra essa tendência.


*Figura 1.1 – Principais motivadores para gastos com segurança de TI.*

Os executivos muitas vezes delegam a responsabilidade pela segurança para os administradores de sistemas sem fornecer recursos adequados para estabelecer os controles de autorização necessários para proteger e manter acessos de privilégios. Por causa disso, uma classe de soluções chamada Administração de Identidade Privilegiada (Privileged Identity Management – PIM) emergiu para ampliar o paradigma da Administração de Identidade e Acesso (Identity and Acess Management – IAM).

## Desmistificando a gerência de identidade privilegiada

Informações do governo dos EUA e do setor privado, um dia inacessíveis ou requerendo anos de preparação tecnológica ou de ativos humanos para serem obtidas, podem agora ser acessadas, inventariadas, perdidas ou roubadas com relativa facilidade, por acidente ou deliberadamente, usando ferramentas sofisticadas de ataque de identidade.

Em um esforço para melhorar a segurança dos negócios, cumprimento de padrões e produtividade, as políticas de autorização de privilégios devem ser reelaboradas, e as permissões de usuários, administradas de modo mais granular. Ainda assim, as soluções de IAM continuam praticamente sem mudanças. As soluções tradicionais respondem por parte significante do custo total do IAM, uma quantia surpreendente quando você considera que essas soluções:

- Não permitem que os usuários de desktop façam seu trabalho com eficiência como usuário padrão (80% dos funcionários acessam a rede com permissões de administrador).
- Não controlam o acesso de superusuários a servidores críticos, dando aos usuários acesso completo e não verificado (98% de todas as quebras de segurança acontecem a partir dos servidores).
- Forçam as organizações a escolher entre produtividade e segurança quando implementando uma solução PIM.

Embora esses desafios possam ter sido historicamente aceitáveis, eles não são mais bons o suficiente em um mundo extremamente complexo e colaborativo, onde o WikiLeaks mostra que os assuntos de qualquer um se tornam assuntos de todos em poucos segundos.

Aqui está o primeiro insight sobre a natureza humana. Quando as pessoas acham que ninguém vai pegá-las, ou que os limites entre legal e ilegal são imprecisos o suficiente, muitos vão optar por fazer o que querem e ignorar as consequências até que sejam forçados a isso. Uma situação similar são furos nas leis sobre impostos – toda vez que alguém descobre um, ele é abusado em massa, até que os legisladores o corrijam.

Foram atribuídos custos específicos a esses abusos que iremos cobrir em detalhes no Capítulo 10, mas é suficiente dizer que esses custos podem variar de US$ 120/desktop/ano a mais de US$ 2 milhões por incidente de servidor. Esses custos não são triviais por nenhuma definição para organizações de qualquer tamanho, e podem estabelecer esta como uma área que precisa ser

endereçada imediatamente, ao contrário de uma área que pode ser endereçada quando o tempo e os recursos permitirem.

É hora de os negócios esperarem mais das suas soluções PIM a fim de melhorar a segurança, o cumprimento de padrões e a produtividade geral, o que é esboçado na figura 1.2.


*Figura 1.2 – Causas de ameaças internas VS. externas.*

## Identidade privilegiada

Definição: qualquer tipo de usuário ou conta que possui permissões extras ou especiais nos sistemas da empresa. Também chamado superusuário. O que é um superusuário e por que eu deveria me importar?

As identidades privilegiadas são geralmente categorizadas nos seguintes tipos:

1. **Contas administrativas genéricas/compartilhadas**: as contas não pessoais que existem virtualmente em todos os dispositivos ou aplicativos de software. Essas contas possuem privilégios de "superusuário" e são muitas vezes compartilhadas entre os membros da equipe de TI (por exemplo, usuário administrativo do Windows, usuário raiz do Unix, ou conta SYS do Oracle).
2. **Contas pessoais privilegiadas**: as contas poderosas usadas pelos usuários de negócios e pela equipe de TI. Essas contas têm alto grau de privilégios, e seu uso (ou mau uso) pode afetar significativamente o negócio da organização (por exemplo, usuário CFO, usuário DBA).

3. **Contas de aplicativos**: as contas usadas pelos aplicativos para acessar bancos de dados e outros aplicativos. Essas contas tipicamente têm acesso amplo a informações de negócios nos bancos de dados.
4. **Contas emergenciais**: contas genéricas especiais usadas pela empresa quando são necessários privilégios elevados para solucionar problemas urgentes, como em casos de continuidade dos negócios ou recuperação de desastres. O acesso a essas contas frequentemente requer aprovação da gerência (por exemplo, IDs fire-call, usuários break-glass etc.).

As identidades privilegiadas envolvem virtualmente todos os setores comerciais. Isso porque cada empresa tem um componente crítico no ciberespaço que é acessível pelos usuários finais, aplicativos, dispositivos e pelas contas dentro desse complexo ecossistema colaborativo.

## A era da autorização

A tecnologia é um aspecto sempre em mutação e evolução nos negócios modernos. O uso da tecnologia é essencial para alcançar muitos dos pontos críticos da reforma de um negócio. A IAM governa três áreas significativas, garantindo a segurança correta de identidades: acesso, autenticação e autorização.

- As soluções de acesso respondem à pergunta: "*Posso entrar?*".
- As soluções de autenticação respondem à pergunta: "*Você é quem diz ser?*".
- As soluções de autorização respondem à pergunta: "*O que você pode fazer depois de entrar?*".

## Acesso

Inclui o processo de fornecer centralmente credenciais baseadas na função e limitadas no tempo para acesso privilegiado a ativos de TI a fim de facilitar as tarefas administrativas. Acesso Privilegiado de Superusuário (Super User Privileged Access – SUPM) e Administração de Senha de Conta Compartilhada (Share Account Password Management – SAPM) são dois pontos focais para o controle correto de acessos.

## SUPM & SAPM

Os analistas industriais classificaram esse espaço em SUPM e SAPM. Quando se trata de derrubar seus sistemas corporativos, destruir dados, apagar ou criar contas e mudar senhas, não é só com os hackers maliciosos que você precisa se preocupar. Qualquer um com acesso de superusuário dentro da sua organização tem o potencial de causar danos similares, seja pelo mau uso acidental, intencional ou indireto de privilégios.

Os superusuários podem ter acesso a informações confidenciais e dados pessoais sensíveis cujos os quais não têm razão nenhuma para ver, quebrando assim os requerimentos regulatórios e se arriscando a ser multados. O problema é que contas com privilégios de superusuário, incluindo contas compartilhadas, são necessárias: você não pode administrar um sistema de TI corporativo sem dar a algumas pessoas os privilégios para realizar tarefas no nível do sistema.

## Quem tem as chaves para a sua empresa?

É aqui que as metodologias SUPM e SAPM entram em cena. Então, qual é o melhor meio de gerenciar contas pessoais e compartilhadas com privilégios de superusuário de modo controlável e auditável? Essa é uma questão-chave que o diretor de pesquisas Perry Carpenter levantou no Gartner Information Security Summit de 2010. Quando se tratam das melhores práticas para gerenciar contas com privilégios de superusuário, Carpenter recomendou criar três tipos de contas:

- Contas pessoais com privilégios de superusuário completos e permanentes.
- Contas pessoais com privilégios de superusuário completos (ou restritos) e temporários.
- Contas pessoais com privilégios de superusuário limitados e temporários.

Carpenter enfatizou que a "atividade de superusuário em qualquer uma dessas contas deve ser monitorada, registrada e reconciliada". Os primeiros dois tipos são voltados para administradores de sistema em tempo integral, e a quantidade dessas contas deve ser minimizada.

"Entretanto, existe um equilíbrio entre ter essas contas em excesso e tê-las em pouca quantidade; e é importante não fazê-las em quantidade muito pequena."

Carpenter avisou que "de outro modo, pode não haver pessoas suficientes num dado momento para tornar uma ação necessária quando é preciso. Também é prudente considerar limitar o escopo dos privilégios do superusuário na infraestrutura da organização perguntando a si mesmo: "um dado administrador precisa ser um superusuário em todos os sistemas da organização?".

"O terceiro tipo de conta, aquele com privilégios limitados e temporários de superusuário, é voltado para desenvolvedores de aplicativos e administradores de bancos de dados. Os privilégios de superusuário dessas contas devem ser limitados aos aplicativos ou outras áreas onde é razoável que eles tenham acesso." Carpenter recomendou usar ferramentas SUPM para controlar esses três tipos de conta:

- Por privilégio (por exemplo, regulando os comandos disponíveis).
- Por escopo (talvez por recursos ou sistemas).
- Por tempo (seja fornecendo privilégios por um período fixo ou por janelas de tempo).

Carpenter também observou que usar ferramentas SAPM permite a uma organização controlar contas:

- Por privilégio (por exemplo, regulando os comandos disponíveis).
- Por fatores de forma (checksum, código de licença, endereço IP).
- Por escopo (talvez por recursos ou sistemas).
- Por tempo (seja fornecendo privilégios por um período fixo ou por janelas de tempo).

## Autenticação

Autenticação é o processo de determinar se alguém ou alguma coisa é, de fato, quem ou o que declarou ser. Em redes de computadores privadas ou públicas (incluindo a internet), a autenticação é comumente feita pelo uso de senhas de acesso. Assume-se que o conhecimento da senha garanta que o usuário seja autêntico.

Cada usuário inicialmente se registra (ou é registrado por alguém) usando uma senha designada ou selecionada. Em cada uso subsequente, o usuário deve conhecer e usar a senha declarada antes. O problema desse sistema para transações significativas (como a troca de dinheiro) é que senhas podem ser roubadas,

reveladas por acidente ou esquecidas. Por esse motivo, negócios na internet e muitas outras transações requerem um processo de autenticação mais rigoroso.

## Autorização

A administração de autorizações é um pilar importante na segurança de identidades, principalmente devido ao fato de que as indústrias estão se movendo de registros em papel para registros eletrônicos. Autorização é o processo de dar a alguém permissão para realizar certas tarefas ou obter certas informações.

Mais formalmente, "autorizar" é definir políticas de permissão. Por exemplo, a equipe de recursos humanos normalmente tem autorização para acessar registros de funcionários, e essa política é geralmente formalizada como regras de corretagem de permissões em um sistema de computadores. Durante a operação, o sistema usa as regras de corretagem de permissões para decidir se as requisições de permissão de usuários (autenticados) devem ser aceitas ou rejeitadas. Os recursos incluem um arquivo, tarefa ou dados individuais.

## Quebras internas de segurança nas notícias

Todos nós sabemos que o ditado popular "a curiosidade matou o gato" nos avisa para não sermos muito curiosos, pois isso resulta em problemas imprevistos, e ainda assim poucos conhecem a segunda parte dessa frase, "a satisfação dela o devolveu", que significa que, se estivermos satisfeitos, não vamos bisbilhotar por aí, para começo de conversa.

Infelizmente não se pode dizer isso sobre três funcionários do University of Iowa Hospitals and Clinics, que foram demitidos após uma investigação no hospital descobrir que eles violaram os registros médicos de jogadores de futebol americano de Iowa; ou sobre os quatro funcionários que foram demitidos do University Medical Center, em Tucson, por acessar registros médicos confidenciais das vítimas do trágico tiroteio envolvendo a representante Gabrielle Giffords (D-Ariz).

Embora nenhuma instituição tenha declarado um motivo oficial, parece provável que nos dois casos haja sido apenas simples curiosidade. Mesmo quando a política diz "não toque", o que as duas instituições claramente fizeram as pessoas às vezes não podem evitar, especialmente no caso de dois conjuntos de pacientes famosos.

Basicamente, enquanto nossa atenção deve estar nos empregados com objetivos mais nefários, as violações de dados também podem acontecer quando as pessoas não conseguem evitar dar uma espiada onde não deveriam.

De qualquer modo, a solução é a mesma:

- As empresas não precisam demitir funcionários que de outros modos (exceto pela tendência humana de bisbilhotar) podem ser bons funcionários. Tudo o que eles precisam fazer é limitar seu acesso por meio da implementação de uma solução de administração de privilégios mínimos. Privilégio mínimo é simplesmente dar somente a autorização (privilégio) aos recursos de TI compatíveis com a função e responsabilidade de um indivíduo, e não super ou subautorizá-los.
- Como iremos reiterar muitas vezes, as organizações não podem confiar na competência das pessoas, ou na sua "santidade", todo o tempo. Não somos perfeitamente consistentes nos nossos princípios pessoais ou profissionais. Limites claros são tudo o que é necessário para colocar a curiosidade firmemente de volta no seu lugar.

Lendo nas entrelinhas dos exemplos do University of Iowa Hospitals e do Tucson University Medical Centers citados antes, você pode ver que, mesmo quando alguém tem acesso, autenticação e autorização, esse alguém ainda pode fazer coisas ruins. A natureza humana é o elo mais fraco na interface entre pessoas, processos e tecnologia, e de fato *os caprichos da natureza humana são o motivador supremo da mudança como a única constante*.

## Contas privilegiadas são universais e problemáticas

Se alguém estiver andando pela sua organização com uma camiseta dizendo "Ajoelhe-se perante mim, pois eu sou raiz", então você terá um grande problema nas mãos quando os auditores vierem ou se um hacker decidir visar à sua empresa para roubo ou cibersabotagem.

*Quão universais são as contas privilegiadas na sua organização?* Comece simplesmente com uma auditoria de autorizações. Peça ao seu departamento de TI, ou fornecedor terceirizado, que gere um relatório do status de acesso de cada usuário (por exemplo, credenciais de autorização) por meio dos servidores, desktops, dispositivos de rede, servidores virtuais e aplicativos de nuvem. Uma vez que você tenha isso, simplesmente some quantas vezes você vê "raiz", "superusuário", "administrador", "su", "suid" ou qualquer outra credencial

com privilégios de superusuário/administrador. Se sua organização for como a maioria das outras, você irá descobrir que existe pelo menos uma conta compartilhada entre administradores de TI para cada servidor e dispositivo de rede. Você pode também descobrir que existe um administrador para cada cinco a dez servidores com esse nível de privilégio. Se você usar o MS Windows na configuração padrão, então cada usuário de desktop terá também acesso de nível de administrador ao seu computador desktop ou laptop. É isso mesmo. Cada desktop Windows vem com o usuário configurado para acesso de nível administrativo por padrão, a menos que alguém o configure na entrega a fim de que o usuário seja um "usuário padrão" ou "Admin. Protegido".

Isso é universal!

*Quão problemáticas são as contas privilegiadas na sua organização?* Simplesmente pergunte a qualquer hacker qual seu alvo número 1 para uma tentativa de infiltração. A resposta será "colher credenciais administrativas para acesso direto ao recurso desejado". A *Forbes.com* publicou uma história em dezembro de 2010 sobre dois estudantes da University of Central Missouri que invadiram os computadores da universidade não só com o intento de aumentar suas notas, mas também para "entrar nas contas da universidade e coletar informações sobre os professores, funcionários e alunos para vender suas identidades a compradores interessados".

*Então como você protege contas privilegiadas na sua organização?* A resposta simples é eliminar todos os direitos administrativos em todos os servidores, desktops, dispositivos de rede, servidores virtuais e ambientes de nuvem.

## As pessoas precisam de limites, não de muros

Vamos encarar: As organizações não podem mais simplesmente construir muros para proteger informações vitais. Entretanto, com o processo de se adaptar ao novo ambiente colaborativo vem o enorme desafio de garantir que o acesso privilegiado a informações críticas não seja mal usado. Os muros que podem ter funcionado uma década atrás são hoje praticamente irrelevantes, já que os usuários procuram caminhos ao redor, por cima ou por baixo dessas obstruções porque elas interferem em suas tarefas principais. Conforme prosseguimos nesta era em evolução, é importante desenvolver o conhecimento sobre como proteger nossos recursos, sejam eles quais forem, usando limites para nos guiar, e não muros.

Reconheça que as empresas hoje são principalmente ecossistemas de informações, pontos dinâmicos e fluidos de troca de informações, e não um silo de informações a ser protegido como um castelo da Idade Média. Podemos então observar a metáfora "limites *versus* muros" pelo que ela é:

- **Muros**: são construídos para manter as coisas do lado de dentro ou de fora de um perímetro específico. Em termos de segurança da informação, isso quer dizer estabelecer fronteiras eletrônicas ao redor dos recursos de TI de modo que somente pessoas selecionadas possam acessá-los.
- **Limites**: são construídos para guiar as coisas ao longo de um caminho específico para garantir o uso correto de um perímetro específico. Em termos de segurança da informação, isso quer dizer estabelecer as autorizações eletrônicas de modo que pessoas específicas possam fazer coisas específicas sob circunstâncias específicas.

Ter uma ideia bem definida dos limites permite aos usuários e aplicativos finais se comunicarem livremente dentro de um ambiente de TI sem se preocuparem com o mau uso intencional, acidental ou indireto de privilégios. Os limites permitem que um diálogo mais produtivo e de acordo com as normas ocorra ente os usuários e o departamento de TI e detêm proativamente as tentativas de mau uso. Se os limites forem respeitados, então o TI permanece no controle da segurança, da conformidade e da produtividade, e tem a autoridade de tomar ações proativas para proteger a empresa. A figura 3.1 demonstra esse ponto.

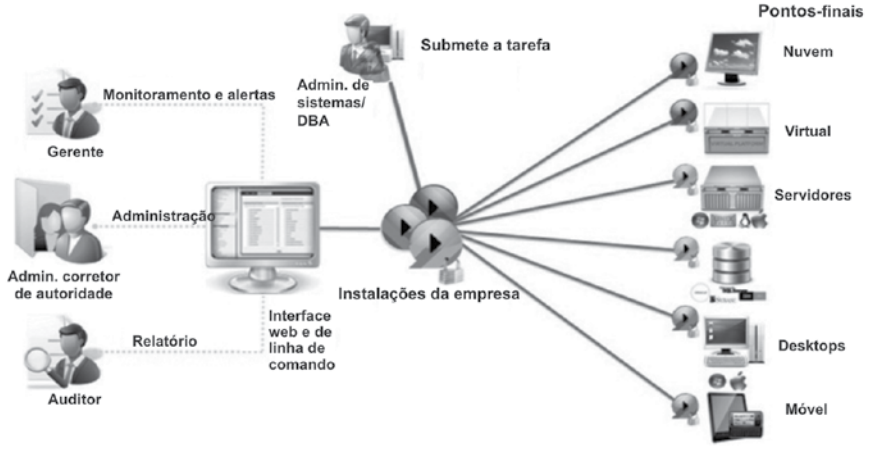


*Figura 1.3 – O privilégio mínimo nos dá limites, não muros.*

## Dez razões principais para se preocupar com quem tem acesso privilegiado à sua TI

Assumindo uma abordagem mais irreverente para destacar os tipos de acesso privilegiado que ocorrem diariamente na maioria das organizações, achamos que uma lista "das dez mais" seria mais atraente para você também. Quantas dessas você já viu na sua organização?

> #10: Michelle, a executiva administrativa do CEO, não é capaz de vender o acesso eletrônico aos segredos da empresa para Julian Assange para seu novo contrato de livro sobre o WikiLeaks.
>
> #9: Sam, o CSO, pode agora dormir à noite sabendo que o excesso de privilégios não será mais responsável por um fracasso nas auditorias SOX, HIPAA, PCI, DSS, GLBA ou FDCC (mesmo ele não tendo que lidar com os dois últimos).
>
> #8: Ted, do suporte técnico, não é capaz de resetar permissões de arquivo e diretório em nenhum servidor Linux a que ele tem acesso de administrador com tamanha facilidade, que qualquer um com um login pode acessar dados confidenciais, só porque isso facilita seu trabalho.
>
> #7: Sid, do desenvolvimento, não é capaz de fazer o download de aplicativos Apache ou de quaisquer "ferramentas" open source não autorizadas que possam potencialmente injetar malware na nossa rede corporativa.
>
> #6: Fiona, a assistente-administrativa, não pode prejudicar a configuração do seu PC quando tentar atualizar um aplicativo e digitar por acidente o endereço IP errado.
>
> #5: Bob, o VP de marketing, não vai sobrecarregar os backups noturnos por carregar 120GB de música do seu iTunes para o laptop corporativo.
>
> #4: Alice, do TI, não vai mais ser responsável por erros de má configuração de DNS, uma vez que sua função não irá facilitar esse nível de privilégio administrativo.
>
> #3: Fred, do TI, não será capaz de instalar um Cavalo de Troia no servidor crítico, derrubando-o por quatro horas e custando à empresa mais de US$1 milhão em transações perdidas porque foi preterido para uma grande promoção.
>
> #2: Sarah, a CIO, não terá mais que ocultar credenciais de raiz Linux em um envelope selado no cofre do seu escritório e lidar com um processo manual de check in/check out.
>
> #1: Tony, o administrador de sistemas de Palo Alto, não poderá mais vestir aquela camiseta velha com o slogan "Ajoelhe-se perante mim, pois eu sou raiz".

## Regulamentações federais para privilégios mínimos

A PIM é crítica para sistemas de negócios e, se não for administrada de modo correto, pode introduzir riscos significativos de cumprimento de padrões. Autorizações privilegiadas são críticas para a administração contínua dos ativos de TI e, se o risco de ameaças internas ainda não estiver claro o suficiente, podem exacerbar uma situação potencialmente arriscada. Ao mesmo tempo, elas expõem uma organização a riscos de segurança, em especial ameaças internas.

Em 16 de maio de 2011, a Casa Branca divulgou uma nova legislação instruindo a indústria privada a melhorar voluntariamente a segurança dos seus computadores e ter esses padrões revisados pelo Departamento de Segurança Interna (Department of Homeland Security – DHS). Aumentando e esclarecendo as penalidades para crimes por computador, federais e corporativos, a administração espera combater a percepção de que as consequências a ciberataques e a roubos de dados são relativamente triviais.

Oficiais da administração admitem que eles irão designar certos sistemas privados de computador como parte da "infraestrutura crítica" sobre a qual o DHS terá maior autoridade. A agência irá também receber a tarefa de trabalhar com as companhias de energia e água e instituições financeiras para classificar e combater as ameaças mais sérias. A nova lei vai requerer, inclusive, que essas empresas trabalhem com auditores comerciais independentes a fim de avaliar seus planos e, no caso das empresas financeiras, reportar esses planos para a Comissão de Segurança e Câmbio (Security and Exchange Commission). A lei também inclui a simplificação e padronização das 47 leis estaduais existentes sobre quebra de segurança de dados, que requerem que as empresas vítimas de invasão informem aos consumidores se o intruso teve acesso aos dados pessoais dos clientes.

O resultado: muitas empresas irão, de imediato, incluir orçamentos e mão de obra adicionais para a tarefa de fazer barricadas contra ameaças externas. Mas esquecendo-se de que essas novas leis ordenam igualmente o monitoramento e a auditoria de comprometimentos internos.

Mas, além de barricadas contra o exterior, as organizações irão precisar endereçar controles internos de acesso, direitos administrativos dos funcionários do TI e soluções de delegação de privilégios do usuário. Os administradores deverão examinar como os ativos de dados são acessados internamente (e por quem), monitorar mudanças para os controles de aplicação que sejam seguros e protejam a integridade dos ativos, e até avaliar proativamente o impacto das mudanças da TI para o negócio e segurança de TI.

O papel crítico da segurança de TI é "proteger o perímetro interno". Aconselhamos veementemente que as empresas olhem para dentro de si mesmas – assim como para fora – a fim de fortalecer a segurança ao redor dos ativos de dados por meio do melhor controle da administração da base de dados de usuários e atividades, permitindo aos usuários de desktop operar usando o conjunto mínimo de privilégios necessários para completar suas funções.

Também não podemos confiar no cumprimento de padrões para nada mais do que estabelecer o limite mínimo para nossas medidas de segurança. Estamos de volta à difícil análise da escolha do impacto real da segurança sobre a produtividade *versus* seus benefícios. E, embora não exista uma resposta simples sobre como fazer essa análise, pode haver um modo diferente de definir o problema. Por exemplo, a BGC Partners adotou uma solução de privilégios mínimos para aplicar a segurança e o cumprimento de padrões de privilégios mínimos na sua rede global, compreendendo seis mil desktops em 20 escritórios por todo o mundo, atendendo mais de 1,4 mil corretores e aproximadamente 2,4 mil funcionários.

"Nosso ambiente atual permite aos usuários privilégios administrativos completos nos seus PCs, e nós limitamos o controle sobre o que o usuário final pode instalar e mudar em um desktop", disse Paulo Pina, gerente global de serviços de desktop da BGC Partners. "Nós limitamos o conhecimento das mudanças sendo promovidas, e na maioria das vezes já é tarde demais se um usuário instala malware e adware, obrigando nossa equipe a ter de apagar incêndios."

"Como gerente global de serviços de desktop na BGC, [nossa solução de privilégios mínimos], tenho a garantia de que meu ambiente está mais protegido contra softwares indesejados, enquanto posso controlar proativamente quais aplicativos ou processos os usuários poderão acessar – sem dar a eles direitos administrativos completos (e os problemas que surgem com esse acesso) –, sem prejudicar seu trabalho diário", Pina acrescentou.

A falta de acesso controlado a recursos críticos de TI traz riscos de segurança devido ao mau uso intencional, acidental ou indireto desses privilégios, enquanto também torna difícil cumprir os objetivos de atendimento de padrões.

Pina disse: "[Nossa solução de privilégios mínimos] permite que sejam feitas mudanças em um sistema ou política de aplicação rapidamente e sem esforço e, mais importante, se quisermos, nos permite configurar usuários para executar um aplicativo em 'modo logado', que irá nos notificar que um aplicativo ou processo de sistema está sendo usado e se precisamos verificar seus privilégios".

## O Yin e Yang da segurança

Às vezes, coisas aparentemente opostas podem de fato interagir de modos complementares. O conceito chinês de Yin-Yang é usado para descrever como forças aparentemente contrárias são interconectadas e interdependentes no mundo natural e como elas dão origem umas às outras. Então, existe um Yin e um Yang da segurança e produtividade? Você pode implementar a segurança de modos que melhorem a produtividade? Nós achamos que sim.

- *Primeiro minimize o impacto da segurança sobre a produtividade tornando-a o mais transparente possível para o usuário final. Idealmente, ele não deveria precisar passar por nenhum comando extra, nenhum pop-up ou nenhuma tela extra para operar com segurança. E, se a ação solicitada pelo usuário for permitida, simplesmente deixe acontecer*. O comando deslizante de controle de acesso do usuário do Windows é um bom exemplo. Se você der a opção para os usuários, eles vão reduzir o nível de segurança a fim de evitar ter de responder a um prompt adicional. Então, se você for lhes dar autoridade para realizar certas ações depois de um prompt, por que perturbá-los com os passos adicionais?
- *Segundo, embora os controles de segurança impeçam as pessoas de fazer coisas ruins, esses mesmos controles podem aplicar as melhores práticas. Além de controlar as ações por conta do risco de segurança, podemos impedir que as pessoas façam coisas que não deveriam em virtude do risco operacional apresentado*. E, com controles implementados corretamente, podemos fazer melhor do que usar pop-ups "Você realmente deseja...", nos quais nós clicamos de qualquer jeito. Controles projetados e implementados corretamente podem resultar em um modo desejado de utilizar as melhores práticas.
- *Finalmente, existe grande potencial no uso de dados sobre o que as pessoas estão fazendo para melhorar a produtividade*. Esses logs detalhados de cumprimento de regras são minas de ouro de informações. Você pode usá-los não só para procurar padrões que indicam uma ameaça à segurança, mas esses mesmos padrões podem mostrar onde a segurança e outros procedimentos, como configurações incorretas de novos sistemas, estão prejudicando a produtividade. Encontrar esses padrões ajuda a descobrir oportunidades para melhores treinamentos, simplificar procedimentos e descobrir as melhores práticas que nem todos estão seguindo. Uma vez que essas melhores práticas são descobertas, você pode usar controles para garantir que sejam seguidas.

## O que esperar a seguir

As seções a seguir examinarão rapidamente os capítulos restantes do livro e darão a você uma ideia sobre o que será tratado em cada um. O livro foi elaborado para ser lido de modo contínuo, mas cada capítulo foi escrito independentemente, visando àqueles que preferem acessar apenas os pontos em que estão mais interessados.

## Examinando o pessoal interno: os vilões

O capítulo 2 é dedicado aos vilões anônimos das empresas. Entre os suspeitos de costume que iremos examinar, temos:

- **Dave Descontente**: Dave foi, um dia, uma pessoa de confiança, com acesso privilegiado a toda a infraestrutura de TI, mas as circunstâncias mudaram de tal modo que ele hoje está infeliz com seu *status quo*, a ponto de ele estar causando danos intencionalmente, como roubar, modificar ou apagar dados e/ou plantar malware.
- **Annie Acidental**: Annie é uma usuária corporativa típica que pode estar acidentalmente usando seus privilégios para fazer coisas contrárias à política corporativa (como o download de softwares da web ou atualizando aplicativos antes da aprovação do TI) e causando pânico no help desk.
- **Irene Ladra de Identidade**: Irene é a pior de todos. Ela é uma pessoa de fora que roubou as credenciais de um interno confiável com muitos privilégios e usa essas credenciais para roubar, modificar ou apagar dados e/ou plantar malware.

## Examinando o pessoal interno: os heróis

O capítulo 3 é dedicado aos heróis anônimos das empresas. Entre os suspeitos de costume que iremos examinar, temos:

- **Sam Seguro**: Sam é um CSO ou gerente de TI típico, responsável pela administração e pelo cumprimento de normas de segurança dos ativos da sua corporação.

- **Lucy Privilégios Mínimos**: Lucy é uma administradora de rede ou sistemas média, responsável por administrar sistemas e/ou infraestrutura, sejam estes sistemas físicos, virtuais ou baseados na nuvem.
- **Carl Cumprimento**: Carl é um auditor clássico, responsável pelo cumprimento das regulamentações e pela auditoria das políticas de TI para a aplicação do controle corporativo.

## Examinando os requerimentos da infraestrutura de TI

Os capítulos 4 a 8 são dedicados a examinar os requerimentos únicos das plataformas físicas e virtuais, os aplicativos e os ambientes de computação em nuvem (*cloud computing*). As plataformas tecnológicas que vamos examinar incluem:

- **Desktops**: um desktop não é uma máquina que precisa mais estar em um local fixo. Com a tecnologia atual, esse termo é sinônimo de uma pessoa (seja quem for) que tem acesso e está usando o Microsoft Windows. Sabe-se que as pessoas se comportam de modo diferente dentro e fora do escritório, onde a cultura é diferente. As linhas entre a vida pessoal e profissional se tornaram imprecisas, e as pessoas tiram os ternos em casa, colocam shorts e fazem o login, mas isso não quer dizer que eles devam também tirar o chapéu corporativo. Mas qual é a resposta? Eliminar direitos administrativos sem permitir a elevação de certos privilégios necessários para o trabalho não é a resposta. Trancar um sistema é como pedir a todos que levantem as mãos para ir ao banheiro. Isso mostra o lado negativo de desconfiar da natureza humana. Confiança não é um valor que possa ser aplicado em doses fixas: ela deve ser medida para atender às necessidades da função do indivíduo.
- **Servidores**: servidores são a espinha dorsal de todos os ambientes computacionais corporativos. Eles são os músculos que mantêm as transações críticas à missão, o local de armazenamento de todos os ativos de informação públicos e privados e a fundação que promove a produtividade do usuário. Eles podem ser de um simples servidor de impressora Linux até uma máquina Unix com multiprocessadores simétricos executando milhões de transações por minuto em terabytes de informação. Por causa disso, eles são o maior alvo de ataques internos e externos, mas é a pessoa de dentro que sabe explicitamente onde eles estão e como acessá-los.

- **Ambientes virtuais**: proteger ambientes virtuais é uma tarefa difícil e tediosa. Por um lado, os privilégios nesse ambiente devem ser gerenciados granularmente para garantir completa segurança. Por outro lado, leva menos tempo e energia permitir aos usuários operar com privilégios totalmente livres em ambientes de datacenters virtualizados. Felizmente há uma resposta para essa questão, fazendo com que os riscos nesse ambiente sejam mitigados.
- **Nuvens privadas, públicas e híbridas**: operar na nuvem é a mais nova tendência no mundo tecnológico. Seja em nuvens privadas, seja em públicas ou híbridas, é para onde estamos indo. Só porque as informações e os aplicativos estão disponíveis de modo tão conveniente não quer dizer que os limites devem ser baixados para tornar tudo conveniente. O princípio do privilégio mínimo se aplica aqui mais do que nunca.
- **Aplicativos, bancos de dados e dados em desktop**: Apps legado são necessários para a operação de empresas em todos os lugares, mas os privilégios para executá-los deixam grandes furos na segurança das empresas. A resposta, obviamente, é não eliminar esses privilégios, mas permitir aos usuários executá-los com base no que é necessário para suas funções. Isso tira a pressão sobre os administradores de TI que acham que a única saída é atualizar ou pagar por um patch produzido internamente. Os privilégios mínimos são, na verdade, o casamento entre segurança e produtividade nesse caso.

## Examinando os requerimentos de governança e de cumprimento de normas

O capítulo 9 é dedicado a examinar as questões governamentais e regulatórias presentes nas empresas de hoje. As regulamentações específicas que iremos examinar incluem:

- **Regulamentações governamentais**: legislações que requerem maior autorização de privilégios, incluindo, mas não limitadas, SOX, HIPAA, GLBA, e PCI DSS. Os auditores estão cientes das políticas que devem ser aplicadas para atender às regulamentações federais, estatais e industriais. O não cumprimento dessas regulamentações pode resultar em multas, perdas financeiras severas, vazamento de dados e danos à reputação de uma empresa. Uma sólida segurança de autorizações ajuda os auditores a validar o cumprimento de normas da empresa. A detecção correta de autorizações e logs de fácil acesso à auditoria para rastreamento do uso de privilégio ajuda o auditor a realizar as complexas tarefas da sua posição.

- **Controle corporativo**: a gerência contínua do acesso, do controle, do monitoramento e da correção de todas as infraestruturas de TI é a própria definição de boa governança. Sem um controle rígido e sempre vigilante desses aspectos da aplicação da política, nenhum indivíduo ou empresa pode esperar satisfazer à miríade de regulamentações impostas a eles.

## Examinando os custos concretos e intangíveis da apatia

O capítulo 10 é dedicado a examinar os métodos para quantificação e qualificação de custos e potencial de retorno. As medições específicas que iremos examinar incluem:

- **Custos intangíveis**: para entender o custo da apatia com relação a vazamentos e privilégio mínimo, devemos primeiro entender que o modo como gerenciamos o risco tem impacto no comportamento humano. Se prendermos as pessoas removendo todos os seus privilégios, elas se sentirão sufocadas e provavelmente irão se rebelar ou se isolar. Se dermos a elas privilégios demais, as pessoas vão ter medo de estragar ou quebrar alguma coisa, ou vão tirar vantagem desses privilégios e abusar do sistema. A chave é dar-lhes o que precisam; elas vão se sentir seguras o suficiente para fazer bem seu trabalho.
- **Custos concretos**: além dos complicados custos intangíveis, você irá descobrir diversos custos concretos muito tangíveis, identificáveis e mensuráveis, associados ao mau uso de privilégios. Milhões de dólares foram gastos com brechas de segurança em servidores, e centenas de dólares com brechas de segurança em desktops. Multiplique isso pelo número de servidores e desktops no seu ambiente e você irá descobrir uma grande exposição financeira.

## Observações finais e examinando as melhores práticas

O capítulo 11 é dedicado a revisar as observações finais e as melhores práticas para mitigar as ameaças internas, impedindo que pessoas boas façam coisas ruins e protegendo o perímetro interno. Os pensamentos específicos que iremos examinar incluem:

- **Observações finais**: existem regulamentações para proteger as empresas de vazamentos de dados. Essas regulamentações exigem que sejam imple-

mentadas medidas de segurança, mas muitas empresas, infelizmente, não atendem a essa obrigação. Privilégio mínimo é a chave para ajudar as empresas a cumprirem as regulamentações baseadas em padrões da indústria.

- **Melhores práticas**: milhares de empresas já implementaram soluções de privilégios mínimos em alguma parte da sua infraestrutura de TI e estão estendendo-as para uma cobertura completa. Avaliando o que foi feito antes por essas empresas podemos descobrir melhores práticas para facilitar o processo.

## Trazendo as contribuições

Vamos fechar cada capítulo trazendo as contribuições dos nossos "Heróis internos". Vamos usar suas vozes para destacar os pontos específicos que você deve notar no capítulo específico baseado na visão deles sobre a situação.

Mudança é a realidade com que todas as organizações devem conviver diariamente e as práticas de segurança devem se adaptar a essas mudanças. Já se foram os dias em que os "bandidos" eram claramente alguém que não era um funcionário, empreiteiro ou parceiro de confiança que podia ter o acesso negado ao perímetro da sua infraestrutura de TI. Mesmo nos filmes de Hollywood os bandidos não são mais aqueles usando uma cartola preta e ostentando um bigode espalhafatoso. Eles se parecem, e de fato são, com as pessoas que se sentam do seu lado todos os dias. No ambiente atual da segurança, o foco mudou do acesso (Posso entrar?) e da autenticação (Você é quem diz ser?) para a autorização (O que você pode fazer depois que entrar?).

### Sam Seguro

Acabamos de mergulhar no modo como as pessoas e a natureza humana permanecem os mesmos no sempre mutável mundo da tecnologia de informação, e esse é um ponto fundamental, já que queremos entender os modos de compensar as consequências da mudança. Pessoas são criaturas voláteis e, muitas vezes, suas expectativas são tão inconsistentes quanto o valor líquido de um computador. Homens de negócios, por exemplo, são um bom exemplo disso. Eles esperam que a produtividade continue alta e, ao mesmo tempo, têm tolerância zero com falhas nas medidas de segurança. Auditorias devem ser passadas; mandatos federais, atendidos; mas as despesas devem permanecer

baixas, e a empresa deve permanecer funcionando de modo eficaz. Enquanto esses mandatos não são irrealistas do ponto de vista individual, esperar que todos juntos sejam atendidos, sem nenhuma folga, historicamente causa dores de cabeça para o departamento de TI de todas as empresas. Isso foi antes de o privilégio mínimo estar disponível. Com esse princípio, uma empresa pode ser segura, continuar produtiva, passar nas auditorias, atender aos mandatos e manter as despesas baixas – tudo ao mesmo tempo. Mudanças podem ser mitigadas, tanto financeira quanto estrategicamente, dando aos usuários apenas o menor número de direitos possível.

## Lucy Privilégios Mínimos

Não podemos enfatizar o suficiente o quanto a mudança é integral para a TI. Talvez tão central quanto os próprios computadores, a mudança é inerente à própria natureza da indústria. Ideias e práticas mudam e evoluem constantemente, e tal fenômeno gera aspectos positivos e negativos. Enquanto a tecnologia está avançando e melhorando, está também deixando as empresas expostas à ameaça crescente dos vazamentos de dados. É difícil permanecer no topo nesse ambiente mutável, e isso se deve em grande parte ao número de usuários requerendo direitos de administrador. Certos aplicativos precisam de privilégios administrativos, e esses aplicativos geralmente são necessários para as funções de trabalho. É uma história contada de novo e de novo: privilégios mínimos são a resposta. Mudanças irão ocorrer em todos os ambientes, mas, quando as organizações permitem aos usuários trabalhar apenas com os direitos que eles realmente precisam, essas mudanças se tornam gerenciáveis.

## Carl Cumprimento

Na verdade, a mudança é a única constante, e conforme o mundo da TI continua a evoluir ao nosso redor, devem ser feitos ajustes para garantir que certas coisas se tornem uma base estável nas nossas organizações. O princípio dos privilégios mínimos é um que fundamentalmente faz sentido; é o padrão dourado no qual podemos basear toda a nossa governança de TI. Usando esse conceito como ponto de referência, é possível ser consistente na determinação de que práticas, políticas e tecnologias são aceitáveis e legais – uma consistência que simplesmente não se pode atingir sem tal conceito. Os auditores não são mais capazes de "brincar de Deus" com as empresas e o modo como elas gerenciam seus dados sensíveis. Usando os privilégios mínimos como marco, eles racionalizam o que é aceitável e o que não é no mundo sempre mutável de TI.