

Guia Básico de Sobrevivência para uma Auditoria de Sistemas – Parte 1 de 2

Dez dicas úteis para manter o seu ambiente seguro e poder provar que isto é feito da forma adequada

Eduardo Vianna de Camargo Neves, CISSP

eduardo@camargoneves.com

Introdução

Durante seis anos trabalhei como *Security Officer* de uma multinacional, onde a área de *Information Services* era auditada ou tinha que fornecer informações e dados para auditores de outras áreas, em média, cinco vezes por ano. Ou seja, eu trabalhava inicialmente 45 dias por ano somente atendendo requisições de auditores e explicando como as coisas funcionavam dentro da empresa. Parece muito tempo para pouco retorno, porém o resultado de qualquer auditoria é o *Audit Report* que é discutido em um *Draft* e posteriormente apresentado em sua versão final durante o *Exit Meeting*.

Este documento tem uma grande força política dentro de qualquer organização que leve uma auditoria a sério, e pode causar desde um clima muito tenso dentro das áreas envolvidas até a demissão de um CIO. Ou seja, é necessário dedicar toda a atenção para o processo de auditoria, de forma a garantir que os resultados reflitam a realidade e possam ser discutidos com base em um entendimento comum de risco existente.

Neste artigo não vou entrar nas questões de discussão do *Audit Report* e o trabalho de gestão de riscos que deve fazer parte das atividades de um *Security Officer*, pois estes temas serão abordados na Parte 2. Apresento aqui dez dicas úteis sobre os itens mais comuns que são analisados por auditores de sistemas, e se não bem administrados continuamente, podem mostrar pequenas fragilidades de uma organização, que em conjunto, transformam-se em um grande problema.

As dicas são baseadas na apresentação “The Top 10 Security and Risk Audit Findings You Need to Avoid” feita pelo Gartner Group em um evento ocorrido em 2007, cujo material original infelizmente não está disponível para download. Usei um formato parecido com o apresentado que achei muito bom, incluindo minhas observações e comentários. Posteriormente, vou aprofundar cada uma das dicas em artigos seqüenciais, onde irei mostrar o que pode ser feito para administrar cada uma das recomendações.

Dica 1: Classificação de Ativos

O Ponto de Auditoria

Não existe um inventário de ativos (ex. Workstations e software) ou o mesmo está desatualizado. Com isso, a empresa não sabe o que tem e muito menos quais medidas de proteção devem ser aplicadas e administradas.

Por que é um problema?

Se abordarmos a parte de hardware, o mínimo que pode acontecer é um equipamento ser furtado e você notar isto somente quando for tarde demais para qualquer ação corretiva. Imagine agora que além deste equipamento ter sido furtado, os dados dentro dele não foram classificados e protegidos de forma adequada. Um [vazamento de informações sensíveis](#) pode acontecer, resultando em [desgaste da imagem](#) perante o público, e diversas [conseqüências legais](#) das partes afetadas.

Como Evitar?

Este é um processo trabalhoso que exige muita dedicação no começo e mais ainda em sua manutenção: classificação e gestão de informações. Deve existir um inventário de todos os equipamentos de TI utilizados pela Organização que mostre a pessoa responsável pela guarda do mesmo, as autorizações para uso de informação sensível, quais softwares estão instalados no equipamento e a licença para uso dos mesmos.

Este inventário deve ser constantemente atualizado, administrado por uma pessoa dedicada (dependendo, é claro, da quantidade de esforço envolvido) e utilizado como uma ferramenta de gestão por toda a equipe de TI. Na prática, o Help Desk tem um papel fundamental na manutenção deste controle, e os membros deste time devem estar muito bem treinados para não deixar passar nenhuma exceção.

Dica 2: Gestão de Mudanças

Ponto de Auditoria

Não existem evidências de que as mudanças feitas em aplicações ou itens da infra-estrutura são requisitadas, desenvolvidas, testadas e aprovadas formalmente.

Por que é um problema?

Qualquer mudança feita sem um mínimo de controle pode resultar em problemas que afetam toda a infra-estrutura de uma Organização. Um exemplo clássico é um [processo de patch management](#) feito de forma inadequada que para uma determinada aplicação de negócio que não estava preparada para funcionar com as mudanças que são implementadas no ambiente que a suporta.

Como Evitar?

Se a empresa não tem uma equipe de desenvolvimento, e faz um outsourcing destes processos, possivelmente não seja necessário ter as evidências disponíveis, mas no mínimo o contrato que rege esta relação comercial deve ter um *Service Level Agreement* (SLA) informando claramente como o processo é feito e as penalidades em caso de não cumprimento do acordo.

Se o desenvolvimento é feito internamente, devem ser mantidos três ambientes segregados; um de desenvolvimento, um de homologação (validação de mudanças) e outro de produção, onde os acessos de desenvolvedores e usuários devem ser diferenciados. E as movimentações e aprovações envolvidas no processo, devidamente registradas.

Dica 3: Compartilhamento de Contas Privilegiadas

Ponto de Auditoria

As contas de acesso privilegiado a um ou mais sistemas/aplicações (ex. admin, root) são compartilhadas entre mais de uma pessoa.

Por que é um problema?

O uso de contas com acesso privilegiado já é um risco. Como estas contas não têm limites dentro do sistema, um usuário mal intencionado (ou mesmo infectado com um vírus?) pode fazer um estrago sem igual dentro da infra-estrutura onde atua. Se forem compartilhadas, a probabilidade de conseguir rastrear a origem de um problema dessa natureza é reduzida significativamente.

Como Evitar?

Administrar uma infra-estrutura de TI sem uma conta privilegiada é um desafio que poucas empresas conseguem vencer, uma vez que exige o estabelecimento de uma política de segurança, o seguimento de procedimentos operacionais específicos e investimento em gente (na maioria das vezes, o que as empresas menos querem fazer ...).

Se isso for possível, excelente solução, se não, é recomendado que as contas administrativas sejam renomeadas e/ou tenham suas senhas alteradas logo após a instalação da aplicação em questão. Além disso, estas contas devem ser reduzidas ao mínimo possível, exigindo de qualquer pessoa que as queiram usar, uma excelente técnica que deve ser aprovada pelo Diretor de TI (ou equivalente).

Dica 3: Administração de Direitos

Ponto de Auditoria

Não é possível determinar quais são os acessos dos usuários dentro ao ambiente e/ou as autorizações para que as concessões fossem feitas.

Por que é um problema?

Sem saber que acessos um determinado usuário tem dentro de um ambiente, fica impossível definir se ele tem os privilégios adequados para a sua função ou se a segregação requerida para a atividade é adequada (ex. quem compra não pode autorizar um pagamento). Um caso recente, ainda sob investigação, que mostra até onde o excesso de privilégios pode levar é a fraude ocorrida no banco francês [Société Générale](#).

Como Evitar?

Existem ferramentas de administração de privilégios (*Identity Management*) que auxiliam na gestão destes controles de forma muito eficaz. Na falta de orçamento para a implementação de uma, as soluções que me parecem mais adequadas tem origem na relação da Equipe de Segurança da Informação (SI) com a área de Recursos Humanos (RH). Quando ocorre uma mudança de qualquer natureza no status (ex. empregado ou demitido), função (ex. analista para supervisor) ou área (ex. de Finanças para Controles internos) de um usuário, RH deve informar SI e os direitos anteriores “congelados” até que o supervisor referente aprove qualquer tipo de inclusão ou manutenção dos privilégios.

Dica 4: Monitoramento de Atividades

Ponto de Auditoria

Não é possível determinar quais são acessos foram feitos por quem, quando e para que em uma ou mais aplicações/sistemas considerados críticos e/ou sensíveis.

Por que é um problema?

O primeiro problema é o entendimento. Existem auditores que tem como regra classificar como um problema a impossibilidade de monitorar todas as atividades dentro de um ambiente informatizado. Isso além de ser um desperdício absurdo de dinheiro, não traz absolutamente nenhum benefício para a organização. Porém, quando falamos de aplicações/sistemas considerados críticos (ex. Folha de Pagamento), o conceito se aplica perfeitamente.

Se não existir o monitoramento das atividades, é impossível identificar os indícios de uma atividade maliciosa ou mesmo rastrear a origem de uma fraude. Este tipo de processo é muito comum em aplicações de grande porte que já tem relatórios prontos (ex. SAP), mas raras nas demais aplicações, que devem ser adaptadas para este propósito.

Como Evitar?

Existem ferramentas de administração de privilégios (*Identity Management*) que auxiliam na gestão destes controles de forma muito eficaz. Na falta de orçamento para a implementação de uma, as soluções que me parecem mais adequadas tem origem na relação da Equipe de Segurança da Informação (SI) com a área de Recursos Humanos (RH).

Quando ocorre uma mudança de qualquer natureza no status (ex. empregado ou demitido), função (ex. analista para supervisor) ou área (ex. de Finanças para Controles internos) de um usuário, RH deve informar SI e os direitos anteriores “congelados” até que o supervisor referente aprove qualquer tipo de inclusão ou manutenção dos privilégios.

Dica 6: Segregação de Funções

Ponto de Auditoria

As funções dos usuários dentro de uma aplicação ou sistema permitem que eles desenvolvam atividades complementares em processos críticos, possibilitando a existência de fraude.

Por que é um problema?

De forma similar a dica anterior, quando um usuário pode executar duas ou mais atividades complementares dentro de um processo de negócio considerado crítico (ex. finanças), por exemplo, ele pode requisitar uma transferência de valores entre duas contas e depois de completada a requisição, aprovar o processo.

Como Evitar?

Sempre aplicar a [segregação de funções](#) em processos que sejam considerados críticos pela empresa. Uma boa forma de fazer isto é desenvolver uma [matriz](#) onde estejam descritos todos os tipos de acesso e os usuários que os tenham, e revisar freqüentemente em conjunto com a área de Controles Internos.

Dica 7: Segurança Física

Ponto de Auditoria

Áreas que mantêm informações e/ou equipamentos que suportam atividades críticas da empresa não mantêm os controles de segurança físicos adequados (ex. detecção e combate a incêndios).

Por que é um problema?

A segurança física é um item constantemente subestimado pelas empresas, não só porque os equipamentos para mantê-la de forma adequada têm um custo substancial de compra, implantação e manutenção, mas também porque a probabilidade de ocorrência de problemas é baixa. Mas quando acontece, uma falha deste tipo pode ter um [impacto](#) realmente grande.

Como Evitar?

Escrevi um [documento](#) no ano passado que mostra boa parte dos controles de segurança física que são recomendados. Além disso, backup, cópias de arquivos importantes e replicação de dados são boas práticas que não aumentam a segurança física, mas reduzem o impacto no caso de ocorrência de um sinistro.

Dica 8: Planos de Continuidade e Recuperação de Desastres

Ponto de Auditoria

A empresa não tem Planos de Continuidade de Negócio (PCN) e Planos de Recuperação de Desastres (PRD), ou mantêm documentos desatualizados (o que é mais comum).

Por que é um problema?

O objetivo de um PCN é garantir que a empresa continue operando após a ocorrência de um impacto com a menor perda possível. Já um PRD, busca recuperar o que foi perdido em um espaço de tempo e com um custo que sejam adequados para a realidade do negócio em questão. Quando as informações que suportam estas estratégias não correspondem à realidade, o PCN e o PRD não passam de uma montanha de papéis inútil, que se forem seguidas em uma emergência, podem causar ainda mais impacto do que o próprio sinistro.

Como Evitar?

A primeira recomendação é entender as [diferenças entre os componentes](#) de uma estratégia de continuidade. Depois de ter claro o que é cada parte, definir o que deve ter uma contingência, escrever os planos e mantê-los atualizados sempre. Note que esta responsabilidade é de todas as áreas que usam e mantêm os componentes que devem ser contingenciados, e não restrita a área de Segurança da Informação ou TI.

Dica 9: Contratos de Outsourcing

Ponto de Auditoria

Os contratos de outsourcing que a empresa mantém com prestadores de serviços não contêm cláusulas de proteção para garantir a extensão dos controles de segurança aplicados dentro da empresa às informações e dados críticos quando estes são levados para um ambiente externo.

Por que é um problema?

Uma das características do mundo dos negócios é o foco no core business da empresa e um grande processo de outsourcing para todo o resto. Porém, os contratos que são assinados entre as partes devem contemplar a extensão da proteção existente na contratante para a contratada, ou todo o processo de segurança some quando os dados são movidos entre os ambientes.

Como Evitar?

No mínimo é necessário interagir com um advogado para ele ajudar na escrita de cláusulas de proteção da informação neste tipo de processo. Por outro lado, fazer uma análise de risco nas instalações do prestador de serviço pode ser mais difícil de ser negociado, mas normalmente resulta em um conjunto de boas práticas para ambas as partes.

Dica 10: Awareness

Ponto de Auditoria

Os usuários da empresa não passam por um processo formal de treinamento e awareness em Segurança da Informação.

Por que é um problema?

Diversas publicações e artigos definem que o elo mais fraco na corrente da Segurança da Informação é o usuário. O desconhecimento das políticas e controles utilizados pela empresa ou mesmo a falta de compromisso com estas práticas são normalmente, as causas mais comuns desta premissa.

Como Evitar?

Processos de treinamento e conscientização reduzem esta fraqueza, explicando quais são os controles existentes na empresa e como devem ser cumpridos por todos. Pessoalmente, recomendo ainda uma interação com o RH da empresa para definir punições administrativas e suporte para possíveis processos de demissão em caso de descumprimento.