

Gestão de Acessos x SOX x Auditorias

Fazer melhor, reduzindo custos e mantendo o nível de excelência.

São Paulo, 17/07/2009. A frase acima é bem conhecida pelos gestores das corporações mundiais. Porém, tentar alcançar a excelência pode representar o aumento nos custos, sem o alcance, contudo, de resultados satisfatórios em algumas ocasiões.

No passado, o desafio das empresas sob regulamentação SOX (Sarbanes-Oxley) era a adequação à norma. Hoje, o desafio é a manutenção desta adequação, reduzindo custos, mitigando riscos e racionalizando processos.

Mesmo para empresas que não estão sob a regulamentação norte-americana, a adoção de boas práticas de Governança Corporativa e Governança de T.I (Tecnologia da Informação) tem se tornado um diferencial competitivo, o que é um requisito importante para a sobrevivência das empresas em um mundo de constantes mudanças.

O assunto abordado neste artigo trata de uma situação que vem trazendo certas dificuldades para empresas e fornecedores no mundo. O controle de acessos aos sistemas que são base para relatórios financeiros - normalmente sistemas ERP (*Enterprise Resource Planning*) - é parte das exigências da SOX. Desde o início da vigência desta regulamentação, as empresas têm alocado recursos financeiros e humanos para garantir a adequação e a manutenção dos controles internos.

Diante da crise financeira mundial, empresas do mundo todo estão passando por ajustes que exigem, basicamente, “fazer mais e melhor”, gastando menos.

Com base neste cenário, podemos relacionar os principais motivadores para a implantação de um processo eficaz de acessos:

- Garantir que usuários desligados tenham acessos revogados conforme regras de negócio e no tempo adequado;
- Evitar que usuários recebam mais direitos que o necessário, minimizando o risco de fraudes;
- Facilitar a revisão de acessos;
- Diminuir o tempo gasto pelos recursos de T.I para geração de evidências para auditoria;
- Facilitar a manutenção das matrizes de segregação de funções (para evitar e/ou detectar fraudes);
- Reduzir custos com auditoria;
- Manter um registro centralizado de evidências - de modo a possibilitar respostas a questionamentos como “Quem aprovou?”, “Quem recebeu tal acesso?”, “Quais sistemas estão envolvidos?”.

Para facilitar o processo de implantação, evitando gastos não programados e trabalho extra, as seguintes fases devem ser consideradas:

1- Definição de escopo (“escopo é tudo”).

É necessário entender o processo como um todo desde os sistemas e as pessoas envolvidas na

	<i>Press Release</i>	PÚBLICO
---	----------------------	---------

solicitação de acesso, até a revisão e a revogação de acessos aos ativos da empresa. O conhecimento do processo permitirá a definição de fases e objetivos que devem ser alcançados em cada uma delas. Assim, teremos uma visão ampla do que é necessário sem perder os objetivos tangíveis de cada uma das fases.

2- Mapeamento de processos atuais da gestão de acessos na empresa.

Entendendo como estamos hoje, fica mais fácil visualizar e planejar onde queremos chegar. Automatizar a gestão de acessos só é produtiva quando o sistema utilizado contempla um fluxo pré-definido e coerente com os processos existentes.

3- Definição de melhorias nos processos.

Uma vez que os processos tenham sido mapeados, precisamos definir pontos que são passíveis de melhoria, de acordo com as regras de negócio e requisitos de auditoria.

4- Planejamento e definição de cronograma.

Utilizar as melhores práticas de mercado para definir um cronograma que atenda aos objetivos definidos para cada uma das fases. O cronograma deve levar em conta as eventuais necessidades de alteração em fluxos, configuração de ferramentas e mesmo desenvolvimento de software para requisitos específicos do negócio. Adicionalmente, situações, onde o sistema pode ser administrado por terceiros, o que também precisa ser considerado.

5- Comunicação e treinamentos.

A cultura das empresas normalmente apresenta certos desafios quando tratamos de mudanças. As pessoas tendem a sentir certo desconforto com mudanças que não estão claras. No entanto, se uma divulgação for realizada de maneira adequada, contando com o apoio dos usuários chave e produzida por pessoas devidamente treinadas, esse desconforto inicial tende a ser consideravelmente minimizado. O esclarecimento de quais são as melhorias no processo pode atrair adeptos à mudança, facilitando o processo de implantação.

6- Testes e Homologação.

Quando o uso de um sistema automatizado de gestão de acessos é definido, é muito importante que a implantação conte com equipes com conhecimento adequado tanto no âmbito técnico quanto em processos. A operação deve ser reproduzida em detalhes no ambiente de homologação. A homologação é o momento onde eventuais novas necessidades são identificadas, normalmente devido à atividades manuais não documentadas no processo anterior.

7- Implantação e início em produção.

As fases devem ser bem planejadas e de acordo com períodos indicados para alterações no ambiente. Normalmente, isto se dá no primeiro e no segundo quartil para empresas com adequação à SOX. É aconselhável a participação do departamento de auditoria ou controles internos para verificar a validade das evidências apresentadas, a existência de controle de erros e a detecção de falhas.

	<i>Press Release</i>	PÚBLICO
---	----------------------	---------

8- Monitoração

A criação e monitoração de métricas é a ferramenta para viabilizar a melhoria contínua do processo. Podemos ressaltar que estar seguro é diferente de estar adequado às normas vigentes.

Métricas, quando devidamente estabelecidas, auxiliam a justificar os custos iniciais com novos projetos de implantação de sistemas automatizados de gestão de acessos.

Finalmente, é sempre recomendado buscar fornecedores com experiência e comprometimento compatíveis com projetos planejados. Em processos complexos como a Gestão de Acessos e Identidades a base instalada é uma referência de grande valia para a escolha do fornecedor.

Adilson dos Anjos, é sócio-consultor da e-trust, graduado em Sistemas de Informação pela Flatec.

Sobre a E-TRUST:

A e-trust é uma *Partner Company* especializada em Segurança da Informação, tendo em seu quadro, colaboradores com certificações internacionais – Lead Auditor ISO27001, CISM, CISA, CISSP, CCSA, CCNA, LPI, MCSA, MCP, entre outras. A partir dos seus escritórios em São Paulo e Porto Alegre, a empresa presta serviços para clientes de grande porte em todo o Brasil e no exterior, em diversos segmentos.

A e-trust é composta por três unidades de negócio especializadas, que estão capacitadas para atender todas as demandas do mercado, sendo eles: Serviços Gerenciados de Segurança, HORACIUS – Sistema de Gestão de Segurança da Informação e Consultoria.

Informações para a imprensa:

www.e-trust.com.br

Tel.:(11) 5521-2021 - (51) 2117-1000

E-mail: comercial@e-trust.com.br