Asugday 2016

RIO DE JANEIRO

EVENTOS REGIONAIS **2016**

Asugday 2016
RIO DE JANEIRO

Mitos e Riscos de Fraude em Segregações de Funções no Perfil SAP

Soluções de Governança em TI

- Riscos SAP
- ITAM (IT Asset Management)
- Avaliação de TI
- Outsourcing

Perguntamos a algumas empresas...

Perguntas-Chave	Resposta típica dos administradores de segurança / Basis	Realidade
Quantas transações existem hoje em um sistema SAP ECC 6.0?	**20.000 transações**	**Mais de 150.000 transações**
Qual finalidade?	**Gerenciamento de acesso**	**Apenas a primeira linha de 'defesa' para acesso**
Quantos objetos de autorização existem em um sistema SAP ECC 6.0?	**"Mais de 20.000" ou "Múltiplos de 20k"**	**1.200 para o sistema ERP padrão (funcionalidade R/3)**
Qual finalidade?	**Restrição dos níveis organizacionais etc.**	**Gerenciamento de direitos de acesso.**

Análise de maturidade

Pequena	Médio	Grande
Sem ações na bolsa	Com ações na bolsa	Ações na bolsa no Brasil e em NY
Auditoria contábil externa, apenas	Controles internos, auditorias interna e externa	Auditorias, CI, área de riscos, certificadores, órgãos nacionais
Sem processo de acesso, área de TI concede conforme área solicita	Procedimento de acesso, acesso com equipe interna, SoD controlada por Excel	Procedimento, controles compensatórios, bloqueios automáticos, alertas
Sem controle de concessão ou riscos de acessos	Controle de acesso realizado por transação	Acesso concedido e monitorado por ferramenta de gerenciamento de riscos
Não há visibilidade dos riscos, tudo está bem	Sou auditado, meu controle em Excel atende às minhas necessidades	Sou auditado, certificado, possuo ferramenta de riscos

Impactos da imaturidade

Pequena	Médio	Grande
Descontrole total: quem acessa o quê? Quem é o dono da informação?	**Acessos fraudulentos através dos objetos de autorização**	**Acessos fraudulentos em transações de ”consulta” ou por quem concede acesso**
Sensação de necessidade de melhoria, mas não é o momento de investimentos	**Sensação de normalidade**	**Conforto pleno**
Sem matriz, o risco é do solicitante do acesso	**Matriz transacional voltada para o atendimento das auditorias**	**Matriz atende aos requisitos das auditorias e o sistema realiza monitoramento dos riscos. Nunca houve reavaliação da matriz**
Auditoria verifica que não sairam valores sem nota fiscal	**A auditoria verifica as transações e os objetos não são contemplados**	**A auditoria SoX, contábil e agências nacionais nunca identificaram falhas.**
Desvios em pagamentos já autorizados, mudança de conta e valores a pagar	Favorecimento de fornecedores (desbloqueio, aumento do limite de crédito), vazamento de tabela de preços, alteração em impostos, ajuste no inventário não autorizado.	

Asugday 2016
RIO DE JANEIRO

Nos três últimos levantamentos, o que identificamos?

Empresa 1 200 usuários	Empresa 2 400 usuários	Empresa 3 2200 usuários
SEM sistema de gerenciamento de riscos	**COM sistema de gerenciamento de risco**	**COM sistema de gerenciamento de risco**
Controle do analista *basis*	**Matriz *standard* atendendo à auditoria**	**Matriz *standard* atendendo à auditoria**
642 RISCOS identificados	607 RISCOS identificados	200 RISCOS identificados
550 transações por usuário, 35 utilizadas	280 transações por usuário, 20 utilizadas	**380 transações por usuário** **40 utilizadas**
• Acesso (SAP_ALL) por 1 dia e voltou ao normal. • Estagiário com 130 perfis • 44 usuários com acesso a transferir e aprovar horas	• **20 usuários com mais de 60 perfis cada** • **90 usuários movimentam mercadorias** • **20 usuários com acesso a modificar dados de clientes**	• **25 firefighters** • ***Range de s_tcode* (A*-Z*)** • **8 execuções de condição de preço de revenda por consultores**

Transações de “consulta”

Resultado seleção

Nome	Denominação breve
MB51	Lista docs.material

Objetos de autorização

Status	Objeto	Denominação de objeto	TST...	Cód.ver...	Propo...
	F_BKPF_BUK	Documento contábil: autorização para empresas		verificar	S
	M_MSEG_LGO	Movimentos merc.: depósito		verificar	S
	M_MSEG_WMB	Docs.de material: centro		verificar	S
	M_MSEG_WWA	Movimentos de mercadoria: centro		verificar	S
	S_ARCHIVE	Arquivamento		verificar	S
	S_DATASET	Autorização para acesso ao file		verificar	S
	S_TCODE	Verificação do código de transação no início da transação		verificar	S
	C_DRAW_TCD	Autorização atividades para documentos		verificar	NÃO
	C_DRAW_TCS	Autorizações dependentes do status para documentos		verificar	NÃO

Nome	Denominação breve
FBV3	Exibir documento pré-editado

Status	Objeto	Denominação de objeto	TST	Cód.ver	Propo
	F_BKPF_BED	Documento contáb.: autorização de acesso a contas p/clientes		verificar	S
	F_BKPF_BEK	Documento contáb.: autorização acesso a contas p/fornecedor		verificar	S
	F_BKPF_BES	Documento contábil: autorização de acesso a contas do Razão		verificar	S
	F_BKPF_BLA	Documento contábil: autorização para tipos de documento		verificar	S
	F_BKPF_BUK	Documento contábil: autorização para empresas		verificar	S
	F_BKPF_GSB	Documento contábil: autorização para divisões		verificar	S
	F_BKPF_KOA	Documento contábil: autorização para tipos de conta		verificar	S

Resultado seleção

Nome	Denominação breve
FBL5N	Partidas individuais de clientes

Objetos de autorização

Status	Objeto	Denominação de objeto	TST...	Cód.verif.	Propo...
	F_BKPF_BLA	Documento contábil: autorização para tipos de documento		verificar	S
	F_BKPF_BUK	Documento contábil: autorização para empresas		verificar	S
	F_BKPF_GSB	Documento contábil: autorização para divisões		verificar	S
	F_BKPF_KOA	Documento contábil: autorização para tipos de conta		verificar	S
	F_IT_ALV	Exibição de partidas individuais: modificar e gravar layouts		verificar	S
	F_KNA1_BED	Cliente: autorização de acesso a conta		verificar	S
	F_KNA1_BUK	Cliente: autorização para empresas		verificar	S
	F_LFA1_BUK	Fornecedor: autorização para empresas		verificar	S
	S_ALV_LAYO	Layout standard ALV		verificar	S
	B_NOTIF_BC	Atividades para mensagens		verificar	NÃO

Matriz SoD

Matriz de Segregação de Funções
Data de emissão: 10 de setembro de 2016

			Vendas e Receita												Compras										
			DADOS MESTRE DE CLIENTES	CLIENTES BLOQUEADOS	GERENCIAMENTO DE CRÉDITO	INCENTIVOS A CLIENTES	CONTRATOS DE CLIENTES	CONDIÇÕES DE PREÇO DE REVENDA	ORDENS DE VENDAS	LANÇAMENTO DE CONTAS A RECEBER	PAGAMENTO DE CONTAS A RECEBER	LANÇAR PAGAMENTO DE CONTAS A RECEBER	FATURAMENTO DE VENDAS	LIBERAÇÃO DE DOCUMENTOS DE VENDA	DADO MESTRE DE FORNECEDOR	FORNECEDORES BLOQUEADOS	FATURAMENTO DE FORNECEDOR E LANÇAME	PAGAMENTO DE CONTAS A PAGAR	LIBERAÇÃO DE FATURAMENTO DE FORNECED	LANÇAR PAGAMENTO DE CONTAS A PAGAR	PROCESSO E IMPRESSÃO DE PAGAMENTOS	EXECUÇÃO DO PROCESSO DE PAGAMENTO	REQUISIÇÃO DE COMPRAS	LIBERAÇÃO DE REQUISIÇÕES DE COMPRA	ORDENS DE COMPRA
			FI	SD	SD	SD	SD	SD	SD	FI	FI	FI	SD	SD	FI	MM	FI	FI	MM	FI	FI	FI	MM	MM	MM
		GRP	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
INCENTIVOS A CLIENTES	SD	04																							
CONTRATOS DE CLIENTES	SD	05			5																				
CONDIÇÕES DE PREÇO DE REVENDA	SD	06			1		5																		
ORDENS DE VENDAS	SD	07			1		5	1																	
LANÇAMENTO DE CONTAS A RECEBER	FI	08	5	5	1		5	1																	
PAGAMENTO DE CONTAS A RECEBER	FI	09			1					1															
LANÇAR PAGAMENTO DE CONTAS A RECEBER	FI	10			1		5			1	2														
FATURAMENTO DE VENDAS	SD	11			1		5		1			4													
LIBERAÇÃO DE DOCUMENTOS DE VENDA	SD	12		3	1		5			1	4	1	1												
DADO MESTRE DE FORNECEDOR	FI	13		3											4										
FORNECEDORES BLOQUEADOS	MM	14													4										
FATURAMENTO DE FORNECEDOR E LANÇAMENTO DE CONTAS A PAGAR	FI	15			1		5	1			1	1			1		1								
PAGAMENTO DE CONTAS A PAGAR	FI	16									2				4		1								
LIBERAÇÃO DE FATURAMENTO DE FORNECEDOR	MM	17																							
LANÇAR PAGAMENTO DE CONTAS A PAGAR	FI	18						2			2				4		1	4							

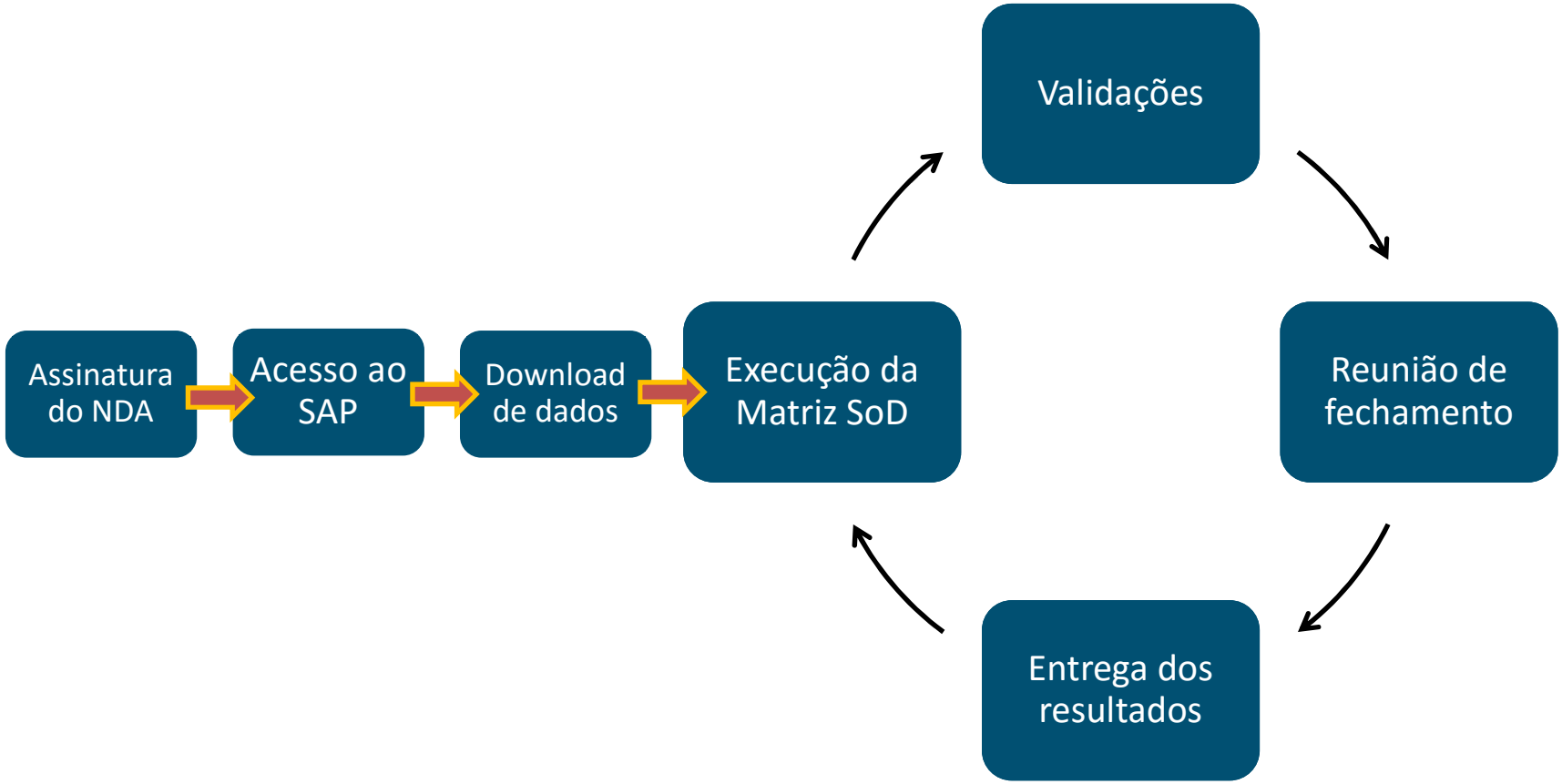
Como apoiamos nossos clientes a aumentarem a maturidade

- **Diagnóstico:**
  - Identificação dos riscos SoD;
  - matriz de segregação de funções (SoD) personalizada com 914 RISCOS cadastrados.

- **Projeto de adequação dos perfis à Matriz SoD:**
  - Reuniões de alinhamento;
  - entrevistas;
  - desenho de controles compensatórios e controles configuráveis;
  - ajustes no sistema.

- **Serviços continuados:**
  - Identificação dos riscos SoD mensalmente (indicadores de riscos e áreas que executaram SoD);
  - manutenção e revisão da matriz de segregação de funções;
  - configuração de perfis conforme necessidade de ajustes SoD;
  - revisão e melhoria do processo de concessão de acesso;
  - manutenção de controles compensatórios;
  - auxílio nos testes de perfis;
  - monitoramento do ambiente remotamente;
  - suporte a auditorias externas.

O Processo


Assinatura do NDA
Acesso ao SAP
Download de dados
Execução da Matriz SoD
Validações
Reunião de fechamento
Entrega dos resultados

O que entregamos – benefícios

- Redução de riscos de FRAUDE através de redução de transações de cada usuário;
- Redução ou substituição de usuários SAP através da identificação de pouca utilização do sistema;
- Matriz SoD mensal com todos os riscos detalhados + visão geral da quantidade de riscos;
- Suporte na tratativa de riscos SoD (controles compensatórios ou controles configuráveis);
- Identificação de novos riscos, seus usuários e motivação de criação (adaptação no perfil, acesso indevido, novo usuário ou fraude de concessão de acesso);
- Matriz de risco personalizada e padronizada para a empresa, em conformidade com SOX;
- Redução de riscos relacionados à imagem no mercado;
- Isenção no risco de criação de usuários/acessos sem autorização;
- Total Compliance com as exigências das auditorias anuais;

MITO - FRAUDE

- MITO é acreditar que possuindo controles validados pela auditoria não haja nenhum outro novo risco.
- MITO é possuir um sistema de gestão de risco com elevado custo e acreditar que não possui problemas.
- MITO é acreditar que o que passa pela auditoria é o que importa.
- FRAUDE é quando não há iniciativa para averiguar novas oportunidades.
- FRAUDE é acreditar que o fraudador irá aonde há segurança.
- FRAUDE é manter-se no mesmo nível de segurança e controle desde que se implantou o sistema.
- SoD não é para atender apenas à auditoria e sim para evitar FRAUDES.
- A Matriz de segregação é crescente, não estática.

E o que importa?

- Revisar/criar uma matriz de riscos orientada para os objetos de autorização, campo e valor de campo. Os riscos identificados devem ser claros na descrição/

- Controlar quem concede e modifica acesso.

- Equilíbrio entre os controles compensatórios e os controles configuráveis; muitos controles compensatórios atrapalham a dinâmica da empresa.

- Pesquisar novos riscos existente, atualmente há muito foco em riscos antigos, reanálise, e pouco há de novas descobertas.

OBRIGADO!

LUIS VIEIRA
luisvieira@itrisk.com.br

21 – 998566913