



Ministério da
Ciência e Tecnologia



Rede GESITI: criada em 18/02/08 possui ~ 1.000 colaboradores

Jornal Rede GESITI - Ed. Outubro/2008

GESITI: acrônimo para Sistemas e Tecnologias de Informação Aplicados à Gestão em Organizações.

- # - A Rede GESITI abrange o estudo inter e multidisciplinar dos Sistemas e Tecnologias de Informação e os aspectos humanos relacionados com o entendimento de como as pessoas procuram, obtêm, avaliam, compartilham, classificam e utilizam o uso da informação.
- # - ÊNFASE: **ASPECTOS SOCIOTÉCNICOS DAS TI**
- # - **OBJETO DA LISTA:** promover o encontro de pesquisadores, educadores, empresários e gerentes de instituições públicas e privadas, visando proporcionar a troca de experiências e o debate sobre trabalhos prospectivos que possam indicar as tendências da área.
- # - **PÚBLICO ALVO:** Empresários, consultores e profissionais vinculados à Gestão de Organizações, profissionais de TI e Informática, professores, pesquisadores e outros interessados no tema.

Contato: GESITI@cti.gov.br ou GESITIs-owner@yahoogrupos.com.br

Conheça o CTI (Centro de Tecnologia da Informação): <http://www.cti.gov.br/>
Acesse “CTI Informa” (Maio/Jun. 2008): http://www.cti.gov.br/cti_informa/cti_informa.htm

VIII Jornal GESITI/2008, editado por Antonio José Balloni (GESITI/DGE/CTI), com a colaboração de Nelma T Zubek Valente (FEA-USP/UEPG).

Palavras dos editores:

Prezado leitor,

Nesta edição, você tem a oportunidade de rever e/ou tomar conhecimento das principais discussões geradas no grupo GESITI com as respectivas contribuições dos diferentes colaboradores da lista, cujos textos foram compilados a partir das mensagens enviadas para a lista GESITI no período de 04 a 07 de setembro de 2008. Houve alguma edição nos textos encaminhados, mas nada que comprometesse a essência das colaborações. Visando facilitar a leitura e análise das diferentes contribuições contidas nas mensagens recebidas, utilizou-se o já tradicional agrupamento por temas, que nesta edição, aparecem subdivididos em: “Auditoria em Tecnologia da Informação”, “Tecnologia da Informação e Planejamento Estratégico” e “Gestão de Riscos”.

Agradecemos a todos os que colaboraram com os temas discutidos nesta edição ao mesmo tempo em que convidamos os demais membros do grupo para uma participação mais efetiva. Afinal este espaço existe para você EPP (Empresário, Profissional ou Pesquisador), que tem algo a contribuir (seja comentando, discordando ou acrescentando) com o estudo e entendimento dos aspectos sociotécnicos relacionados ao uso da Tecnologia e Sistemas de Informação.

Note que as mensagens selecionadas para este Jornal serão apagadas da rede GESITI. As mensagens não selecionadas (porque, apesar de estarem no escopo da rede, não tratam do propósito desejado: *gerar discussão dentro de um contexto estabelecido*) permanecem no endereço <http://br.groups.yahoo.com/group/GESITIs/messages>. Todas as edições do Jornal Rede GESITI estão disponíveis para download no [Portal Mundo Acadêmico](#) (http://mundoacademico.unb.br/contendos/pesquisa.php?pesqP_02=GESITI)/Ministério da Educação ou no site da Revista digital *Ciência y Técnica Administrativa* (<http://www.cyta.com.ar/boletines/gesiti.htm>).

Ainda, se você que não participa da Rede GESITI e que tem interesse em colaborar e contribuir com as discussões dos temas propostos pelo grupo fazemos o convite para que entre em contato com GESITI@cti.gov.br ou GESITIs-owner@yahoogrupos.com.br para o envio de mensagens e respectivas contribuições. EPP. Você somente saberá se sua opinião é importante após disponibilizar a mesma para a rede!

Abraços a todos.

Jornal GESITI/CTI - www.cti.gov.br



Ministério da
Ciência e Tecnologia



Rede GESITI: criada em 18/02/08 possui ~ 1.000 colaboradores

Tema I – Auditoria em Tecnologia da Informação

=====

PARTICIPAÇÃO em 05/09/08, por **Cosme Leandro do Patrocínio**

=====

Quero escrever sobre o assunto “Governança de TI: um desafio para a auditoria interna” (4º CONTECSI/07 (Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação)).

Trabalhamos com o conceito de que a auditoria interna deve identificar e avaliar os riscos relacionados com a área de TI e propor as ações necessárias para que os riscos sejam mantidos em níveis aceitáveis pela organização. Utilizamos como referência o **COBIT**, que apresenta e detalha os controles necessários para uma Governança de TI adequada para a organização, tendo em vista a importância e os riscos que a TI representa para os processos de trabalho e o alcance dos objetivos estabelecidos.

A metodologia que elaboramos busca apresentar às auditorias internas uma forma de executar os trabalhos nas áreas de TI. Cabe acrescentar que a metodologia proposta no artigo encontra-se ainda em evolução, considerando que está sendo implementada na empresa em que trabalho.

Para pensarmos!!! Quanto aos riscos relacionados ao processo de desenvolvimento de sistemas de informação, identificamos que existe um grande gargalo no processo, que acredito merecer estudos na área acadêmica. As áreas de negócios demandam sistemas de informação para a TI. No entanto, nem sempre conhecem, com a profundidade necessária, aquilo que será automatizado. Este fato leva dificuldades para a equipe de desenvolvimento, que além de realizar as suas funções definidas no processo de desenvolvimento, recebe o custo do mapeamento do processo de negócio, que acredito ser de responsabilidade da área de negócio. O que pensam sobre a questão colocada? A TI deve assumir o papel de mapeamento dos processos de negócio?

Cosme Leandro do Patrocínio
cleandro-df

=====

PARTICIPAÇÃO em 06/09/08, por **Daniel Silveira**

=====

Em resposta ao Sr. Cosme Leandro (mensagem anterior) e a todos que participam positivamente do Grupo GESITI, informo que: Também participo da rede GESITI, trabalho com Auditoria e Segurança, utilizando um *software* que filma as informações na rede e gostaria de saber sua opinião, pois não monitoramos as pessoas, e sim, a informação, inclusive VoIP. Estamos com reuniões agendadas em órgãos reguladores. O *software* utilizado denominado “**Rootnet**” possibilita isolar, controlar e monitorar, em detalhes, uma aplicação,

um usuário, um servidor, filmando o trânsito das informações na rede. Encaminho, abaixo, Notícias na Mídia, sobre o assunto:

- Fórum de Segurança (On Line). **Nielsen reforça gerenciamento de rede e reduz gastos com aumento de banda.** (<http://www.oxxys.com.br/midia/forum-seguranca.html>)
- COMPUTERWORLD (On Line). **Tyco adota solução nacional para gerenciar rede de dados.** (http://www.oxxys.com.br/midia/CW_Tyco.htm)
- Correio do Estado de Campo Grande. **Monitore o tráfego da rede e o seu desempenho.** (http://google.amixsi.com.br/rootNet/CE_CG.pdf)
- Revista PC & Cia. **Nova solução nacional monitora tráfego e otimiza desempenho de redes.** (http://google.amixsi.com.br/rootNet/PC_Cia.htm)

Daniel Silveira

silveira@oxxys.com.br

(11) 3825-9985 - (11) 9485-3516 – www.oxxys.com.br

=====

PARTICIPAÇÃO em 06/09/08, por GESITI

=====

Quanto ao questionamento levantado pelo Cosme Leandro (mensagem acima), cujo conteúdo aparece resumido abaixo(*), seguem alguns comentários.

a) Note que, conforme previamente mencionado por Fauzi Shubeita (ver pag. 01 do I-Jornal GESITI FEV/MAR_08, disponível em: <http://mundoacademico.unb.br/users/rachelmoraes/1222611527170274112141704181.pdf> ou http://www.cyta.com.ar/suplementos/gesiti/gesiti_02_2008.pdf) “[...] o fator crítico que observo nas relações quando o assunto é um SI reside na falta de visão da área de desenvolvimento sobre o negócio (TI não entende o negócio) e a falta de embasamento técnico por parte da organização (o negócio cria falsas expectativas sobre o SI).”

b) Ainda, nesse mesmo Jornal (ver pag. 01 do I-Jornal GESITI_FEV/MAR_08/moderador disponível em: <http://mundoacademico.unb.br/users/rachelmoraes/1222611527170274112141704181.pdf> ou http://www.cyta.com.ar/suplementos/gesiti/gesiti_02_2008.pdf), discutimos alguns desses aspectos. Como essencial e relacionado com o tema levantado por Cosme Leandro: “[...] Ao desenvolver um SI de informação é preciso muito mais que uma mera redistribuição de máquinas e trabalhadores e, sim, mudanças em quem tem o controle da informação, quem tem o direito de acessar e atualizar a informação e quem toma a decisão sobre quem, quando e como. Existem ALGUNS PONTOS DE INTERSECÇÃO que precisam ser considerados nesse desenvolvimento:

- * As POLÍTICAS ORGANIZACIONAIS: Pontos de vistas divergentes conduzem a disputa, competição e conflito político. Atrasam a mudança organizacional, especialmente o desenvolvimento de novos SI.
- * A CULTURA: é a força unificadora da organização MAS pode também ser uma poderosa limitadora para mudanças, especialmente tecnológicas. * etc.



Ministério da
Ciência e Tecnologia



Rede GESITI: criada em 18/02/08 possui ~ 1.000 colaboradores

O Desenvolvimento e a implantação de SI possuem diferentes impactos sobre diferentes tipos de organizações. A introdução de um novo SI vai afetar a estrutura organizacional, seus objetivos, projetos de trabalho, valores, competição entre grupos de interesses, a tomada de decisão e até o comportamento dia/dia. Para se colher os benefícios da TI, mudanças na Cultura, Valor, Normas e Alinhamento de Grupos de Interesses Organizacionais precisam ser gerenciadas com muito planejamento e esforço; como precisam ser gerenciadas as mudanças Tecnológicas. SI podem mudar a hierarquia da tomada de decisão nas organizações, pela diminuição dos custos de aquisição de informação e ampliando a sua distribuição. Reduzem a necessidade de gerenciamento médio e suporte administrativo. Portanto, o desenvolvimento de um SI pode de fato afetar quem faz o que, para quem, quando, onde e como na organização. A implantação de um SI em uma organização leva em consideração a competição entre subgrupos organizacionais que influenciam as políticas organizacionais, seus procedimentos e os seus recursos. Isto posto, um SI torna-se inevitavelmente inserido dentro da política organizacional, pois influenciam no acesso aos recursos-chaves da organização (as informações): SI podem de fato afetar quem faz o que, para quem, quando, onde e como na organização. Então, devido ao fato de SI potencialmente mudar a estrutura organizacional, sua cultura, política e trabalho, existe uma considerável resistência quando se quer introduzir um SI, ou seja, quando se implanta um SI traz-se conseqüências para a missão da organização, para a estrutura e para as pessoas: todos os três resistem contra a implantação de uma nova TI [...].

Nesse mesmo Jornal ([ver pag. 02 do I-Jornal GESITI FEV/MAR 08/moderador](http://www.cyta.com.ar/suplementos/gesiti/gesiti_02_2008.pdf), disponível em: <http://www.mundoacademico.unb.br/users/rachelmoraes/12226115271702741112141704181.pdf> ou http://www.cyta.com.ar/suplementos/gesiti/gesiti_02_2008.pdf), em fomento ao cerne da questão levantada por Cosme Leandro, apresentamos que, de fato, a TI não entende de negócio:

"[...] o que se precisa é analisar qual processo de negócio precisa ser automatizado (e aí, de forma simplista, precisa **conhecer** o negócio: visitar o chão de fábrica para verificar gargalos e analisar se VALE a pena eliminar, POR AUTOMATIZAÇÃO, esses gargalos). VEJAM: Quando se compra, instala ou se desenvolve um SI para otimizar um modelo de negócio ou um processo de negócio errado (por ex., um sistema ERP padrão que promete automatizar tudo) seu negócio pode passar a fazer, de modo mais eficiente, o que **não** deveria fazer! Portanto, quando se automatizam processos de negócio que não deveriam ser automatizados, sua organização pode fazer de modo ainda mais ineficiente aquilo que estaria fazendo sem estar automatizada. Como resultado, sua empresa se torna vulnerável E/OU AINDA, pode perder vantagem competitiva [...]. Uma das decisões estratégicas mais importantes que uma empresa pode tomar é: ENTENDER qual o processo de negócio que precisa de melhoria e NÃO decidir como usar SI para melhorar processos de negócios [...]."

Esperando ter contribuído, aguardamos novas considerações.

GESITI/CTI
gesiti@cti.gov.br

=====
PARTICIPAÇÃO em 06/09/08, por **Daniel Silveira**
=====

Quanto ao questionamento levantado pelo Sr. Cosme Leandro (mensagem pag.2) segue meu breve comentário.

Você já imaginou uma ferramenta que coleta todo o trânsito dos dados de sua rede, 24 horas por dia, sendo capaz de armazená-las, gerando históricos auditáveis de todos os dados transacionados, (identificando suas Origens e Destinos)?

Existem 04 elementos básicos em todas as redes:

1. Pessoas (Usuários e Administradores da rede)
2. Ativos de Rede (Servidores e Aplicações)
3. Meio (Links externos e a rede interna)
4. E aInformação.....

Nosso segredo é monitorar a informação, pois através dela monitoramos os demais elementos, de qualquer rede. Peça um *test-drive* para sua empresa.

Espero ter contribuído neste questionamento.

Daniel Silveira

silveira@oxxys.com.br

(11) 3825-9985 - (11) 9485-3516 – www.oxxys.com.br

=====
PARTICIPAÇÃO em 06/09/08, por **Fauzi Shubeita**
=====

Estou gostando dessa discussão. Podemos pensar em monitorar as informações, mas... Quem vai fazer isso? O pessoal de TI? Ou seria o estratégico? Mas a ferramenta é de TI e a informação interessa ao estratégico... ..

Oportunas as considerações (sobre o monitoramento das informações) e já fui dar uma espiada no *folder* da ferramenta **Rootnet** (mencionada na pag. 2, deste jornal).

Aguardo novas postagens. Aliás, se alguém da lista utiliza essa ferramenta e já escreveu algo sobre os resultados, por favor, nos comunique.

Fauzi Shubeita

shubeita@terra.com.br

=====
PARTICIPAÇÃO em 06/09/08, por **Daniel Silveira**
=====

Em resposta à solicitação do Sr. Fauzi (mensagem anterior), informo que sou a pessoa que apresentou o **Rootnet** (*software* de monitoramento de informações, mencionado na pag. 2 deste Jornal), e gostaria de apresentar outras discussões a respeito de *Softwares* Auditáveis, nesta nossa rede, com os quais trabalho há cerca de 08 anos.



Ministério da
Ciência e Tecnologia



Rede GESITI: criada em 18/02/08 possui ~ 1.000 colaboradores

Mas respondendo às suas questões, acredito que a função da TI é gerar históricos auditáveis para as áreas de auditoria e segurança da informação, pois estas sim são as responsáveis por tais ações. Cabe à essas áreas, portanto, a responsabilidade pela prestação das informações de modo transparente às autoridades que os convocam a prestar estes tipos de esclarecimentos, seja em um banco ou em uma empresa de Telefonia ou Telecom.

No caso das empresas os funcionários são previamente avisados de que serão monitorados, sendo válida, legalmente, esta ação, inclusive em ligações gravadas em *Call Centers*. Gostaria de informações de alguém da rede a respeito de:

1. Quando um *software* de Auditoria da Informação se torna um *software* Auditável ?

Pelos Normativos Internacionais (Sarbanes-Oxley, COSO, CobiT, ITIL e Basileia II) são:

- quando não há interferência humana nas etapas de coleta, processamento e elaboração dos dados;
- quando as "trilhas de logs" são **auditáveis**, ou seja, indelévels ou "indeleteáveis"; e
- que haja registro de tentativas de acesso à base de dados da auditoria e controle da segurança da informação em empresas e instituições que são responsáveis e possam responder legalmente, por tais informações.

Daniel Silveira

silveira@oxsys.com.br

(11) 3825-9985 - (11) 9485-3516 – www.oxsys.com.br

Tema II - Tecnologia da Informação e Planejamento Estratégico

=====
PARTICIPAÇÃO em 05/09/08, por **Denis Alcides Rezende**
=====

É muito importante que a TI vá muito além da TI, ou seja, que efetivamente se integre ao negócio da organização. A integração operacional se faz no dia a dia e de acordo com as limitações e condições da organização. Já a integração gerencial e estratégica exige planejamento tanto da organização, quanto das informações, sistemas de informações e tecnologia da informação e seus recursos.

Sugiro, para tanto, alguns modelos que podem ser encontrados no livro que acabei de lançar: Tecnologia da informação e planejamento estratégico: alinhamento e integração com a inteligência organizacional privada ou pública. (Informações: <http://www.netpar.com.br/engsoft>).

Também posso fornecer alguns artigos para os interessados.

Denis Alcides Rezende, Dr.

<http://www.netpar.com.br/drezende>

(41) 9974.1168 - drezende@netpar.com.br

Tema III – Gestão de Riscos

=====
PARTICIPAÇÃO em 06/09/08, por **GESITI**
=====

Prezados Colaboradores,

Não é minha especialidade tratar sobre o tema Gestão de Risco, mas, como existe um vasto material no assunto, resumo uma pesquisa simples e repasso para suas análises e considerações. É importante que considerem o conteúdo da mensagem (GESITI pág. 3) e (links lá informados), sobre os aspectos sociotécnicos das TICs (& Auditoria em Tecnologia da Informação), pois estou certo que, para os mais experientes dessa rede no tema gestão de riscos & auditoria, fica claro que tais temas estão inter-relacionados. A seguir, o resumo da referida mensagem:

"[...] A viabilidade da maioria dos negócios está hoje fortemente apoiada na infra-estrutura de Tecnologia da Informação. O relacionamento das empresas com seus colaboradores, clientes, fornecedores e acionistas é mediado, na maior parte das vezes, por computadores. Esse uso intensivo de tecnologia proporciona inúmeras oportunidades, mas também altos riscos para a continuidade do negócio se os sistemas em uso não forem totalmente seguros (vejam, sem trocadilhos, a dificuldade de uma rede, como a GESITI, no que se relaciona a gestão aberta & riscos [...]). Bem, gerenciar o risco digital é tão importante quanto administrar riscos financeiros e outros riscos operacionais. Segundo dados da Ernst & Young, mais da metade das empresas experimenta interrupções inesperadas de algum sistema crítico ao longo do ano. A perda e a violação de informações têm impacto altamente negativo na reputação e estabilidade financeira de sua organização [...] Além disso, um processo de tomada de decisões reflete a essência da dinâmica empresarial. Portanto, administrar é decidir, e a continuidade de qualquer negócio depende da qualidade das decisões tomadas por seus administradores nos vários níveis organizacionais. E estas decisões, por sua vez, são tomadas a partir de dados e informações viabilizados pela contabilidade, levantados a partir do comportamento do mercado e do desempenho interno da empresa. No entanto, esse processo de tomada de decisão vem assumindo complexidade e risco cada vez maiores: desequilíbrios nas taxas de juros, desajustes de mercado e competitividade, entre outros aspectos, vêm exigindo uma capacidade mais analítica e questionadora das unidades decisórias com relação ao risco empresarial. Conceitos financeiros consagrados em outros ambientes costumam encontrar enormes dificuldades de adaptação, demandando um conjunto de ajustes e reflexões nem sempre seguidos pelo mercado [...] Por outro lado, o conceito de 'Gestão de Riscos de TI' é bastante novo. No passado, os riscos associados à TI estavam limitados a aspectos como segurança e continuidade dos negócios. Hoje, o conceito sobre riscos de TI evoluiu e tornou-se clara a visão de que os riscos de TI não são unidimensionais. Com base nessas considerações, pergunto:



Ministério da
Ciência e Tecnologia



Rede GESITI: criada em 18/02/08 possui ~ 1.000 colaboradores

1.3 - O que significa, efetivamente, um planejamento em Gestão de Risco e quais os aspectos gerenciais desta gestão?

2.3 - Qual o investimento exigido em recursos tecnológicos e humanos e qual o impacto sociotécnico envolvido nessa atividade?

3.3 - O que um programa de gestão de riscos de TI deve avaliar em relação à segurança e disponibilidade de dados? (ver conteúdo da pag. 01/02 do I-Jornal GESITI FEV/MAR 08, disponível em: <http://mundoacademico.unb.br/users/rachelmoraes/12226115271702741112141704181.pdf> ou http://www.cyta.com.ar/suplementos/gesiti/gesiti_02_2008.pdf).

GESITI/CTI
gesiti@cti.gov.br

variáveis de risco conhecidas e relacionadas com o objetivo da rede e ofereceria recomendações de controles para mitigar esses riscos, sem deixar de considerar a relação custo x benefício (Temos que tomar o cuidado de não recomendar controles que inviabilizem o alcance do objetivo do negócio).

O valor agregado da auditoria, neste caso, estaria na possibilidade de que os eventos conhecidos (*spam*), que estão levando alguns colegas a solicitar suas saídas da rede, não estivessem ocorrendo.

Cosme Leandro do Patrocínio
cleandro-df

=====
PARTICIPAÇÃO em 06/09/08, por Cosme Leandro do
Patrocínio

=====
PRÓXIMA EDIÇÃO: NOV/2008 – Participem!

Caros Colegas da GESITI,

Mensagens para: GESITI@cti.gov.br ou GESITIS-owner@yahoo grupos.com.br

Estou gostando de ver o 'movimento' da rede em relação ao questionamento que apresentei sobre os riscos relacionados com o desenvolvimento e a implementação de sistemas de informação nas organizações e da responsabilidade pelo mapeamento dos processos de negócio.

Rede GESITI: Bom para sua empresa, bom para você e bom para todos.

Participem!

Atuo na área de auditoria interna em TI, que é independente da área de TI. Os auditores de nossa área, dentro do princípio de independência que trabalhamos, têm a responsabilidade de avaliar os controles internos relacionados com todos os processos de TI desenvolvidos na organização, com a finalidade de assegurar, com razoável certeza, a qualidade e a segurança no recebimento e na entrega das informações para as áreas de negócio. Esses processos envolvem questões relacionadas às aplicações, informações, infraestrutura e também às pessoas, devendo a auditoria interna atuar em todos esses recursos.

Outro aspecto importante é que a auditoria está perdendo a característica de "fiscalização" e está apontando para o sentido da "consultoria", devendo atuar de forma pró-ativa, antes da concretização dos riscos.

Cabe acrescentar que existem as 'auditorias' que geralmente observam a conformidade dos processos de TI, diferente do papel da auditoria interna.

Entendo que um dos grandes desafios da auditoria interna é "convencer" os gestores de TI da importância de instituir os controles necessários para uma boa governança de TI e das vantagens que estes poderão agregar aos processos. Nesse ponto identificamos as dificuldades políticas e a necessidade de definir estratégias de ação, para alcançar os objetivos com o menor desgaste possível.

Gostaria de colocar como exemplo o risco de perda de associados que a TI está permitindo à rede GESITI, que tem como um dos objetivos integrar pessoas com interesses comuns para discutir temas relacionados à TI. A auditoria interna avaliaria todas as