FACULDADE DE TECNOLOGIA DO NORDESTE

Autores: Alberto Imbunde; Alciolina Erica Lopes Furtado; Demba Semedo Baldé; Ensa Mané; José Fali Jau; Jeferson Plínio.

Professor orientador:

João Luiz Saraiva

Trabalho Pratico: Política de Segurança e Ética.

Fortaleza: 2012

NOME DA EMPRESA

“GUISOLUÇÕES ltda”

ÁREA DE NEGOCIO

A empresa Guisoluçoes atua na área de criação e desenvolvimento dos projetos de TIC tecnologia de informação e comunicação.

DEPARTAMENTALIZAÇAO

A empresa Guisoluções contém seguintes departamentos:

Departamento de gerenciamento de projetos (DGP); Departamento de recursos humano(DRH); Departamento de finanças e contabilidade(DFC) Departamento de tecnologia da informação (DTI) Departamento de compras(DC) Departamento de controle e segurança (DCS); Departamento de Marketing.

A empresa Guisoluçoes descreve quatro principais departamentos de prioridade, para trabalhar o seu plano de contingencia:

Primeira prioridade: Departamento de Tecnologia da Informação (DTI).

Segunda prioridade: Departamento de Administração e Finanças (DAF).

Terceira prioridade: Departamento de Desenvolvimento dos Projetos (DDP).

Quarta prioridade: Departamento dos Recursos Humanos:

MISSAO

A nossa missão e aperfeiçoar os produtos e serviços da informática eliminando os desperdícios do tempo e recursos nos projetos de tecnologia de informação e comunicação TIC, através de uma gestão qualificada. Proporcionando ao mercado um custo beneficio a cada nível do negocio.

VISSAO

A nossa visão e conquistar o nosso nicho de mercado nacional e internacional ganhar um credito de confiança das pequenas e medias e grandes empresa no nosso primeiro (3) anos de vida.

VALORES

Temos como valores fundamentais:

Ética, responsabilidade social; responsabilidade profissional; respeito ao cliente compromisso; qualidades; querência; e satisfação.

POLITICA DE SEGURANÇA

A Guisolucões trabalha com os projetos de terceiro, desde desenvolvimento ate na parte da infraestrutura da tecnologia da informação e comunicação TIC. Porem, como empresa responsável, a guisolucoes propõe sua política de segurança e ética.

1º - É de responsabilidade do gerente do projeto assinar o termo de abertura do projeto, desde que o projeto adquirido foi analisado em três etapas de comitê de gerenciamento de projeto.

2º - No caso do projeto de software cada desenvolvedor, ou seja, diferentes desenvolvedores cuidarão das diferentes páginas.

3º - Das mudanças nos projetos: Toda e qualquer mudança no projeto em curso só poderá ser aprovada no conselho das partes interessadas (staholders) e será atualizada numa versão específica documentado do projeto.

4º - Da adesão dos contratos: No momento de negociar qualquer contrato com qualquer que seja cliente, ele será fornecido um documento que explicitará todo o nosso padrão de desenvolvimento dos projetos e a seguir estes será assinado por ambas às partes.

5º - De acesso às informações: Será elaborado um plano específico de comunicação para cada projeto, de acordo com o proprietário do projeto e as

partes interessadas, quem, como e quando devem ser fornecidas as informações do projeto.

6º - Dos projetos críticos do software: Cada etapa de software será responsabilizada por um engenheiro especifico, no final do projeto só um engenheiro coordenador do projeto terá acesso todo o código fonte de software e responsabilizará a entregá-lo ao dono.

7º - De acesso a visitantes: É expressamente proibido o acesso estranho na sala de analise e desenvolvimento do projeto

TERMO DE COMPROMISSO

Comprometo-me a:

1. Executar as minhas tarefas, de forma a cumprir as minhas obrigações e as orientações da política da segurança com as normas e os padrões vigentes da organização em pauta.

2. Usar adequadamente os patrimônios, valores e espaço institucional, ou seja não frequentar nos Departamentos dos quais não estou lotado, e nem acessar as informações dos mesmos salvo em casos especiais, ou por determinação do seu chefe.

3. Em circunstancia nenhum revelar fora do âmbito profissional os fatos ou informações relacionados aos projetos ou seja a corporação em geral se não em delegação do seu superior hierárquico.

4. Não abandonar a corporação de forma alheia pondo em risco as tarefa que me são atribuídas ou prejudicar de forma alguma os projetos em curso, ou a corporação em geral.

5. Obedecer aos padrões de acesso aos equipamentos da informática estabelecidos pelo DTI:
    a) Mudanças de senha
    b) Cancelamento ou bloqueio de qualquer site.
    c) Manutenção preventiva das maquinas (backup e formatação).

6. Não instalar e nem desinstalar qualquer tipo de programa nos computadores corporativos, sem conhecimento do DTI.

7. Comprometo a seguir com as políticas de segurança, respeitando os padrões e a cultura desta organização.

Declaro estar ciente das determinações acima, comprometendo que quaisquer descomprimindo dessas regras podem implicar das sanções disciplinares com forme a legislação do pais.

Fortaleza, ___de_____de 20__.

Dep. Recursos Humanos:

_____

Responsável.

_____

Testemunha1 Testemunha2

_____ _____

Plano de contingencia

Plano de contingência, ou seja, *plano de recuperação de desastres*, tem como objetivo de descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos a corporação,

A Empresa Guisoluções desenvolve o seu plano de contingencia, baseado em padrão de quatro etapas:

Primeira Etapa: conscientização.

A equipe dos especialistas definidas para desenvolver o projeto do plano de contingencia estabelece um roteiro para esta primeira fase.

1º- O responsável do projeto terá um encontro inicial com a alta direção da organização solicitando o apoio e comprometimento da mesma no projeto.

a) Dar detalhes sobre o q é um plano de contingencia, a sua vantagem, o seu suposto custo, e os impactos da sua ausência na organização.
b) Divulgação do projeto.
c) Criação de um comitê, no qual devem participar os gerentes departamentais.

2º - O gerente do projeto terá que apresentar o comitê objetivo, cronograma e premissas dos projetos, e cabe a ele propor seguintes questões e recolher informações preliminares.

a) Nível de dependência de TI no departamento
b) Qual valor da informação no departamento?
c) Qual o impacto de ausência de TI no departamento?
d) Problemas mais frequentes ligados a TI.
e) Comportamento comum dos usuários de TI no departamento.

3º perante este fato o gerente explicitará ameaças ligados a cada parte, e enfim, com a colaboração de comitê será marcada reunião departamentais ou por equipe, discutindo os pontos em destaques. Os membros do projeto acompanhará as reuniões departamentais e terão como função explicar nitidamente sobre riscos e ameaças menos consideráveis e seus possíveis impactos.

Segunda Etapa: Identificação e avaliação dos riscos e vulnerabilidade.

Identificação dos riscos no Departamento de Tecnologia da Informação (DTI).

1 – Queda de internet;

2 – Mão uso do hardware;

3 – Circuito interno;

4 – Acesso estranho a rede coorporativo;

5 – Desastre climático ou orquestrado;

6 – Uso do software não autorizado ou sem licença.

Identificação dos riscos no departamento administração e finanças (DAF).

1 - Inflação;

2 – Invasão de conta coorporativa;

3 – Falsificação dos cheques coorporativos;

4 – Quebra do banco (falência);

5 – Atraso em pagamento das faturas.

Identificação dos riscos no departamento de desenvolvimento dos projetos (DDP).

1 – Desfalque do gerente do projeto no pleno projeto;

2 – Desvio de verbas de um projeto em andamento;

3 – Atraso em desenvolvimento e entrega de um projeto;

4 – Perda de dados e requisitos de um projeto;

5 – Fatores externos (climáticos, geográficos, econômico e político).

6 – Falta de colaboração na implementação de um projeto na organização terceiro (resistência dos usuários).

IDENTIFICAÇÃO DOS RESCOS NO DEPARTAMENTO DOS RECURSOS HUMANOS (DRH).

1 – escassez dos especialistas para projeto;

2 – Infiltração dos funcionários fantasmas;

3 – Emigração dos técnicos / especialistas para melhor mercado;

4 – Conflitos e interesses pessoais;

5 – Resistência em adaptar novos programas / modelos dos projetos.

AVALIAÇAO E ANALISE DOS RISCOS.

Análise preliminar de risco

A análise de risco é fundamental para a identificação de medidas de prevenção e preparação, com consequências importantes para a resposta a emergências.

1.DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇAO (DTI)

CODIGO DOS RISCOS DESCRIÇAO DOS RISCOS

R01	Queda de Internet
R02	Mao uso de hardware
R03	Circuito interno
R04	Acesso estranho a rede corporativo
R05	Desastres climáticos ou orquestrados
R06	Uso dos softwares não autorizado/ sem licença

1.1-QUANTIFICAÇAO DOS RISCOS IDENTIFICADOS

A severidade será calculada multiplicando-se a probabilidade pelo impacto, sendo seus valores baseados nas tabelas de valores abaixo, validadas com a equipe do projeto:

Probabilidade	valor
Muito alto	0,9
Alto	0,7
Moderado	0,5
Baixo	0,3
Muito baixo	0,1

Impacto	valor
Muito alto	0,8
Alto	0,3
Moderado	0,2
Baixo	0,1
Muito baixo	0,05

1.2-QUALIFICAÇAO DOS RISCOS IDENTIFICADOS CONSIDERANDO PROBABILIDADE & IMPACTO

Riscos	Probabilidade	Impacto
R01	Moderado	Alto
R02	Alto	Moderado
R03	Moderado	Muito alto
R04	Moderado	Moderado
R05	Baixo	Muito alto
R06	Moderado	Alto

1.3-VALOR DE CRITICIDADE

Risco	Probabilidade	Impacto	Criticidade	Qualificação
R01	Moderado	Alto	0,25	Moderado
R02	Alto	Moderado	0,14	Moderado
R03	Moderado	Muito alto	0,45	Alto
R04	Moderado	Moderado	0,10	Moderado
R05	Baixo	Muito alto	0,24	Moderado
R06	Moderado	Alto	0,15	Moderado

1.4-METODO DE RESPOSTA AOS RISCOS = MITIGAR; IMPEDIR; TRANFERIR e ACEITAR.

Riscos qualificação dos riscos método de respostas

R01	Alto	Mitigar
R02	Moderado	Mitigar
R03	Alto	Mitigar
R04	Moderado	Impedir
R05	Alto	Aceitar /Mitigar
R06	Moderado	Mitigar

2.DEPARTAMENTO DE FATURAMENTO E FINANÇAS (DAF)

CODIGO DOS RISCOS DESCRIÇAO DOS RISCOS

R01	Inflação
R02	Invasão da conta corporativa
R03	Falsificação dos cheques corporativos
R04	Quebra do banco/ falência
R05	Atrasos em pagamento das facturas.

2.1-QUANTIFICAÇAO DOS RISCOS IDENTIFICADOS

Probabilidade valor Impacto valor

Muito alto	0,9
Alto	0,7
Moderado	0,5
Baixo	0,3
Muito baixo	0,1

Muito alto	0,8
Alto	0,3
Moderado	0,2
Baixo	0,1
Muito baixo	0,05

2.2-QUALIFICAÇAO DOS RISCOS IDENTIFICADOS CONSIDERANDO PROBABILIDADE & IMPACTO

Riscos Probabilidade Impacto

R01	Alto	Alto
R02	Moderado	Muito alto
R03	Moderado	Muito alto
R04	Baixo	Alto
R05	Moderado	Alto

2.3-VALOR DE CRITICIDADE

Risco Probabilidade Impacto Criticidade Qualificação

R01	Alto	Alto	0,35	Alto
R02	Moderado	Muito alto	0,40	Alto
R03	Moderado	Muito alto	0,40	Alto
R04	Baixo	Alto	0,15	Moderado
R05	Moderado	Alto	0,25	Moderado

2.4-METODO DE RESPOSTA AOS RISCOS: MITIGAR; IMPEDIR; TRANFERIR; ACEITAR.

Riscos qualificação dos riscos método de respostas

R01	Alto	Aceitar
R02	Alto	Mitigar
R03	Alto	Mitigar
R04	Moderado	Mitigar
R05	Alto	Impedir

3.DEPARTAMENTO DE DESENVOLVIMENTO DOS PROJETOS (DDP)

COD. DOS RISCOS DESCRIÇAO DOS RISCOS

R01	Desfalque do gerente do projeto no pleno projeto.
R02	Desvio de verba de um projeto em andamento
R03	Atraso em desenvolvimento e entrega de um projeto.
R04	Perda de dados ou requisitos de um projeto.
R05	Fatores externos (climático, geográfico, econômica e política).
R06	Falta de colaboração na implementação de um projeto.

3.1QUANTIFICAÇAO DOS RISCOS IDENTIFICADOS

Probabilidade valor Impacto valor

Muito alto	0,9
Alto	0,7
Moderado	0,5
Baixo	0,3
Muito baixo	0,1

Muito alto	0,8
Alto	0,3
Moderado	0,2
Baixo	0,1
Muito baixo	0,05

3.2-QUALIFICAÇAO DOS RISCOS IDENTIFICADOS CONSIDERANDO PROBABILIDADE & IMPACTO

Riscos Probabilidade Impacto

R01	Moderado	Alto
R02	Baixo	Muito alto
R03	Alto	Muito alto
R04	Moderado	Muito alto
R05	Alto	Alto
R06	Moderado	Moderado

3.3-VALOR DE CRITICIDADE

Risco Probabilidade Impacto Criticidade Qualificação

R01	Moderado	Alto	0,25	Moderado
R02	Baixo	Muito alto	0,24	Moderado
R03	Alto	Muito alto	0,56	Muito alto
R04	Moderado	Muito alto	0,40	Alto
R05	Alto	Alto	0,35	Alto
R06	Moderado	Moderado	0,10	Moderado

3.4-METODO DE RESPOSTA AOS RISCOS: MITIGAR; IMPEDIR; TRANFERIR; ACEITAR.

Riscos qualificação dos riscos método de respostas

R01	Alto	Transferir
R02	Alto	Impedir
R03	Muito alto	Mitigar
R04	Alto	Mitigar
R05	Alto	Aceitar / Mitigar
R06	Moderado	Transferir

4. DEPARTAMENTO DOS RECURSOS HUMANOS (DRH)

CODIGO DOS RISCOS DESCRIÇAO DOS RISCOS

R01	Escassez dos especialistas para os projetos
R02	Infiltração dos funcionários fantasmas.
R03	Emigração dos especialistas/técnicos para melhor mercado.
R04	Conflitos e interesses pessoas.
R05	Resistência em adaptar novos programas/modelos de projetos.

4.1-QUANTIFICAÇAO DOS RISCOS IDENTIFICADOS

Probabilidade valor Impacto valor

Muito alto	0,9
Alto	0,7
Moderado	0,5
Baixo	0,3
Muito baixo	0,1

Muito alto	0,8
Alto	0,3
Moderado	0,2
Baixo	0,1
Muito baixo	0,05

4.2 - QUALIFICAÇAO DOS RISCOS IDENTIFICADOS CONSIDERANDO PROBABILIDADE & IMPACTO

Riscos Probabilidade Impacto

R01	Moderado	Alto
R02	Baixo	Moderado
R03	Moderado	Alto
R04	Alto	Alto
R05	Baixo	Moderado

4.3-VALOR DE CRITICIDADE

Risco Probabilidade Impacto Criticidade Qualificação

R01	Moderado	Alto	0,25	Moderado
R02	Baixo	Moderado	0,06	Baixo
R03	Moderado	Alto	0,25	Moderado
R04	Alto	Alto	0,35	Alto
R05	Baixo	Moderado	0,2	Muito baixo

4.4-METODO DE RESPOSTA AOS RISCOS: MITIGAR; IMPEDIR; TRANFERIR; ACEITAR.

Riscos qualificação dos riscos método de respostas

R01	Alto	Mitigar
R02	Baixo	Impedir
R03	Alto	Mitigar
R04	Alto	Mitigar
R05	Muito baixo	Aceitar

Terceira Etapa – Desenvolvimento do plano de resposta aos riscos

Resposta de riscos de TI

R01: Caso houver a queda da Internet, imediatamente deverá houver a verificação (motivo da queda). Se for provedor, abrir o chamado para provedor e se for o problema de hardware troca-lo imediatamente. Enquanto fica na espera de provedor será acionado o nosso segundo provedor para poder continuar numa situação normal.

R02: Caso acontecer a tragédia devido ao mão uso do equipamento, imediatamente fazer a troca da maquina e fazer backup de disco.

R03: Circuito Interno – ter extintor no lugar adequado, ter backup com capacidade de assegurar equipamento ligado nela durante um certo intervalo do tempo.

R04: Bloquear alguns site (site de relacionamento).

R05: Uso de dois servidores simultaneamente e hospedagem de dados nas nuvens.

R06: Ter especialistas internos de inspeção e auditoria da empresa.

RESPOSTA DE RISCOS DE DEPARTAMENTO DAS FINANÇAS

R01: INFLAÇÃO – sendo o risco que pode ser o positivo ou negativo, a empresa sempre terá o seu capital de giro para aplicar no momento positivo e terceirização nos momentos dos crises.

R02: As informações de transição coorporativa serão guardadas parcialmente pelos principais responsáveis da organização. Ao tentando uma transição todos receberão uma mensagem de pedido de confirmação da transição.

R03: Qualquer levantamento feito em cheque, só poderá ser efetuado totalmente com comprovação de cópias autenticados dos documentos das pessoas autorizadores.

R04: A empresa procurará fazer aplicações em ao menos dois bancos, e sempre a primeira opção será num banco federal ou estadual a principal opção será nunca deixar criar parcerias coorporativas profissionais.

R05: Primeiro plano será pagamento a tempo das faturas, e o segundo plano negociação das faturas atrasadas.

RESPOSTAS DOS RISCOS DE DEPARTAMENTO DE DESENVOLVIMENTO DOS PROJETOS.

R01: Trabalhar com gerente auxiliar com níveis balanceados do treinamento em relação ao gerente sênior.

R02: Criar uma parceria efetiva com agencia bancaria de deposito e credito, onde a organização poderá depositar e fazer creditos mediante a necessidade da empresa.

R03: Negociar a prorrogação e a data da entrega, e aceleração de produção do projeto.

R04: Fazer backup diariamente, e manter a redundância dos dados.

R05: Desenvolver projeto de acordo com legislação local respeitando padrões governamentais dando um treinamento adequado à equipe do projeto tendo em conta a situação sócio-ambiental.

RESPOSTA DOS RISCOS DO DEPARTAMENTO DOS RECURSOS HUMANOS.

R01: Aproveitar sempre os recursos positivos dos projetos passados selecionar as pessoas com experiências vividas na organização interna.

R02: O departamento dos recursos humanos criará um plano de treinamento seminários e palestras para todos os funcionários ligados a empresa ou a folha do pagamento da empresa isso acontecerá trimestralmente para ajudar na atualização de bancos de dados dos funcionários da empresa

R03: Para contingenciar esta situação será criada um plano de manutenção para os funcionários internos desenvolver e manter um modelo de conhecimento explicito e redundante, para no caso da ausência de um técnico será imediato a colocação do outro com o nível balanceado co conhecimento, sem prejudicar o andamento do projeto.

R04: Este risco é natural e faz parte de qualquer que seja organização, mas a GUISOLUÇÃO tem um plano para amenizar este risco. Sendo criar uma força tarefa “meu sonhos e minhas ações” que terá como objetivo estudar

conflitos e atender as necessidades de forma a criar um comprometimento mutua com a organização.

R05: Uma vez que a empresa trabalhará com serviços dos terceiros será muito comum se deparar com a situação da resistência dos usuários sobre o novo projeto. Se isso acontecer a GUISOLUÇÃO assumirá estes riscos oferecendo um treinamento sobre a integração do sistema, em simultaneamente com o desenvolvimento do mesmo.

QUARTA ETAPA: TESTE E MANUTENÇÃO

1 - Nesta etapa temos seguintes tarefas: Para começar a primeira tarefa, será feita a revisão de todos os riscos levantados. A seguir fazer um check list de todos os riscos, verificando detalhadamente se todos eles têm realmente um plano de resposta.

2 – Será pegar todos os planos simulando um caso de erro aplicando o plano de resposta previsto, concluindo se realmente esta contingência corresponderá com a falha e o seu tempo médio de retorno (TMR). Caso contrário toma-se novas medidas à viabilização do caso.

Observação: É de salientar que o nosso plano, será sujeito a manutenção conforme o desenvolvimento e o crescimento da demanda.

CONCLUSÃO

Do ponto de vista da equipe, durante o desenvolvimento deste trabalho conclui-se que as atribuições das responsabilidades vêm desde nos primórdios, e não deixou de prevalecer na nossa era da informática. Porem inter-relacionando o vídeo assistido na sala de aula, com a realidade empresarial, comprova-se que em cada tarefa ou a função empresarial sempre há de ter pessoas responsabilizadas para executar as mesmas por mais críticos, ou seja, sigilosos que ela é. Sempre é o homem o responsável fundamental para executa-las.

Nesta ótica vai se enquadrar a política de segurança e ética, as políticas, para regimentar e atribuir responsabilidades as pessoas executoras das tarefas. A pesar de tudo a ética é fundamental para que a política funcione.

FORMULÁRIO DE SOLICITAÇÃO USUÁRIO / ACESSO

Solicitação de Usuário / Acesso	Criação	(x)
	Renovação	( )
Usuário: João Luis RG / CPF: N° 623.152.154-76 Matricula: 20120712 Depto: Marketing. Função: Publicitário		
Responsável pela solicitação (nome/depto): Alciolina E. L. Furtado / Ger. Marketing		
Acesso dexter rede (diretório/pastas): 10.176.2.2\Publicidade \ Dexter 172.165.1.3\Eventos \ Dexter 192.168.56.46\ Entregas\ Dexter		
(x)Acesso Protheus Microsiga (perfis/funções):		
(x)Revogação de Acesso SGA (perfis/funções):		

MODELO

Solicitação de Bloqueio usuário / Revogação Acesso
Usuário: João Luis RG / CPF: N° 623.152.154-76 Matricula: 20120712 Depto: Marketing Cargo: Publicitário
Responsável pela solicitação (nome/depto): Alciolina E. L. Furtado
Revogação de Acesso Dexter rede (diretórios / pastas): Acesso dexter rede (diretório/pastas): 10.176.2.2\Publicidade \ Dexter 172.165.1.3\Eventos \ Dexter 192.168.56.46\ Entregas\ Dexter
(x)Acesso Protheus Microsiga (perfis/funções):
Revogação de Acesso SGA (perfis/funções):
(x) Revogação de Acesso e-mail (grupos): (x)Revogação de Acesso Internet
Data de solicitação pela área de negócios: 10/12/2011 Data de bloqueio / revogação pela área de TI: 07/12/2012 Responsável pelo Bloqueio / revogação: Demba Semedo Baldé

Solicitação de Bloqueio usuário Revogação / Acesso

_____

Usuario: _____

RG / CPF: N° _____

Matricula: _____

Depto: _____ Cargo: _____

Responsável pela solicitação (nome/depto):

( ) Revogação de Acesso dexter rede (diretório/pastas):

_____\\ Dexter

_____\\ Dexter

_____\\ Dexter

_____\\ Dexter

_____\\ Dexter

_____\\ Dexter

_____\\ Dexter

( ) Revogação de Acesso Protheus Microsiga (perfis/funções):

( ) Revogação de Acesso SGA (perfis/funções):

( ) Revogação de Acesso e-mail (grupos):

( ) Revogação de Acesso Internet:

Para uso da área de TI

Data de solicitação pela área de negócios: ___/___/20__

Data de Bloqueio/revogação pela área de TI: ___/___/20__

Responsável pelo Bloqueio/revogação:_____