ROSEMARY FRANCISCO

A IMPORTÂNCIA DE UM PLANO DE CONTINUIDADE DO NEGÓCIO NA ORGANIZAÇÃO

Trabalho de Conclusão de Curso submetida ao Instituto Superior Tupy como parte dos requisitos para a obtenção do grau de Bacharel em Sistemas de Informação com ênfase em redes, sob a orientação do professor Marcos Aurélio Pchek Laureano.

Joinville

2004

A IMPORTÂNCIA DE UM PLANO DE CONTINUIDADE DO NEGÓCIO NA ORGANIZAÇÃO

Rosemary Francisco

Este trabalho de conclusão de curso foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação com ênfase em redes, e aprovada em sua forma final pelo Departamento de..... do Instituto Superior Tupy.

Joinville, _____ de _____ de _____.

_____

Marcos Aurélio Pchek Laureano, Mestre em Informática Aplicada

_____

Marco André, Mestre em Ciência da Computação

Banca Examinadora:

_____

Mehran Misaghi, Mestre em Ciência da Computação

_____

Adriana Klemann Rohweder, Mestranda em Administração

Dedico este trabalho ao meu esposo Marcos e

minha família com muito amor e carinho.

AGRADECIMENTOS

Em especial, ao meu esposo Marcos que me deu todo o apoio necessário para o desenvolvimento deste trabalho.

A minha família e amigos, pela compreensão durante as minhas ausências.

Gostaria de agradecer ao professor Marcos Aurélio Pchek Laureano pelo compartilhamento de experiências e pelas suas orientações.

Aos meus colegas de trabalho, em especial ao Marcelo Motta Bastos que me ajudou com material e revisão do trabalho e a querida Rosane Strey, que me ensinou dicas valiosas para a elaboração do trabalho no editor do texto.

Quero agradecer também a todos os entrevistados na pesquisa de campo realizada neste trabalho.

E a todos os professores do IST que colaboraram para a minha formação durante estes quatro anos de estudo.

RESUMO

A continuidade é um fator muito importante que tem contribuído em grande escala para que a organização torne-se competitiva, característica considerada a chave para o reconhecimento público e, por conseguinte, sucesso de uma organização. Porém adquirir e manter esta característica exigirá um grande esforço de todas as pessoas envolvidas, independente de seu nível hierárquico, tanto dentro quanto fora da organização.

Este esforço estará sempre direcionado para a preparação, planejamento e execução das estratégias da organização a fim de garantir a fidelidade dos clientes já conquistados e também proporcionar novas oportunidades de mercado.

Garantir a continuidade então, deve ser encarado como um dos itens necessários para a sobrevivência de uma organização dentro deste mercado global.

Desta forma, o presente trabalho tem como objetivo realizar o estudo e a análise da importância de um PCN – Plano de Continuidade do Negócio – para as organizações, assim como, sua viabilidade de implantação.

Palavras-chave: Plano de Continuidade do Negócio, Plano de Contingência, Plano de Recuperação de Desastres, Prevenção de Ameaças

ABSTRACT

Continuity is an extremely important factor which has contributed on a great scale to an organization becoming competitive, a feature held to be key for public recognition and, consequently, the success of an organization. However, to acquire and maintain this feature will require a big effort by all the people involved, regardless of their hierarchical level, both inside and outside the organization.

This effort will be directed towards preparing, planning and executing the strategies of the organization in order to ensure the loyalty of the customers already conquered and also provide new market opportunities.

So, ensuring continuity must be seen as one of the items required for the survival of an organization in the global market.

Thus, the present paper aims to study and analyze the importance of a BCP – Business Continuity Plan – for organizations, as well as how feasible it is to implement.

Key words: Business Continuity Plan, Contingency Plan, Disaster Recovery Plan, Prevention of Threats

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

1 INTRODUÇÃO

A informação sempre teve grande importância para a realização dos grandes feitos da humanidade. Além disso, foi por intermédio dela que a evolução tecnológica tornou-se possível e está cada vez mais inovadora e abrangente atualmente.

A partir do momento que o processo de globalização tornou-se constante, e em razão disso, a ocorrência de grandes mudanças na economia mundial, o grau de importância da informação cresceu rapidamente, possibilitando muitas vantagens e benefícios àquele que a possuísse. Porém, isso fez com que o nível de competição entre as organizações aumentasse consideravelmente, e a busca pela informação se tornasse fator primordial de sobrevivência.

Em função destes eventos e levando em consideração que obter uma certa informação poderia repercutir em grandes vantagens e competitividade à organização, a preocupação com a segurança da informação tem crescido constantemente. Tornou-se imprescindível possibilitar a organização gerar, manipular e armazenar suas informações de forma segura. Por meio desta necessidade, surgiu então o processo de Segurança da Informação, meio pelo qual se torna possível a proteção das informações mantendo-as íntegras, confidenciais e disponíveis quando necessário.

Assim, a função do processo de Segurança da Informação é proteger todos os dados e informações da organização de possíveis perdas e manipulação incorreta. Porém, para que isso seja possível, é necessário que a organização invista em tecnologia e tenha conhecimento de quais são as informações estratégicas imprescindíveis para o funcionamento de seus principais processos. Também é importante que organização conheça o mercado e avalie quais os possíveis

riscos que a perda destas informações e conseqüentemente o conhecimento adquirido, ameaçam a continuidade de seu negócio.

Analisando este cenário, é possível perceber que as organizações estão cada vez mais dependentes da tecnologia. A tecnologia se tornou uma parte fundamental tanto para a geração, quanto para a devida proteção das informações. Esta dependência tecnológica pode trazer grandes problemas, pois se a organização não possuir um bom planejamento para contornar uma interrupção em um processo crítico, causado pela falta ou funcionamento inadequado de algum equipamento de suporte ao processo, as perdas podem tornar-se irreversíveis. E é neste contexto que surge a importância da utilização de um PCN – Plano de Continuidade do Negócio. O objetivo do PCN é a garantia da continuidade dos seus processos, minimizando assim o impacto que uma interrupção poderia trazer ao negócio da organização.

Este trabalho tem por objetivo demonstrar a importância de um PCN dentro da organização, assim como as atividades necessárias para a sua elaboração.

1.1 TEMA, QUESTÕES E OBJETIVOS DO TRABALHO

O Plano de Continuidade de Negócio foi escolhido como tema para o desenvolvimento deste trabalho, pois é uma prática ainda muito recente no Brasil. Apesar de sua grande importância, ainda existem organizações que desconhecem o seu significado. E mesmo aquelas que já estão mais interadas ao tema, ainda não estão totalmente preparadas para dar continuidade ao seu negócio caso ocorra algum problema ou desastre no seu ambiente produtivo.

Com base neste cenário, foram levantadas algumas hipóteses que estarão sendo abordadas no trabalho:

- As empresas estão cada vez mais dependentes dos sistemas e toda a tecnologia que os envolvem;
- Ao ocorrer um desastre, existe um grande potencial de perdas;
- No Brasil a preocupação com este planejamento é muito pequeno, devido algumas das ameaças serem ocasionais;
- Poucas empresas têm alocado verbas adequadas para estabelecer a redundância dos elementos de TI (dados, sistemas, redes, etc.) necessários à continuidade dos seus processos de negócios;
- Um plano de continuidade deve garantir a recuperação dos dados críticos;
- Um plano de continuidade exige investimento, tanto de recursos físicos quanto humanos;
- A empresa se torna mais competitiva quando possui um plano de continuidade do seu negócio.

Desta forma, constituí-se objetivo específico deste trabalho demonstrar que a melhor forma de possibilitar a continuidade do negócio da organização após uma contingência é através de um bom planejamento. Com um planejamento bem elaborado, preparado e testado a organização obterá sucesso na execução dos procedimentos de recuperação e continuidade necessários para mantê-la sempre ativa.

1.2 IMPORTÂNCIA DO TRABALHO

Por meio deste trabalho será possível demonstrar a importância de um plano de continuidade de negócios (PCN – Plano de Continuidade do Negócio) que tem por objetivo garantir a operação da organização com o mínimo impacto aos clientes em situações de contingência. Uma vez implantado o plano, é importante que as organizações também exijam de seus parceiros e principais fornecedores o plano de continuidade para que uma possível ameaça não afete seu negócio por estarem relacionados.

1.3 ORGANIZAÇÃO DO TRABALHO

O presente trabalho está dividido em seis capítulos. O primeiro capítulo define brevemente os objetivos do trabalho e as razões de sua elaboração.

O segundo capítulo apresenta uma breve introdução ao tema Segurança da Informação e seus princípios básicos.

No terceiro capítulo são abordadas a análise de riscos e duas metodologias que podem ser utilizadas para sua devida aplicação.

O detalhamento sobre o Plano de Continuidade do Negócio, o que é, para que serve e quais os padrões existentes para sua elaboração, serão tratados no quarto capítulo.

No quinto capítulo apresentam-se a importância do estudo sobre PCN, o resultado de uma pesquisa de campo realizada com empresas da região e um modelo guia para auxiliar na elaboração do plano dentro das organizações.

Por fim no sexto capítulo são apresentadas as considerações finais do trabalho, suas contribuições e sugestão de trabalhos futuros.

2 SEGURANÇA DA INFORMAÇÃO

2.1 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Existem diversas definições para informação, a que melhor se adapta à nossa área é a definição da Norma NBR ISO/IEC 17799:2001:

> "Informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegido."

Baseando-se nesta definição, é possível afirmar que a informação é a chave para o desenvolvimento e sucesso de uma organização e sua falta ou manipulação indevida pode acarretar em sérios problemas. Assim é muito importante que a informação esteja segura e sempre disponível dentro do seu ambiente para que possa realmente auxiliar no processo de desenvolvimento da organização.

Segundo a definição obtida pelo Dicionário Aurélio (1999, p. 1829) segurança é:

> Segurança. S. f. 2. Estado, qualidade ou condição de seguro. 3. Condição daquele ou daquilo em que se pode confiar. 4. Certeza, firmeza, convicção.

> Seguro. [Do lat. securu.] Adj. 1. Livre de perigo. 2. Livre de risco; protegido, acautelado, garantido. 8. Em quem se pode confiar. 9. Certo, indubitável, incontestável. 10. Eficaz, eficiente.

Desta forma, a Segurança da Informação protege a informação de uma gama extensiva de ameaças para assegurar a continuidade dos negócios, minimizar os danos empresariais e maximizar o retorno em investimentos e oportunidades.

Para garantir a Segurança da Informação, é necessário que os seguintes princípios básicos sejam respeitados (ISO/IEC 17799:2001):

- **Confidencialidade**: significa proteger informações contra sua revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.
- **Autenticidade**: O controle de autenticidade está associado com identificação correta de um usuário ou dispositivo. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital, sendo possível também utilizar cartões. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário, de um sistema para outro sistema ou de um usuário para outro usuário. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos.

- **Integridade**: A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como: escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de backup. Integridade significa garantir que o dado está lá, não foi corrompido, portanto encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada de mensagens (ex. tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade).
- **Disponibilidade**: consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

Através da correta aplicação desses princípios, a segurança da informação pode trazer benefícios como: aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e, finalmente garantir a funcionalidade das aplicações críticas da empresa.

2.2 AMEAÇAS

Os sistemas de informação e redes das organizações estão expostos a ameaças de várias origens como fraudes, espionagem, sabotagem, vandalismo, incêndio e inundação. Outras origens como vírus, *hacking* e ataques de paralisação de serviços estão se tornando cada vez mais comuns e sofisticados (NAKAMURA, 2002).

A dependência dos sistemas de informação significa que as organizações estão cada vez mais vulneráveis às ameaças de segurança. A interconexão entre redes públicas e privadas e o compartilhamento de recursos aumenta a dificuldade do processo de controle ao acesso. Desta forma, é imprescindível que as organizações estejam atentas aos tipos de ameaças que podem ocorrer dentro do seu ambiente cooperativo para poder prevenir possíveis ataques.

A figura 2.1 ilustra bem essa afirmação referente o nível de incidentes de segurança que ocorreram entre os anos de 1999 e 2004.

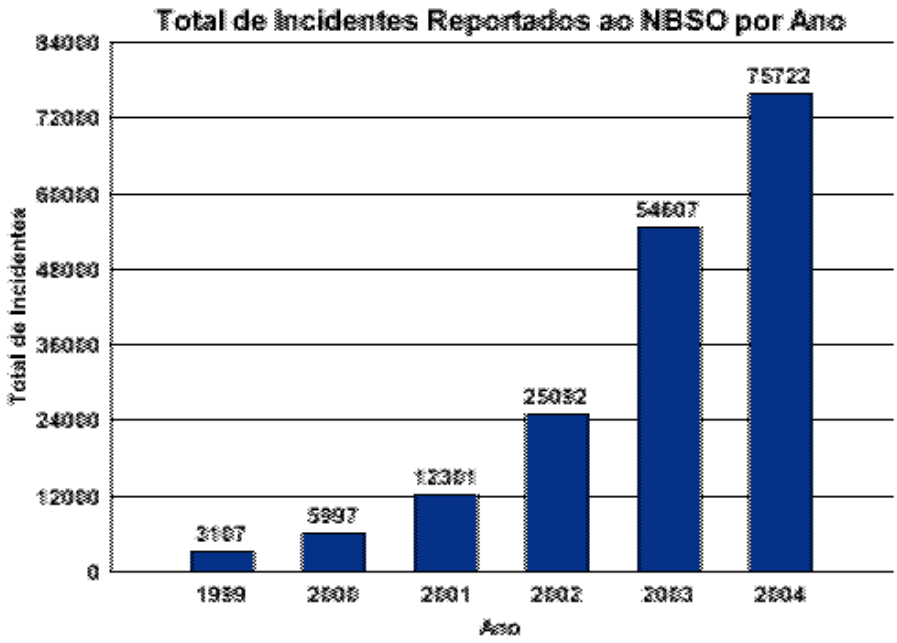


Figura 2.1 – Gráfico Incidentes de Segurança (Fonte: NBSO)

2.2.1 Ameaças Internas

De acordo com NAKAMURA (2002, p. 41), a concretização de uma ameaça interna resulta em um maior prejuízo para a organização do que a concretização de uma ameaça externa. Esta afirmação pode ser comprovada, pois uma ameaça interna em sua grande maioria resulta em roubo e/ou perda de propriedade intelectual.

A nona pesquisa nacional de segurança da informação realizada pelo Módulo Security Solutions demonstra que incidentes como: Vírus (66%), funcionários insatisfeitos (53%), divulgação de senhas (51%), acessos indevidos (49%) e vazamento de informações (47%) são as cinco principais ameaças internas à segurança das informações nas empresas.

Assim, as organizações devem estar atentas para poder evitar que estes tipos de ataques ocorram. Para isso são necessárias algumas medidas de proteção, das quais podemos destacar as mais importantes (NAKAMURA, 2002 p. 100):

- A segurança é mais importante do que os serviços. Caso não haja conciliação, a segurança deve prevalecer, a não ser que os executivos assumam formalmente os eventuais riscos existentes.
- A política de segurança deve evoluir constantemente, de acordo com os riscos e as mudanças na estrutura da organização.
- Aquilo que não for expressamente permitido será proibido. O ideal é restringir tudo, e os serviços só poderão ser liberados caso a caso, de acordo com a sua análise e a dos riscos relacionados.

- Devem ser realizados testes, a fim de garantir que todos os objetivos sejam alcançados.
- Nenhuma senha deve ser fornecida ‘em claro’, ou seja, sem a utilização de algum método de proteção.
- As informações utilizadas na computação móvel, principalmente em notebooks, deve ser cifradas.

No tópico 2.4 serão abordados outras formas de defesa para as ameaças ao ambiente corporativo.

2.2.2 Ameaças Externas

As ameaças externas, como o próprio nome já menciona, são àquelas relativas a incidentes ou ataques realizados de fora para dentro da organização. De acordo com a nona pesquisa nacional de segurança da informação realizada pelo Módulo Security Solutions, 60% das organizações indicam a Internet, e por conseqüência o seu crescimento, como a principal ameaça externa aos seus sistemas e informações.

Estas invasões podem ser executadas por meio da exploração de vulnerabilidades dos sistemas que podem ter como base a engenharia social ou invasões técnicas. A engenharia social será melhor discutida no tópico 2.3. Geralmente estes tipos de invasões exploram deficiências na concepção, implementação, configuração ou no gerenciamento dos serviços e sistemas, e continuarão existindo na medida em que o mercado é centrado nas características dos produtos, e não segurança (NAKAMURA, 2002 p. 51).

De acordo com NAKAMURA (2002, p. 40), o termo genérico para identificar quem realiza o ataque em um sistema computacional é *hacker*. Essa generalização, porém, tem diversas ramificações, já que os ataques aos sistemas apresentam objetivos diferentes, e o seu sucesso depende do grau de segurança dos alvos, ou seja, os sistemas bem protegidos são mais difíceis de serem atacados, exigindo desta forma, mais habilidade do invasor. Uma classificação dos diversos tipos de invasores podem ser a seguinte:

- **Script Kiddies** - Iniciantes.
- **Cyberpunks** – Mais experientes que os *script kiddies*. Dedicam-se às invasões de sistemas por puro divertimento e desafio.
- **Insiders** – Empregados insatisfeitos.
- **Coders** – são aqueles que resolveram compartilhar seus conhecimentos escrevendo livros ou proferindo palestras e seminários sobre suas proezas.
- **White Hat** – utilizam seus conhecimentos para descobrir vulnerabilidades nos sites e aplicar as correções necessárias.
- **Black Hat** – utiliza seus conhecimentos para invadir sistemas e roubar informações secretas das organizações.
- **Gray Hat** – geralmente trabalham na área de segurança, pois possuem conhecimento sobre atividades de *hacking*.

A lista de ameaças mais comuns utilizadas pelos invasores são (NAKAMURA, 2002):

- **Ataques do tipo DoS – *Denial of Service*:** ataques crescentes de negação de serviços, tais como "*Ping of Death*", "*SYN Flood*" e "*Land Atack*" não visam roubar informação, mas incapacitar um dispositivo ou toda a rede para que os usuários não tenham mais acesso aos recursos. Até mesmo se a rede não está

sendo atacada, ela pode ser usada como um aliado inconsciente em ataques DoS em outras redes. Usando os "Trojan Horse" ou outros anexos, invasores "plantam" ferramentas em centenas e em até milhares de computadores para serem usados em ataques futuros.

- **Vírus:** programas destrutivos que se anexam aos e-mails, aplicações e arquivos. Também podem ser usados como "entregadores" de ferramentas de invasores, colocando em dúvida a segurança da organização, mesmo havendo um firewall instalado.
- **Captura de dados privados que transitam pela Internet:** conforme os dados privados se movem pela Web, os invasores, que usam programas chamados "farejadores de pacotes" ou "sniffers", podem capturá-los e convertê-los em um formato legível.

2.3 ENGENHARIA SOCIAL

A engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas, assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização. Essa técnica explora o fato de os usuários estarem sempre dispostos a ajudar e colaborar com os serviços da organização (NAKAMURA, 2002).

Um ataque de engenharia social clássico consiste em se fazer passar por um alto funcionário que tem problemas urgentes de acesso ao sistema. O *hacker*, assim, é como um ator, que, no papel que está representando, ataca o elo mais fraco da segurança de uma organização, o

ser humano. Esse ataque é difícil de ser identificado, pois o que está em jogo é a confiança, a psicologia e a manipulação das pessoas (NAKAMURA, 2002).

2.4 DEFESAS

2.4.1 Política de Segurança

A política de segurança é a base para todas as questões relacionadas à segurança de qualquer organização. O seu desenvolvimento é o primeiro e o principal passo da estratégia de segurança das organizações; e é por meio dessa política que são definidos todos os aspectos envolvidos na proteção dos recursos existentes.

Com uma política de segurança bem definida é possível evitar muitos problemas, pois ela trata de aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos de negócios. Desta forma é muito importante ao desenvolvê-la que os responsáveis tenham o conhecimento dos diversos aspectos de segurança, além da familiarização com as questões culturais, sociais e pessoais que envolvem o bom funcionamento da organização.

2.4.2 Firewall

A mais antiga definição para *firewall* foi dada por Bill Cheswick e Steve Bellovin, em *Firewalls Internet Security: Reppling the Wily Hacker*. Segundo eles, *firewall* é um ponto entre

duas ou mais redes, no qual circula todo o tráfego, além de registrar, por meio de *logs*, todo o tráfego da rede, facilitando assim sua auditoria.

Com base nessa definição, pode-se dizer que *firewall* é um ponto entre duas ou mais redes, que pode ser um componente ou um conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados (NAKAMURA, 2002). Assim, esse ponto único constitui um mecanismo utilizado para proteger, geralmente, uma rede confiável de uma rede pública não-confiável.

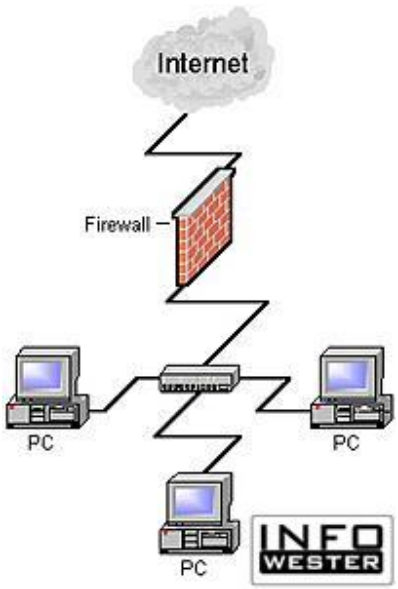


Figura 2.2 - Funcionamento do Firewall (Fonte: INFOWESTER)

Destacam-se dois grandes grupos de *firewalls*:

- ***Firewalls* baseado em filtragem de pacotes:** Utiliza endereços IP e portas de acesso para, através de um conjunto de regras estabelecidas pelo administrador, bloquear ou permitir o tráfego entre duas redes, geralmente a Internet.

- ***Firewalls* baseados em aplicações:** Os *firewalls* baseados em aplicações trabalham como se fosse um intermediador nas comunicações entre duas redes. Verifica as requisições provenientes de usuários remotos e bloqueia ou não a sua utilização. O cliente e o servidor não conversam diretamente, o servidor *proxy* intermedia a conexão e analisa de acordo com as regras definidas, a autorização para a conexão, permitindo ou bloqueando.

2.4.3 Sistema de detecção de intrusões - SDI

O SDI é capaz de detectar e alertar os administradores quanto a possíveis ataques ou comportamentos anormais na organização. Informações importantes sobre tentativas de ataques, que não se pode obter normalmente, podem ser conseguidas por meio desses sistemas. Elas podem oferecer subsídios suficientes para que a organização melhore sua proteção contra quaisquer tipos de ataque, principalmente os considerados internos.

2.4.4 Criptografia

A criptografia é uma ciência que tem importância fundamental para a segurança, ao servir de base para diversas tecnologias e protocolos, tais como a *Public Key Infrastructure* (PKI) e o *IP Security* (IPSec). Suas propriedades – confidencialidade, integridade, autenticação e não-repúdio – garantem o armazenamento, as comunicações e as transações seguras, essenciais no mundo atual (NAKAMURA, 2002 p.165).

Quando se fala sobre criptografia, fala-se também sobre chaves, pois são elas quem fecham e abrem a criptografia dos dados. Existem dois métodos para se trabalhar com chaves criptográficas, eles são:

- **Criptografia de chaves simétricas:** É responsável pela confidencialidade das informações, por meio da utilização de chave secreta para a codificação e decodificação dos dados. Os algoritmos de chave simétrica têm como característica a rapidez de sua execução, porém eles não permitem a assinatura e a certificação digitais (NAKAMURA, 2002 p. 166). A figura 2.2 ilustra o funcionamento de criptografia com utilização de chaves simétricas.

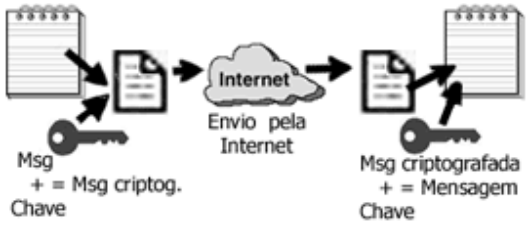


Figura 2.3 - Criptografia de chave simétrica (Fonte: SANTOS)

- **Criptografia de chaves assimétricas:** A criptografia de chave pública ou criptografia assimétrica possibilita, além da confidencialidade, integridade e não-repúdio, a autenticidade por meio da assinatura digital e da certificação digital. As comunicações são realizadas por meio de dois pares de chaves diferentes, uma chave privada e uma chave pública para cada entidade. Uma mensagem, por exemplo, pode ser cifrada utilizando-se uma chave pública, e decifrada utilizando-se a chave privada correspondente, ou vice-versa. Esse tipo de algoritmo, porém, é cerca de 60 a 70 vezes mais lento do que os algoritmos simétricos

(NAKAMURA, 2002 p. 166). A figura 2.3 ilustra o funcionamento de criptografia com utilização de chaves assimétricas.

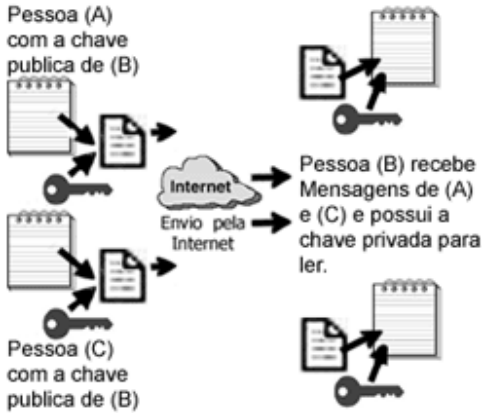


Figura 2.4 - Criptografia de chaves assimétricas (Fonte: SANTOS)

2.5 CONCLUSÃO

A informação tem sido um dos fatores principais para o bom desenvolvimento do negócio das organizações no mercado atual, pois por meio da sua correta manipulação é gerado o conhecimento necessário para o planejamento e execução das estratégias de sucesso.

Assim é muito importante que as informações estejam protegidas de acordo com os princípios básicos da segurança: Confidencialidade, Autenticidade, Integridade e Disponibilidade.

Este capítulo teve por objetivo demonstrar a importância da segurança da informação, as possíveis ameaças que as organizações e suas informações estão sujeitas e os tipos de defesas que podem ser aplicados para minimização e / ou eliminação da ocorrência destas ameaças.

3 ANÁLISE DE RISCOS

3.1 CONCEITOS

Risco é um evento ou condição incerta que, se acontecer, tem um efeito positivo ou negativo para a segurança da informação da empresa (PMBOK 2000, p.127).

Segundo a definição obtida pelo Dicionário Aurélio risco é (1999, p. 1772):

> Risco: s. m., perigo, inconveniente, probabilidade de perigo; em risco de: em perigo de.

De acordo com estas definições, é possível afirmar então que o risco é uma incerteza. Esta incerteza, na maioria das vezes, tem resultado negativo e, portanto é necessário que as empresas conheçam os riscos que podem dificultar ou impossibilitar o bom desempenho de seu negócio.

Assim, para avaliar e conhecer os riscos que podem ocorrer é necessário que a empresa saiba qual é o valor da informação, ou seja, qual seria a conseqüência no caso da falta ou perda desta informação para o negócio da empresa. Uma vez quantificado o valor de uma informação, devem ser levantados os meios em que esta se encontra, tanto armazenada quanto em trânsito, e delimitado o escopo de atuação. Este escopo deve estar focado no que realmente é significativo para a empresa, pois desta forma será possível gerenciar os riscos de uma melhor maneira.

Com o escopo de atuação definido, é possível aplicar a Análise e o Gerenciamento de Riscos. De acordo com a norma ISO/IEC 17799:2001, as definições para Análise ou Avaliação de Riscos e Gerenciamento de Riscos são:

> Avaliação de Riscos: avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência.
>
> Gerenciamento de Riscos: processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

Com base na definição da norma, é possível concluir que a Análise de Riscos tem por objetivo identificar os riscos de segurança presentes na empresa, fornecendo conhecimento para que sejam implementados controles eficazes de segurança.

Já o Gerenciamento de Riscos, diminui o efeito dos riscos, porém de acordo com Vargas (2001, p. 115) não é possível eliminar a ocorrência dos riscos. É possível identificá-los e planejar para que tenha uma aceitação razoável na medida em que o risco aparece.

3.2 GERENCIANDO RISCOS

A Análise de Risco se divide em cinco partes de igual importância, isoladas estas partes representam muito pouco ou quase nada. Alinhados e geridos de forma adequada, estes componentes da análise de risco podem apontar caminhos seguros na busca ao nível adequado de segurança de uma empresa. Os cinco pontos são (RAMOS, 2002):

- **Identificação e Classificação dos Processos de Negócio:** Identificar junto aos gestores e colaboradores os Processos de Negócio existentes na empresa.
- **Identificação e Classificação dos Ativos:** Identificar os ativos que serão considerados na Análise de Risco: Pessoas, Infra-estrutura, Aplicações, Tecnologia e informações.

- **Análise de Vulnerabilidades:** Identificar as vulnerabilidades existentes nos ativos que possam causar indisponibilidade dos serviços ou serem utilizadas para roubo das suas informações.
- **Análise de Ameaças e Danos:** Identificar os agentes que podem vir a ameaçar a empresa.
- **Análise de Impacto:** Tendo identificado as vulnerabilidades e ameaças, é identificado o impacto que estes podem causar na empresa, como roubo de informação, paralisação de serviços, perdas financeiras entre outros.

Uma Análise de Risco bem realizada dará informações à empresa para garantir a confidencialidade, disponibilidade e integridade das suas informações. Utiliza-se como métrica as melhores práticas de segurança da informação do mercado, apontadas na norma ISO/IEC 17799/2001. A partir destas informações faz-se possível à elaboração do perfil de risco, que segue a fórmula:

(Ameaça) x (Vulnerabilidade) x (Valor do Ativo) = RISCO.

A Análise de Riscos deve ser um processo contínuo dentro da empresa. A figura 3.1 ilustra o modelo padrão para a realização deste processo:

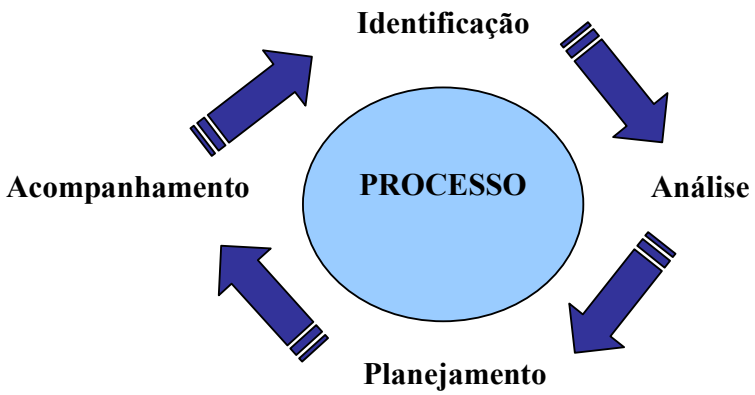


Figura 3.1 - Processo da Análise de Riscos

A primeira etapa de qualquer projeto de segurança é definir os riscos que precisam ser tratados. Os riscos de segurança são uma combinação dos ativos, das ameaças que podem afetá-los e das vulnerabilidades desses ativos que podem ser exploradas de alguma maneira. A adoção dessa etapa no processo de Análise de Riscos ajuda a estabelecer um conjunto de riscos de segurança que podem ser adequadamente analisados e priorizados. Os passos que são aplicados nesta etapa são (MICROSOFT):

- **Priorização dos ativos –** classificação dos ativos por valor financeiro, custo para criação, custo para proteção, custo para recuperação e seu valor perante a concorrência.
- **Estabelecer os valores dos ativos** - determinar o valor do ativo, levando em conta vários itens, como o valor físico e o valor comercial dos dados localizados nesses ativos.

- **Identificar a probabilidade das ameaças sobre os ativos** – determinação da probabilidade de uma ameaça em potencial ocorrer. A tabela 3.1 demonstra um exemplo de como analisar as probabilidades de ameaças.

Tabela 3.1 - Exemplo de Probabilidades de Ameaça (Fonte: MICROSOFT)

Ameaça	Probabilidade
Incêndio	0,05
Inundação	0,025
Vento	0,025
Terremoto	0,001
Falta de Energia	0,0002
Falta de hardware	0,1
Falta da rede	0,3
Usuários desinformados	0,2
Código mal-intencionado (vírus)	0,6
Espiões industriais	0,1
Atacantes internos	0,6
Atacantes externos	0,4

Na segunda etapa do processo, com base nas informações coletadas na primeira etapa, será feita uma análise de cada vulnerabilidade por meio de vários critérios. Essa etapa ajuda a determinar o risco geral ao qual a organização está exposta, de acordo com cada ameaça. Para isso, geralmente é feita uma declaração concisa de risco referente a cada combinação de atacante, exploração, vulnerabilidade e ativo. Os passos que são aplicados nesta etapa são (MICROSOFT):

- **Declaração dos riscos** – descrição das conseqüências específicas de cada risco

- **Definição dos fatores de criticidade** – medida do dano que uma determinada exploração pode causar a um ativo utilizando a vulnerabilidade em questão
- **Determinar o esforço para explorar as vulnerabilidades identificadas** - o esforço é a quantidade de trabalho, conhecimentos ou experiência de que um atacante necessita para utilizar uma determinada exploração. O nível de esforço para utilizar a exploração específica deve ser medido pela simplicidade do ataque.
- **Determinar fatores de vulnerabilidade** - o fator de vulnerabilidade é a medida da susceptibilidade a uma determinada forma de ataque

Na etapa de planejamento, é desenvolvido um plano para administração e monitoramento dos riscos. Através deste plano, será possível atribuir responsabilidades, definir planos de contenção para reduzir a ocorrência do risco e definir planos de contingência para redução do efeito de um risco.

Por fim, na etapa de acompanhamento, será feito o monitoramento da ocorrência dos riscos com base no plano definido na etapa de planejamento, a fim de garantir que os passos previstos sejam realizados. Além disso, como nesta etapa é feito um monitoramento da ocorrência de possíveis riscos, novas informações de ameaças não previstas no plano estabelecido serão levantadas para que o processo de Análise de Riscos tenha sua continuidade e garanta a segurança da informação à empresa.

3.3 MÉTODOS PARA GERÊNCIA DE RISCOS

Existem diversas abordagens que auxiliam na aplicação da Gerência de Risco dentro da empresa. Embora tenham características próprias, cada abordagem tem alguns princípios e atividades em comum.

Nessa seção serão analisadas as diferentes perspectivas das atividades que compõem o processo de gerência de risco. As normas e modelos serão apresentados segundo a visão do PMBOK - Project Management Body of Knowledge - e segundo o MSF - Microsoft Solutions Framework.

3.3.1 Gerência de risco no PMBOK - Project Management Body of Knowledge

O PMI - Instituto de Gerência de Projetos (Project Management Institute) tem definido como prática essencial da gerência de projetos a execução do processo de gerência de riscos (PMI MG, 2000). O Gerenciamento dos Riscos é um processo sistemático de identificar, analisar e responder aos riscos do projeto. Isso inclui maximizar a probabilidade e conseqüência de eventos positivos e minimizar a probabilidade e conseqüência de eventos adversos aos objetivos do projeto.

A figura 3.2 fornece uma visão geral dos principais processos aplicados no gerenciamento de riscos:

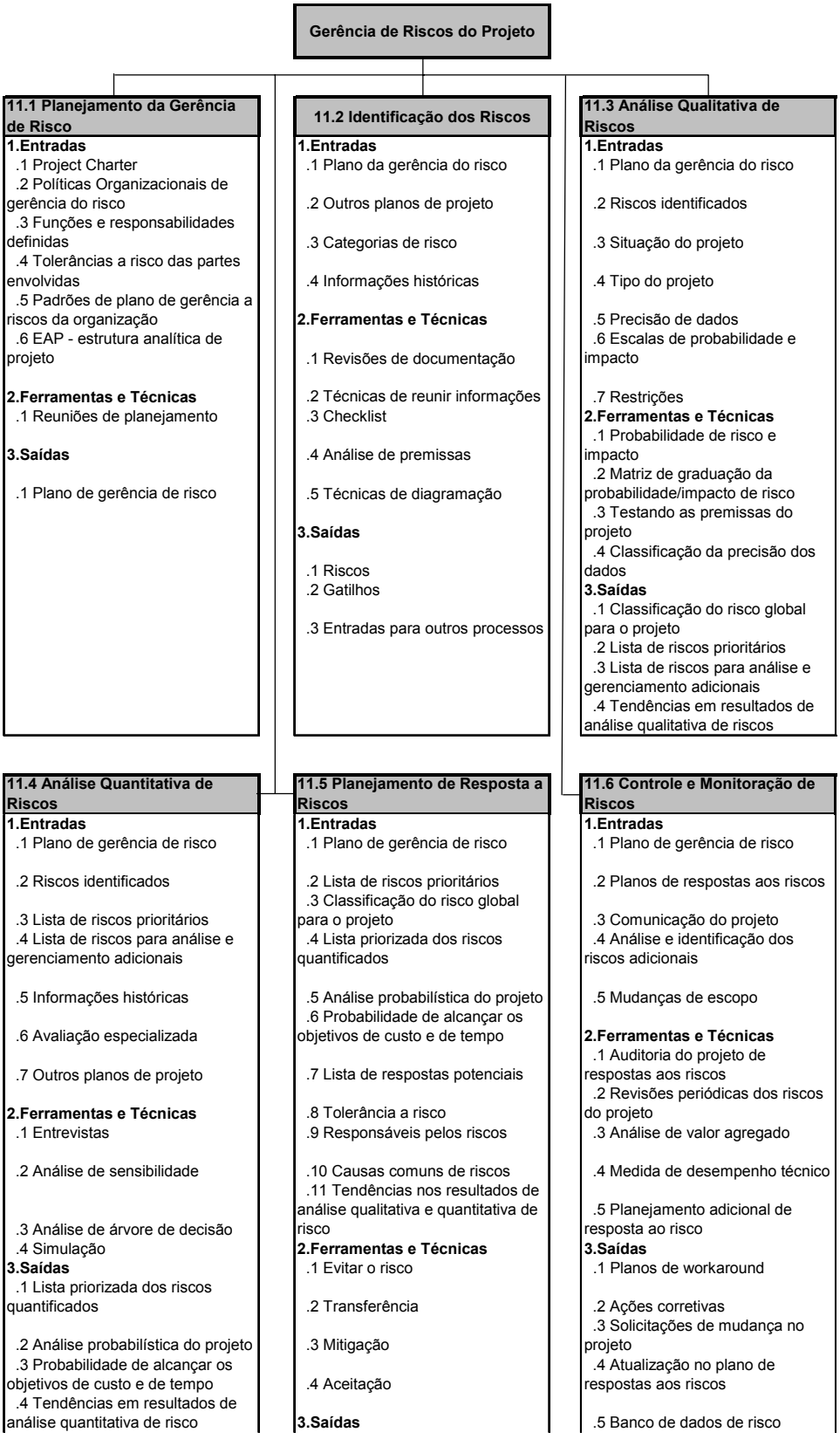

Gerência de Riscos do Projeto
11.1 Planejamento da Gerência de Risco
1.Entradas
.1 Project Charter
.2 Políticas Organizacionais de gerência do risco
.3 Funções e responsabilidades definidas
.4 Tolerâncias a risco das partes envolvidas
.5 Padrões de plano de gerência a riscos da organização
.6 EAP - estrutura analítica de projeto
2.Ferramentas e Técnicas
.1 Reuniões de planejamento
3.Saídas
.1 Plano de gerência de risco
11.2 Identificação dos Riscos
1.Entradas
.1 Plano da gerência do risco
.2 Outros planos de projeto
.3 Categorias de risco
.4 Informações históricas
2.Ferramentas e Técnicas
.1 Revisões de documentação
.2 Técnicas de reunir informações
.3 Checklist
.4 Análise de premissas
.5 Técnicas de diagramação
3.Saídas
.1 Riscos
.2 Gatilhos
.3 Entradas para outros processos
11.3 Análise Qualitativa de Riscos
1.Entradas
.1 Plano da gerência do risco
.2 Riscos identificados
.3 Situação do projeto
.4 Tipo do projeto
.5 Precisão de dados
.6 Escalas de probabilidade e impacto
.7 Restrições
2.Ferramentas e Técnicas
.1 Probabilidade de risco e impacto
.2 Matriz de graduação da probabilidade/impacto de risco
.3 Testando as premissas do projeto
.4 Classificação da precisão dos dados
3.Saídas
.1 Classificação do risco global para o projeto
.2 Lista de riscos prioritários
.3 Lista de riscos para análise e gerenciamento adicionais
.4 Tendências em resultados de análise qualitativa de riscos
11.4 Análise Quantitativa de Riscos
1.Entradas
.1 Plano de gerência de risco
.2 Riscos identificados
.3 Lista de riscos prioritários
.4 Lista de riscos para análise e gerenciamento adicionais
.5 Informações históricas
.6 Avaliação especializada
.7 Outros planos de projeto
2.Ferramentas e Técnicas
.1 Entrevistas
.2 Análise de sensibilidade
.3 Análise de árvore de decisão
.4 Simulação
3.Saídas
.1 Lista priorizada dos riscos quantificados
.2 Análise probabilística do projeto
.3 Probabilidade de alcançar os objetivos de custo e de tempo
.4 Tendências em resultados de análise quantitativa de risco
11.5 Planejamento de Resposta a Riscos
1.Entradas
.1 Plano de gerência de risco
.2 Lista de riscos prioritários
.3 Classificação do risco global para o projeto
.4 Lista priorizada dos riscos quantificados
.5 Análise probabilística do projeto
.6 Probabilidade de alcançar os objetivos de custo e de tempo
.7 Lista de respostas potenciais
.8 Tolerância a risco
.9 Responsáveis pelos riscos
.10 Causas comuns de riscos
.11 Tendências nos resultados de análise qualitativa e quantitativa de risco
2.Ferramentas e Técnicas
.1 Evitar o risco
.2 Transferência
.3 Mitigação
.4 Aceitação
3.Saídas
11.6 Controle e Monitoração de Riscos
1.Entradas
.1 Plano de gerência de risco
.2 Planos de respostas aos riscos
.3 Comunicação do projeto
.4 Análise e identificação dos riscos adicionais
.5 Mudanças de escopo
2.Ferramentas e Técnicas
.1 Auditoria do projeto de respostas aos riscos
.2 Revisões periódicas dos riscos do projeto
.3 Análise de valor agregado
.4 Medida de desempenho técnico
.5 Planejamento adicional de resposta ao risco
3.Saídas
.1 Planos de workaround
.2 Ações corretivas
.3 Solicitações de mudança no projeto
.4 Atualização no plano de respostas aos riscos
.5 Banco de dados de risco

Figura 3.2 - Processos Gerência de Riscos PMBOK (Fonte: PMI MG)

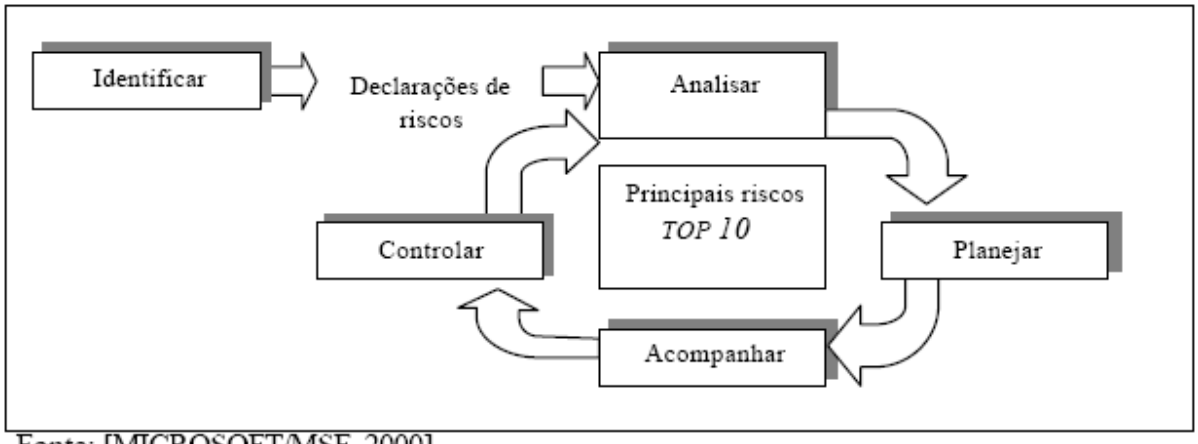
- **Planejar a Gerência de Risco** – determinar qual a abordagem e planejar as atividades de gerência de risco.
- **Identificar Riscos** - determinar quais riscos podem afetar o projeto e documentar as suas características.
- **Analisar Riscos Qualitativamente** - executar uma análise qualitativa dos riscos e das condições para priorizar seus efeitos nos objetivos do projeto.
- **Analisar Riscos Quantitativamente** - medir a probabilidade de ocorrência e as conseqüências dos riscos e estimar as suas implicações nos objetivos do projeto.
- **Planejar as Respostas aos Riscos** - desenvolver procedimentos e técnicas para avaliar oportunidades e reduzir as ameaças aos objetivos do projeto.
- **Controlar e Monitorar Riscos** - monitorar riscos residuais, identificar novos riscos, executar planos de redução de riscos e avaliar seus efeitos através do ciclo de vida de projeto.

3.3.2 Gerência de risco definida na MSF - Microsoft Solutions Framework

O MSF - Microsoft Solutions Framework foi criado em 1994 para apoiar a execução dos serviços de consultoria da Microsoft. O MSF para a gerência de risco possui as seguintes atividades (Figura 3.3) (MICROSOFT/MSF, 2000):

- **Passo 1 - Identificar riscos** - apresentar os riscos à equipe para que possam ser tratados antes de impactarem no projeto.

- **Passo 2 - Analisar riscos** - converter dados de risco em informações para utilização da equipe de projeto para a tomada de decisões. A análise assegura que a equipe está trabalhando nos riscos corretos. Nessa fase, deve ser gerada a lista dos 10 mais riscos (Top 10).
- **Passo 3 - Planejar riscos** - construir planos que suportarão a tomada de decisão e as ações. Planejar envolve o desenvolvimento de ações para endereçar riscos individualmente, priorizar ações para os riscos e criar um plano integrado de gerência de risco.
- **Passo 4 - Acompanhar riscos** - monitorar a situação dos riscos e as ações para reduzi-los.
- **Passo 5 - Controlar riscos** - transferir a gerência de risco para as atividades do dia-a-dia.



Fonte: [MICROSOFT/MSF, 2000]

Figura 3.3 - Framework de Risco da MSF (Fonte: MICROSOFT)

3.4 CONCLUSÃO

O risco sempre esteve presente na vida da humanidade. Desde o homem pré-histórico, que optou por viver em cavernas para garantir a sua vida e reduzir o risco de servir como alimento para animais maiores; até os dias atuais, onde a informação é a grande arma que possibilita o sucesso ou o fracasso de uma organização.

O fato é que, o risco sempre existe, porém sua ocorrência dependerá da ação de outros agentes, internos ou externos à organização. Assim, é importante que as organizações estejam atentas aos riscos que rondam o seu negócio, a fim de garantir sua segurança, por meio de respostas no momento da ocorrência de uma ameaça.

Desta forma, para que as organizações possam estar preparadas para enfrentar estas ameaças, é necessária a implementação de um processo para a gestão dos riscos ao seu negócio. Este processo irá identificar, analisar e controlar todos os riscos possíveis, reduzindo sua ocorrência e possibilitando à organização maior flexibilidade e competitividade na execução dos seus processos críticos.

Este capítulo teve por objetivo, demonstrar estes conceitos sobre a análise e gerenciamento de riscos, além de fazer um estudo sobre duas metodologias que auxiliam as organizações no desenvolvimento do processo de gerência de riscos.

4 PLANO DE CONTINUIDADE DO NEGÓCIO - PCN

4.1 CONCEITOS

As interrupções nos processos de negócios, curtas ou prolongadas, sempre afetam os negócios, causando impactos que muitas vezes são irreversíveis. Segundo o DRI – *Disaster Recovery Institute* - de cada cinco empresas que possuem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos. Este dado é justificado no mercado mundial um dos maiores desafios dos executivos é garantir a continuidade de seus negócios independente do tipo de evento que possa ocorrer. Desta forma, para garantir a continuidade dos negócios, as organizações podem e devem adotar o planejamento da continuidade de negócios.

Segundo Ferreira (2004, p.86), planejamento da continuidade de negócios é:

> "O processo de obtenção e análise de informações que gera, como produto final, uma estratégia integrada e seu plano correspondente, para reagir a uma interrupção não programada nas atividades de negócio".

Já para Saldanha (2000, p. 18), o conceito chave que define o plano de continuidade de negócios é:

> "Plano de Continuidade é composto por um conjunto de procedimentos previamente definidos e testados de forma a garantir a continuidade dos processos e serviços vitais de uma organização, ainda que sob o impacto de um desastre, súbito e inesperado, previamente identificado".

Analisando as afirmações de Ferreira e Saldanha, é possível definir que um plano de continuidade está integrado diretamente com os processos de negócio da organização, sendo seu

objetivo principal, fornecer, em um período de tempo aceitável, todos os recursos necessários para operar os processos críticos de negócio no caso da ocorrência de uma falha ou interrupção.

Para entender melhor como um plano de continuidade funciona, é necessário identificar o que são os processos de negócios. Os processos de negócio podem ser definidos como a divisão da organização em vários departamentos (contabilidade, serviços ao cliente, vendas e etc.), onde cada processo possui um conjunto de atividades que é realizado periodicamente e que produz algo de valor para a organização ou para o cliente. Assim, o objetivo do PCN é assegurar a continuidade destas atividades exercidas por cada processo dentro da organização.

Os principais objetivos que devem ser atingidos pelo PCN são:

- Garantir a segurança dos empregados e visitantes;
- Minimizar danos imediatos e perdas numa situação de emergência;
- Assegurar a restauração das atividades, instalações e equipamentos o mais rápido possível;
- Assegurar a rápida ativação dos processos de negócio críticos;
- Fornecer conscientização e treinamento para as pessoas-chave encarregadas desta atividade.

O PCN é imprescindível para empresas que não podem sofrer interrupção em seus processos de negócios, porque isso representaria risco de perdas financeiras, degradação da imagem no mercado e insatisfação do seu maior patrimônio: seus clientes.

4.2 ELABORAÇÃO DO PLANO DE CONTINUIDADE DO NEGÓCIO

De acordo com a norma ISO/IEC 17799:2001, o processo para a elaboração do plano de continuidade do negócio deve ser composto das seguintes etapas:

- Entendimento dos riscos a que a organização está exposta, no que diz respeito à sua probabilidade e impacto, incluindo a identificação e priorização dos processos críticos do negócio;
- Entendimento do impacto que as interrupções terão sobre o negócio;
- Consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade;
- Definição e documentação de estratégia de continuidade consistente com os objetivos e prioridades estabelecidos para o negócio;
- Detalhamento e documentação de planos de continuidade alinhados com a estratégia estabelecida;
- Testes e atualizações regulares dos planos e procedimentos implantados;
- Garantia de que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização.

O processo de planejamento deve focar os objetivos requeridos do negócio, como, por exemplo, a recuperação de determinados serviços específicos para os clientes, em um período de tempo aceitável. Convém que os serviços e recursos que possibilitarão isto ocorrer sejam previstos contemplando pessoal, recursos em geral, além dos de tecnologia de informação, assim como itens de reposição dos recursos e instalações de processamento da informação.

É importante que o plano de continuidade do negócio especifique claramente as condições de sua ativação, assim como as responsabilidades individuais para a execução de cada uma das atividades do plano. Quando novos requisitos são identificados, é importante que os procedimentos de emergência relacionados sejam ajustados de forma apropriada.

A figura 4.1 ilustra o diagrama indicativo do padrão de planejamento e desenvolvimento de um Plano de Continuidade de Negócios de acordo com o DRI Internacional.

Figura 4.1 - Diagrama Padrão DRI (Fonte: MARINHO, p. 37)

4.2.1 Início e Administração do Projeto

Nesta etapa será definido o escopo / necessidade para o desenvolvimento de um Plano de Continuidade de Negócios, incluindo questões sobre aquisição de patrocínio (apoio), organização e gerenciamento do projeto para atender os limites de prazos e orçamento (MARINHO, 2003).

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Auxiliar o patrocinador do projeto na definição dos objetivos, políticas (conceitos) e análise de fatores de sucesso (métricas) com definições ou indicações de: Escopo, Objetivos, Atendimento às leis e normas, Requisitos, Histórico, Casos.
- Coordenar, organizar e gerenciar o projeto do Plano de Continuidade de Negócios, através da convocação de um comitê administrativo e de uma força-tarefa operacional, esclarecendo as diferenças entre:
    - Recuperação de desastres e Continuidade de Negócios;
    - Resposta a crises e gerenciamento de crises;
    - Reduzir e impedir os riscos de ocorrência dos eventos.
- Supervisionar o projeto de PCN por meio de ferramentas de controle efetivas e do gerenciamento de mudanças.
- Apresentar (divulgando e comprometendo) o projeto aos gestores e aos funcionários da organização.
- Desenvolver o plano do projeto e orçar seus custos.

- Definir a estrutura do projeto e recomendar a delegação de responsabilidades.
- Gerenciar todo o processo.

4.2.2 Avaliação e Controle dos Riscos

As atividades relacionadas à avaliação e controle de riscos definem os possíveis e prováveis cenários que fazem parte do ambiente corporativo e que podem afetar a organização tanto com interrupções quanto com desastres. Nesta etapa serão determinados quais os possíveis danos relacionados a cada evento e quais as medidas necessárias para prevenir e reduzir os efeitos de uma potencial perda. É possível incluir nesta etapa, uma análise de ROI – *Return of Investment* – para facilitar a justificativa dos custos no controle de redução de riscos (MARINHO, 2003).

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Conceber a função da redução de riscos, através da organização.
- Identificar potenciais riscos para a organização, identificando: Probabilidades e Conseqüências.
- Identificar a exigência de suporte técnico externo.
- Identificar vulnerabilidades, ameaças e exposições.
- Identificar alternativas de redução ou minimização de riscos.
- Identificar a consistência das fontes de informação.
- Atuar com a gerência corporativa para definição dos níveis aceitáveis de risco.
- Documentar e apresentar dossiês.

A figura 4.2 ilustra uma metodologia padrão utilizada para a avaliação e controle de riscos.

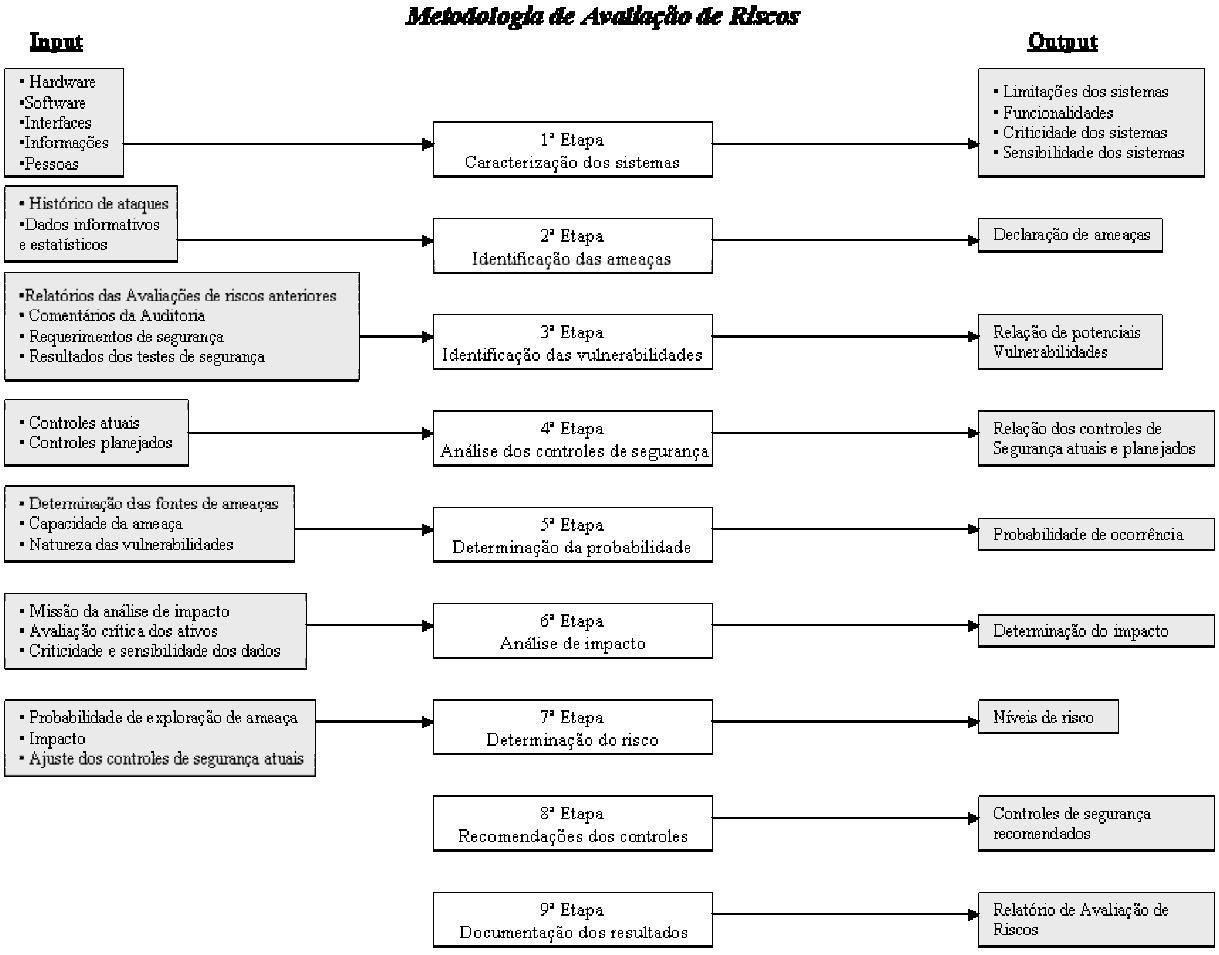


Figura 4.2 - Metodologia de Avaliação de Riscos (Fonte: FERREIRA, p. 89)

4.2.3 Análise de Impacto nos Negócios (*Business Impact Analysis* - BIA)

Nesta etapa serão identificados e avaliados os impactos resultantes da interrupção e dos cenários de desastres que podem afetar a organização, bem como as técnicas para quantificar e

qualificar esses impactos. Além disso, é definida a criticidade dos processos de negócios, suas prioridades de recuperação e interdependências, para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos (MARINHO, 2003).

As principais atividades realizadas nesta etapa, de acordo com a norma ISO/IEC 17799/2001 são:

- Identificação dos eventos que podem causar interrupções nos processos de negócios.
- Avaliação de risco para determinação do impacto destas interrupções.
- Plano Estratégico para se determinar a abordagem mais abrangente a ser adotada para a continuidade do negócio

Para realizar estas atividades, o profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Identificar os processos de negócios da organização.
- Identificar os representantes ou responsáveis de cada um destes processos, que possam fornecer informações confiáveis sobre a sua função.
- Definir e identificar critérios de criticidade.
- Auxiliar a gerência na definição de critérios para a análise.
- Coordenar a análise.
- Identificar as interdependências.
- Definir objetivos e janelas de recuperação, incluindo os tempos de recuperação, as perdas previstas e as prioridades.
- Identificar requisitos de informações necessários para a análise.

- Identificar os recursos necessários para a análise.
- Definir os formatos dos relatórios.
- Avaliar custos de interrupção de processos e componentes.
- Preparar e apresentar a BIA.

Durante a análise de impacto, deve ser dada atenção adequada para as vantagens e desvantagens das avaliações quantitativas e qualitativas. A avaliação quantitativa fornece a medida específica da magnitude dos impactos, que poderá ser utilizada para realizar análise de custo-benefício para implementação de controles de segurança. Sua desvantagem é que, dependendo de como esta medida for expressa, o resultado da análise poderá não ser preciso. A avaliação qualitativa, por sua vez, prioriza os riscos e identifica áreas para melhorias imediatas. Sua desvantagem é não fornecer medidas específicas da magnitude dos impactos.

A tabela 4.1 demonstra as categorias de impacto que podem ser utilizadas para medição quantitativa dos impactos.

Tabela 4.1 - Categorias de Impacto (Fonte: FERREIRA, p. 100)

Nível	Definição
Alto	• Perda significante dos principais ativos e recursos • Perda da reputação, imagem e credibilidade • Impossibilidade de continuar com as atividades de negócio
Médio	• Perda dos principais ativos e recursos • Perda da reputação, imagem e credibilidade
Baixo	• Perda de alguns dos principais ativos e recursos • Perda da reputação, imagem e credibilidade

4.2.4 Desenvolvendo Estratégias de Continuidade de Negócios

Nesta etapa são definidas as estratégias operacionais para a recuperação dos processos e dos componentes de negócios dentro dos prazos de recuperação desejados enquanto processos corporativos críticos são mantidos em atividade. Para a definição destas estratégias, os procedimentos serão divididos em dois planos distintos (MARINHO, 2003):

- **Plano de Recuperação de Desastres –** responsável pelas atividades direcionadas à recuperação ou substituição de componentes
- **Plano de Contingência –** responsável pelas atividades de manutenção dos processos de negócios.

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Identificar as possíveis alternativas para continuidade de negócios disponíveis, suas vantagens e desvantagens, com as respectivas características de custo, incluindo a mitigação (redução de riscos) como estratégias de recuperação.
- Identificar estratégias de recuperação compatíveis com as áreas funcionais de negócios, pois cada ambiente e topologia possuem características e exigências de negócio próprias.
- Consolidar as estratégias; reduzindo o risco de incompatibilidade ou de "gargalo estratégico".
- Identificar necessidades de armazenagem remota e instalações alternativas.
- Desenvolver a unanimidade das unidades de negócio.

- Obter comprometimento da gerência com as estratégias apresentadas.

4.2.4.1 Plano de Recuperação de Desastres

As estratégias de recuperação fornecem meios para restaurar, rapidamente, as operações de tecnologia da informação em caso de interrupções não programadas. Além disso, devem contemplar os impactos de uma paralisação e o tempo máximo aceitável de parada (MARINHO, 2003).

As principais estratégias de recuperação utilizadas são:

- **Backup –** cópia de segurança dos dados e informações da organização.
- **Localidades Alternativas –** ambientes externos preparados para ativação de contingências no ambiente interno da organização.
- **Reposição de equipamentos –** através de contrato com fornecedores e inventário de equipamentos.
- **Regras e responsabilidades –** cada equipe deve ser treinada e estar preparada para responder às situações de emergência / ativação do plano.

4.2.4.2 Plano de Contingência

O Plano de Contingência deve documentar as capacidades e requisitos técnicos que suportarão as operações de contingência. Para isso, é imprescindível definir regras bem

detalhadas, assim como responsabilidades, equipes e procedimentos relacionados com a recuperação do ambiente informatizado após a ocorrência de um desastre (MARINHO, 2003).

A figura 4.3 demonstra a estrutura geral do plano de contingência.

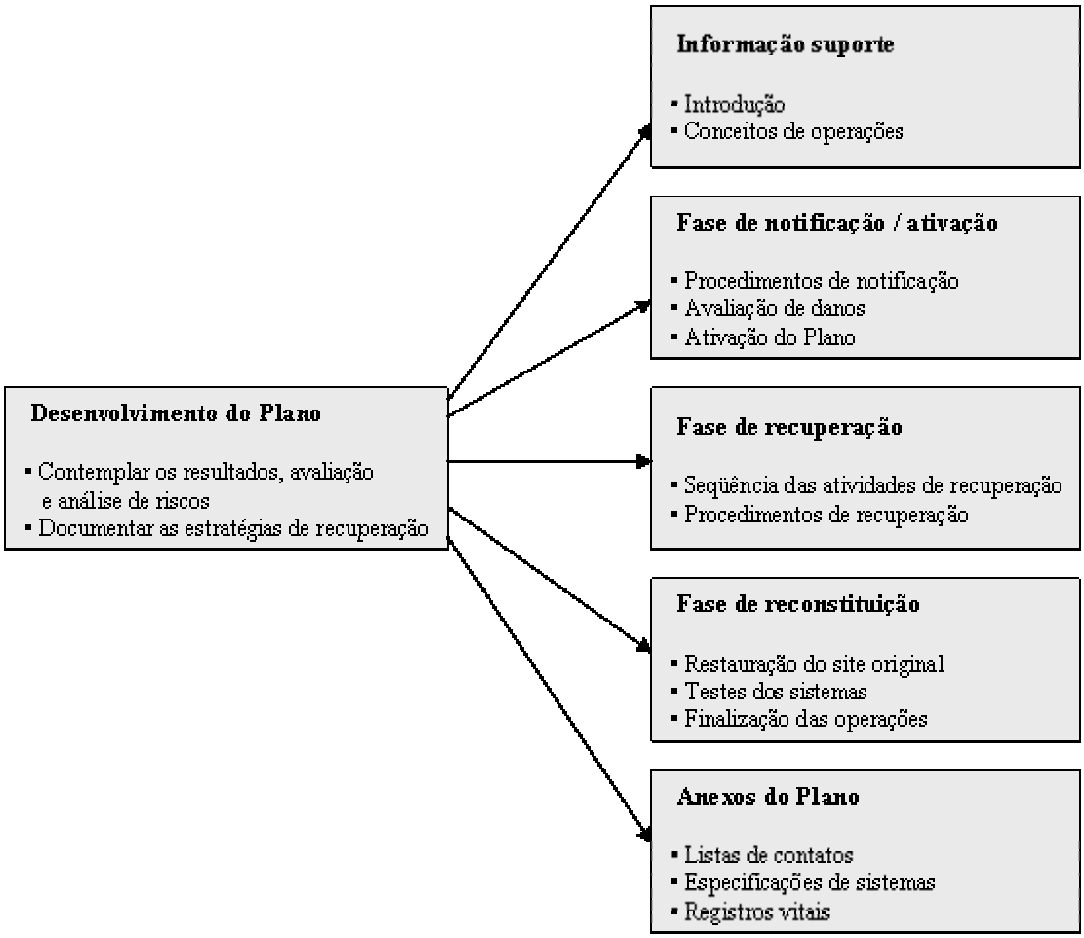


Figura 4.3 – Estrutura Geral do Plano de Contingência (Fonte: FERREIRA, p. 113)

4.2.5 Respostas e Operações de Emergência

Nesta etapa são desenvolvidos e implementados procedimentos de resposta e estabilização de situações por meio de um incidente ou evento, incluindo a criação e a especificação de normas

para o gerenciamento de um centro operacional de emergência (COE) utilizado como central de comando durante uma crise.

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Identificar os tipos potenciais de emergências e as respostas necessárias (por exemplo: incêndio, inundação, greves etc.).
- Verificar a existência de procedimentos de resposta apropriados às emergências.
- Recomendar o desenvolvimento de procedimentos de emergência quando não existam.
- Integrar os procedimentos de resposta à emergência com os procedimentos de recuperação de desastres e de Continuidade de Negócios.
- Identificar os requisitos de comando e controle para gerenciamento de emergências.
- Sugerir a elaboração de procedimentos de comando e controle para definir o papel das autoridades e os processos de comunicação para o gerenciamento das emergências.
- Assegurar que os procedimentos de resposta a emergências estejam integrados com os procedimentos de órgãos públicos.

O Plano de Resposta Emergencial deve ter início no momento T-2 até o momento T+1, ou seja, o tempo disponível para a realização dos procedimentos será em função da antecedência do alarme de desastre até a duração do desastre propriamente dito. A figura 4.4 ilustra o fluxograma da estratégia de um plano de resposta emergencial.

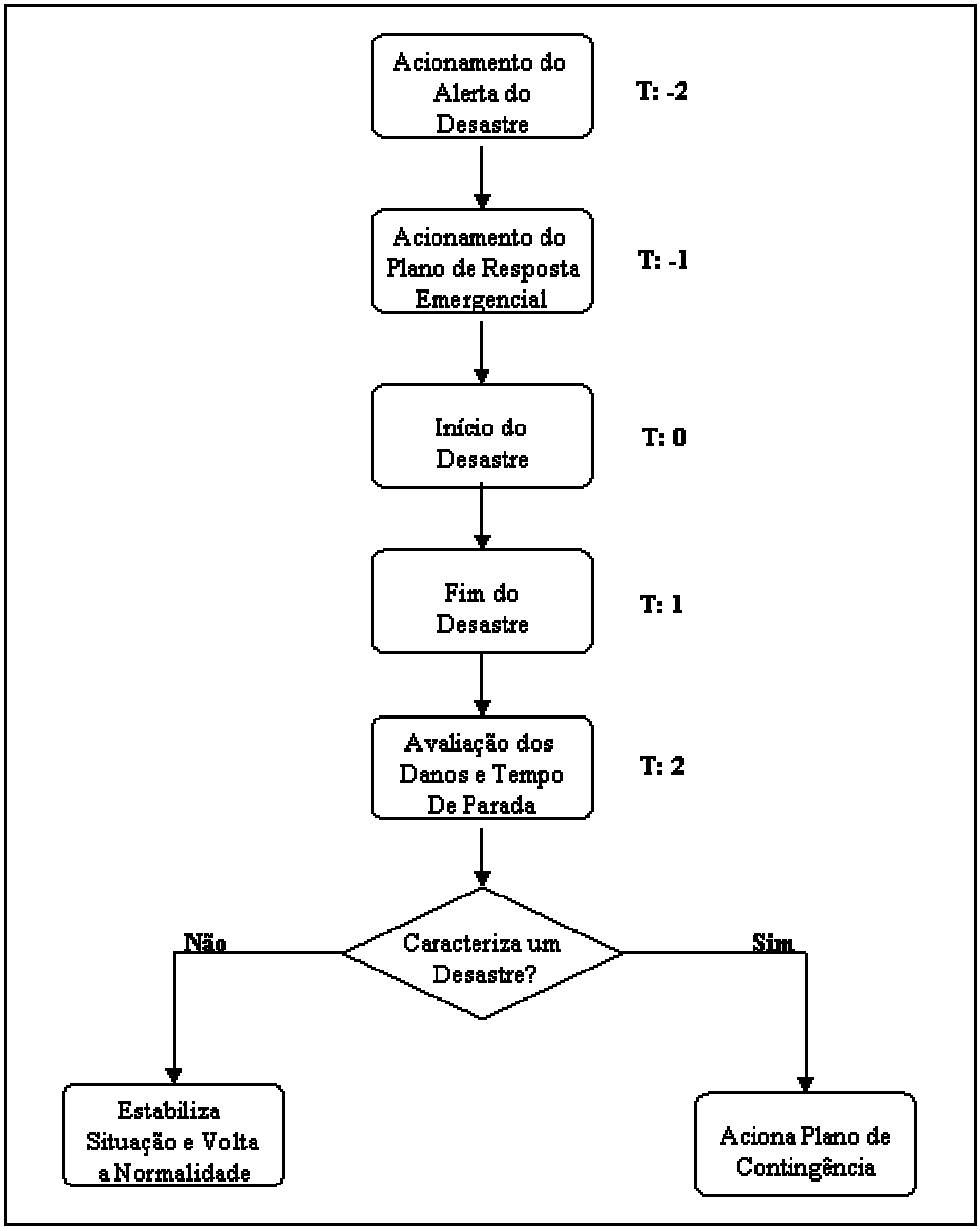


Figura 4.4 - Fluxograma da Estratégia do Plano de Resposta Emergencial (Fonte: SALDANHA, p. 104)

4.2.6 Desenvolvendo e Implementando PCN

Nesta etapa serão integrados todos os componentes até então elaborados e planejados, em um Plano de Continuidade de Negócios, a fim de permitir o atendimento às janelas de recuperação dos componentes e dos processos da organização (MARINHO, 2003).

De acordo com a norma ISO/IEC 17799:2001, o PCN deve ser desenvolvido para a manutenção ou recuperação das operações do negócio, na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos. Para isso, recomenda-se que o processo de planejamento da continuidade do negócio considere os seguintes itens:

- Identificação e concordância de todas as responsabilidades e procedimentos de emergência.
- Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. (Atenção especial deve ser dada à avaliação de dependências externas ao negócio e de contratos existentes.).
- Documentação dos processos e procedimentos acordados.
- Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise.
- Teste e atualização dos planos

O processo de planejamento deve focar os objetivos requeridos do negócio, como por exemplo, a recuperação de determinados serviços específicos para os clientes, em um período de tempo aceitável. É importante que o plano especifique claramente as condições de sua ativação, assim como as responsabilidades individuais para a execução de cada uma das atividades.

Quando novos requisitos são identificados, é imprescindível que os procedimentos de emergência relacionados sejam ajustados de forma apropriada, permitindo desta forma, sua execução com sucesso.

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Identificar os componentes de planejamento dos processos:
  - Planejar a metodologia.
  - Organizar o plano.
  - Dirigir os esforços.
  - Definir o pessoal envolvido.
- Controlar o processo de planejamento e produzir o plano.
- Implementar o plano.
- Testar o plano.
- Definir a manutenção do plano.

4.2.7 Implementando a Consciência e os Programas de Treinamento

Nesta etapa será desenvolvido um programa para incrementar a cultura corporativa, incentivando as habilidades necessárias para elaborar, implementar, atualizar e executar um Plano de Continuidade de Negócios (MARINHO, 2003).

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Estabelecer os objetivos e os componentes do programa de treinamento.
- Identificar requisitos para o treinamento funcional.
- Desenvolver metodologia de treinamento.

- Desenvolver o programa de conscientização.
- Solicitar ou adquirir treinamento de apoio.
- Identificar oportunidades de treinamento externo.
- Identificar veículos de conscientização corporativa.

4.2.7.1 Treinamento

O treinamento das equipes começa com a distribuição do plano para cada um dos seus componentes. A respectiva parte do plano deve ser encaminhada para cada membro, acompanhada da visão geral do plano e da visão geral da sua equipe. Telefones de emergência, dos demais membros da equipe e de fornecedores também devem fazer parte do conjunto de instruções básicas.

Durante a contingência, os membros de cada equipe não estarão necessariamente desempenhando exatamente os mesmos papéis que desempenham no seu dia-a-dia. Desta forma, é necessário que os membros sejam pessoas aptas e preparadas para desempenhar satisfatoriamente as funções e executar a contento as atividades que lhes couberem. O objetivo do treinamento, por sua vez, é familiarizar os participantes com o plano e suas atribuições.

4.2.7.2 Conscientização

Além do treinamento, é interessante também que seja adotado um programa de conscientização para a importância das medidas preventivas e para a importância dos

procedimentos de garantia de continuidade. Esse programa deve utilizar todas as mídias de comunicação existentes na organização e possuir como meta manter o nível de conscientização permanentemente elevado.

Algumas ações que podem ser utilizadas para manter a conscientização em alta são:

- Distribuir artigos sobre Desastres Operacionais
- Distribuir artigos sobre Plano de Continuidade
- Produzir e divulgar um vídeo apresentando o Plano, sua razão de existir e seu escopo
- Incluir o nome dos responsáveis na lista de usuários do DRJ - *Disaster Recovery Journal* - na www
- Promover palestras
- Mandar periodicamente matérias para jornais internos
- Incluir os fornecedores entre o público a ser conscientizado
- Cobrar dos fornecedores a implementação de um plano de continuidade ou um SLA - *Service Level Agreements*
- Criar uma página na Intranet para divulgação de notas sobre a prevenção, segurança e continuidade operacional
- Promover encontro com responsáveis pelo PCN de outras organizações

4.2.8 Mantendo e Exercitando o PCN

Nesta etapa será elaborado um pré-plano para coordenar os exercícios do PCN, avaliando os resultados obtidos. Além disso, serão desenvolvidos processos para a manutenção das

variáveis dos planos de acordo com os objetivos estratégicos da empresa. Desta forma, será possível apresentar uma comparação entre o resultado obtido e um ambiente corporativo convencional, relatando as diferenças de forma concisa e clara.

É importante que o PCN seja mantido por meio de análises críticas regulares e atualizações, de forma a assegurar a sua contínua efetividade. Convém que seus procedimentos sejam incluídos no programa de gerenciamento de mudanças da organização, de forma a garantir que as questões relativas à continuidade de negócios estão devidamente tratadas.

Alguns exemplos que podem demandar atualizações no plano incluem a aquisição de um novo equipamento, atualizações dos sistemas operacionais ou ainda alterações:

- De pessoal
- De endereços ou número telefônicos
- De estratégia de negócio
- Na localização, instalações e recursos
- Na legislação
- Em prestadores de serviço, fornecedores e clientes-chave
- De processos (inclusões e exclusões)
- No risco (operacional e financeiro)

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Preparar o planejamento dos exercícios.
- Coordenar os exercícios.
- Avaliar os exercícios do plano.
- Implementar o exercício das atividades dos planos.

- Documentar os resultados.
- Avaliar os resultados.
- Atualizar e adequar os planos.
- Reportar os resultados e a avaliação dos exercícios aos gestores.
- Assimilar as diretivas estratégicas do negócio.

4.2.8.1 Testes

O PCN pode apresentar falhas quando testado, geralmente devido a pressupostos incorretos, omissões ou mudanças de equipamentos, pessoal e novas tecnologias. Por isto, ele deve ser testado regularmente, de forma a garantir sua permanente atualização e eficácia. É importante que tais testes também assegurem que todos os membros da equipe de recuperação e outras pessoas de relevância estão conscientes sobre o plano.

A norma ISO/IEC 17799:2001 indica os seguintes tipos de testes para a validação do plano:

- Testes de mesa, simulando diferentes cenários, citando os procedimentos de recuperação para diferentes formas de interrupção;
- Simulações (particularmente útil para o treinamento do pessoal nas suas atividades);
- Testes de recuperação técnica, para assegurar que os sistemas de informação possam ser efetivamente recuperados;
- Testes de recuperação em um local alternativo, executando os processos de negócio em paralelo com a recuperação das operações;

- Testes dos recursos, serviços e instalações de fornecedores garantindo que os serviços e produtos fornecidos atendam aos requisitos contratados;
- Ensaio geral, testando se a organização, o pessoal, os equipamentos, os recursos e os processos podem enfrentar interrupções.

4.2.8.2 Manutenção

Para ser eficaz, o PCN deve estar devidamente atualizado, refletindo as reais e atuais configurações de sistemas, procedimentos, estruturas organizacionais e suas políticas. Assim é essencial que o plano seja revisado e atualizado regularmente, como parte do processo cotidiano da organização.

Os seguintes itens devem ser considerados na revisão do PCN:

- Exigências operacionais;
- Exigências de segurança;
- Procedimentos técnicos;
- Hardware, software e outros equipamentos também essenciais (tipos, especificações e quantidade);
- Nomes e formas de contato com os membros das equipes;
- Nomes e formas de contato com os fornecedores e prestadores de serviços;
- Exigências e recursos necessários nas localidades alternativas.

4.2.9 Relações Públicas e Gerenciamento de Crises

Esta etapa é responsável pelo desenvolvimento, coordenação, avaliação e exercício no manuseio de mídias e documentos durante situações de crise, bem como os possíveis meios de comunicação que minimizem os impactos traumáticos entrem a organização, seus funcionários e suas famílias, clientes-chave, fornecedores, investidores e gestores corporativo. Através dos procedimentos desta etapa, será possível assegurar o fornecimento de informações para todos os investidores, por meio de uma fonte única e constantemente atualizada (MARINHO, 2003).

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Estabelecer programas de relações públicas para o gerenciamento proativo de crises.
- Estabelecer a necessária coordenação de crises com agências externas.
- Estabelecer a comunicação essencial de crise com grupos de investidores relevantes.
- Estabelecer e testar as atividades do plano para o manuseio de mídias da organização e suas unidades de negócio.

4.2.10 Parceria com Entidades Públicas

Nesta etapa serão estabelecidos os procedimentos necessários e as políticas de coordenação de resposta, atividades de Continuidade e Restauração de Negócios, com o auxílio de autoridades públicas para o atendimento de normas e leis.

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Coordenar preparativos de emergência, resposta, recuperação, retomada e procedimentos de restauração com o apoio de órgãos públicos.
- Estabelecer procedimentos de acordos e contratos durante situações de crise, emergência ou desastre.
- Manter a atualização do conhecimento de leis e normas públicas, relacionadas a procedimentos de emergência.

4.2.11 Parceria com Entidades Particulares

Nesta etapa serão estabelecidos diretrizes de procedimentos e coordenação de resposta, atividades de Continuidade e Restauração de Negócios, com o auxílio de organizações que compartilham interesses comuns e de terceiros contratados para a execução de tarefas e serviços devido à especialização de sua estrutura e objetivo de negócio para limitação de responsabilidades e funções.

O profissional responsável por esta etapa deverá atingir os seguintes objetivos:

- Coordenar preparativos de emergência, resposta, recuperação, retomada e procedimentos de restauração com o apoio de procedimentos planejados para atividades realizadas por parceiros e terceiros.
- Estabelecer procedimentos de acordo e contratos para cenários de crise, emergência ou desastre.
- Manter atualizado o conhecimento de modificações estatutárias, organizacionais, leis e normas envolvendo o relacionamento entre parceiros e terceiros, que sejam relacionadas a procedimentos de emergência.

4.3 CONCLUSÃO

Oferecer produtos e serviços com qualidade tornou-se uma premissa para ser competitivo no mercado global atualmente. Porém a qualidade é apenas um dos fatores que possibilita a competitividade para a organização. Atualmente os clientes exigem garantias de que o produto ou serviços que adquiriu ou tem adquirido possui suporte, ou então, uma continuidade no futuro.

E para garantir que a organização esteja preparada para esta exigência, é imprescindível possuir no mínimo a preocupação com o rumo que o negócio irá tomar, passo importante para a gestão da continuidade de seus negócios.

> "Hoje, devido à grande dependência tecnológica das empresas, o PCN é um seguro contra eventuais paradas, cujo tempo de recuperação é sinônimo de perda financeira".
>
> Fernando Marinho

O objetivo deste capítulo foi demonstrar o que é e como funciona o PCN, além de explicar detalhadamente os passos necessários para a elaboração do plano de acordo com o DRI – *Disaster Recovery Institute*.

5 PROJETO

5.1 ESTUDO SOBRE A IMPORTÂNCIA DO PCN

Principalmente no Brasil, onde a cultura de prevenção não tem um papel muito importante na sociedade, as organizações não estão totalmente preparadas para dar continuidade ao seu negócio caso ocorra algum problema ou desastre no seu ambiente produtivo. Para evitar as perdas e os prejuízos que um desastre pode causar à estabilidade da organização, é necessário desenvolver um bom planejamento para a continuidade do seu negócio.

Para desenvolver este planejamento é necessário investimento, mudança na cultura da organização, além do alinhamento dos processos de acordo com a estratégia do negócio. E geralmente são estes os fatores que contribuem para que a organização deixe o PCN para um segundo plano.

Um PCN pode consumir recursos financeiros significativos da organização, uma vez que pessoal e equipamentos de reserva para comunicação e processamento de informações em locais alternativos serão necessários. Porém, sua inexistência pode acarretar em uma perda mais significativa que seu investimento. Um exemplo disso pode ser identificado nos seguintes incidentes ocorridos:

- Blecaute em Wall Street em 13 de agosto de 1990, quando 28 empresas deslocaram seus processamentos de dados para locais de recuperação previamente planejados (UNIDADE VI).

- Enchente na região central de Chicago em 13 de abril de 1992, quando 33 empresas fizeram o mesmo. A Bolsa de Mercadorias de Chicago, uma das mais importantes do mundo, ficou paralisada completamente no primeiro dia da enchente, afetando mercados financeiros no resto do mundo devido ao volume de negócios não fechados (UNIDADE VI).
- O ataque terrorista ao World Trade Center em 11 de setembro de 2001, que teve impacto significativo nos mercados dos Estados Unidos e mundial. A Bolsa de Valores de Nova Iorque, o American Stock Exchange e a NASDAQ não abriram em 11 de Setembro e permaneceram fechadas até 17 de Setembro. As instalações e centros de processamento de dados remotos da Bolsa de Valores de Nova Iorque ("NYSE") mais as empresas participantes, consumidores e mercados foram incapazes de se comunicarem devido aos danos ocorridos à instalação de chaveamento telefônico próxima ao World Trade Center. Quando os mercados de ações reabriram em 17 de Setembro de 2001, após o maior período em que estiveram fechadas desde a Grande Depressão em 1993, o índice do mercado de ações Dow Jones Industrial Average ("DJIA") caiu 684 pontos, ou 7,1%, para 8920 pontos, sua maior queda em um único dia. No fim da semana, o DJIA tinha caído 1369,7 pontos (14,3%), sua maior queda em uma semana na história. O mercado de ações americano perdeu 1,2 trilhão de dólares em valor em uma semana (WIKIPEDIA).

Mas não é apenas fora do Brasil que incidentes acontecem, no ano passado (2003), a capital Florianópolis ficou três dias no escuro por causa de um blecaute que começou na tarde da quarta-

feira dia 29 de outubro de 2003, quando explodiu um contêiner de gás usado na manutenção da ponte que liga a cidade ao continente, provocando fogo e afetando as linhas de transmissão. A falta de energia elétrica e de água, o trânsito congestionado em vários pontos e mais a perda de alimentos pela ausência de refrigeração foram apenas alguns dos transtornos que atingiu a população da ilha.

Possuir um PCN pode ser um fator de diferenciação num ambiente altamente competitivo como o de hoje. Ele é parte de organizações conscientes da qualidade de seus compromissos com seus acionistas, funcionários, clientes e fornecedores.

5.2 PESQUISA DE CAMPO COM EMPRESAS DA REGIÃO

Para identificar como está a preocupação das organizações em relação ao PCN, foi desenvolvida uma pesquisa de campo com algumas empresas da região. Para verificar a pesquisa na íntegra, verifique o Anexo 1 deste trabalho.

As organizações entrevistadas foram:

- Marisol
- Transjoi Operações de Transportes
- Palhares Advogados Associados
- Companhia Fabril Lepper
- Embraco
- Tuper Escapamentos – SICAP
- Tigre
- Tupy

- Portobello
- SOCIESC
- CIESC – Centro das Indústrias do Estado de SC

O gráfico 5.1 ilustra o ramo de atividade das empresas entrevistadas.

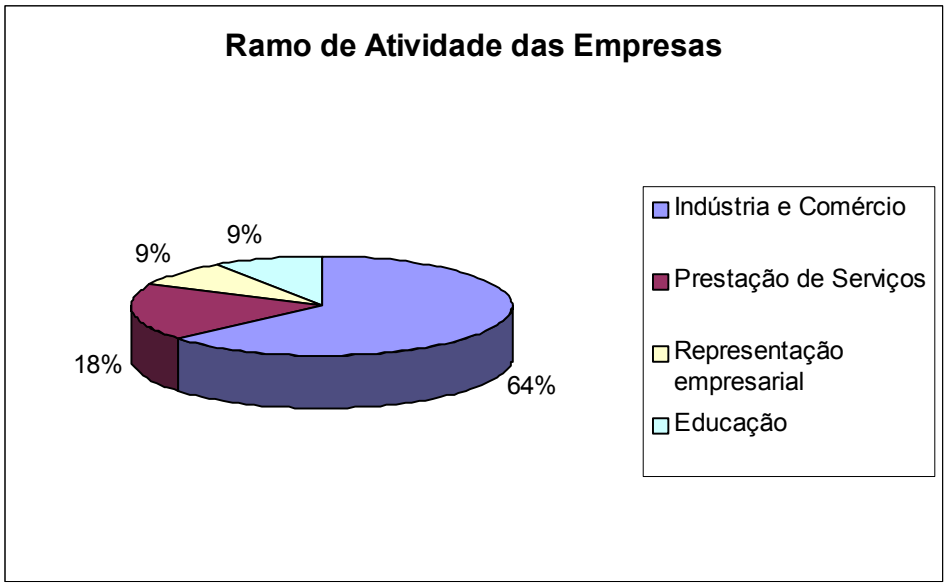


Gráfico 5.1 - Ramo de Atividade das empresas entrevistadas

Das empresas entrevistadas 82% possui alguma certificação. O gráfico 5.2 ilustra quais os tipos de certificação que as empresas entrevistadas possuem.

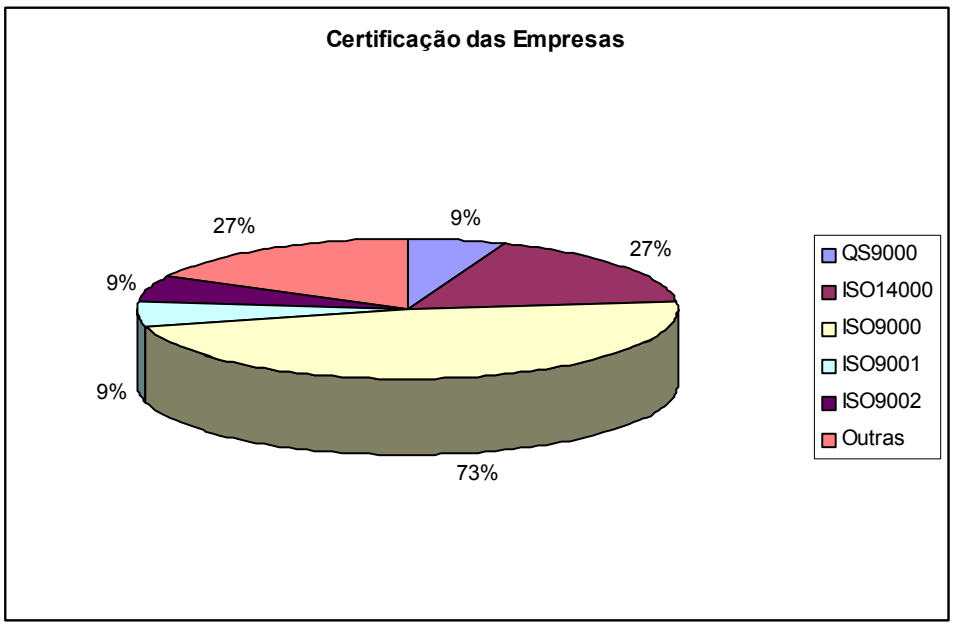


Gráfico 5.2 - Tipos de Certificação das empresas entrevistadas

Grande parte das empresas entrevistadas são indústrias de grande porte, que possuem reconhecimento nacional. Assim para suprir a demanda do mercado, a quantidade de equipamentos que suportam os seus processos está entre 500 até mais de 1000. Isto demonstra que quanto maior é a empresa, maior é o seu parque tecnológico e conseqüentemente maior será a sua preocupação com a segurança da informação e funcionamento dos processos. O gráfico 5.3 ilustra a quantidade de equipamentos que as empresas possuem.

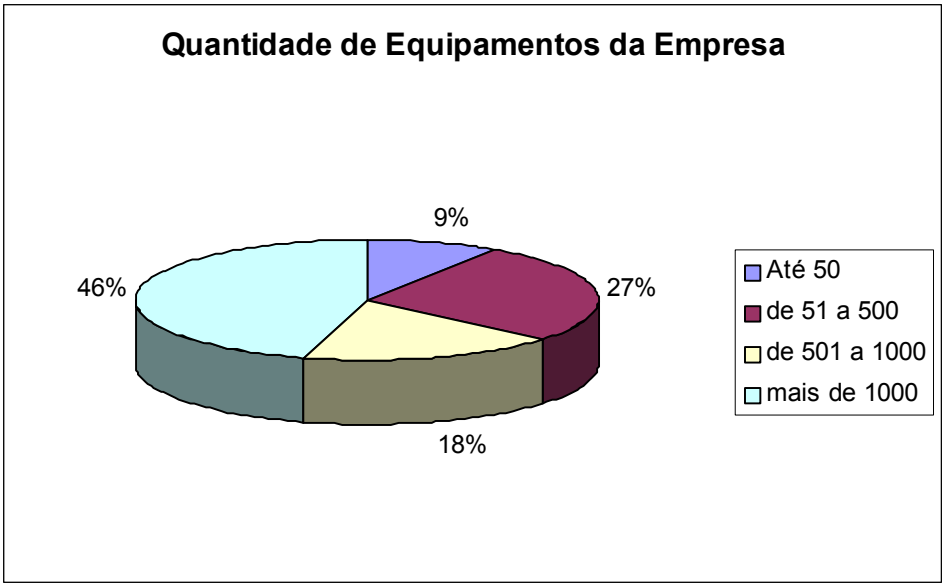


Gráfico 5.3 - Quantidade de Equipamentos das empresas entrevistadas

Mesmo possuindo um grande parque tecnológico, apenas 46% das empresas possuem um orçamento específico para recursos com segurança. O percentual disponível para este orçamento é de menos de 1% até 5% do orçamento global da empresa. Além disso, apenas 46% destas empresas possuem algum processo que trata da gestão da continuidade. E 36% desconhecem esta informação. Levando em consideração que uma das premissas para a implantação do PCN dentro da organização é a sua divulgação, é quase possível avaliar que estas empresas não possuem um processo específico sobre o tema. Pela importância que estas empresas tem no mercado nacional, é preocupante pensar no impacto que uma interrupção traria para a economia. O gráfico 5.4 ilustra o percentual das empresas em relação a existência de processos específicos para a gestão da continuidade.

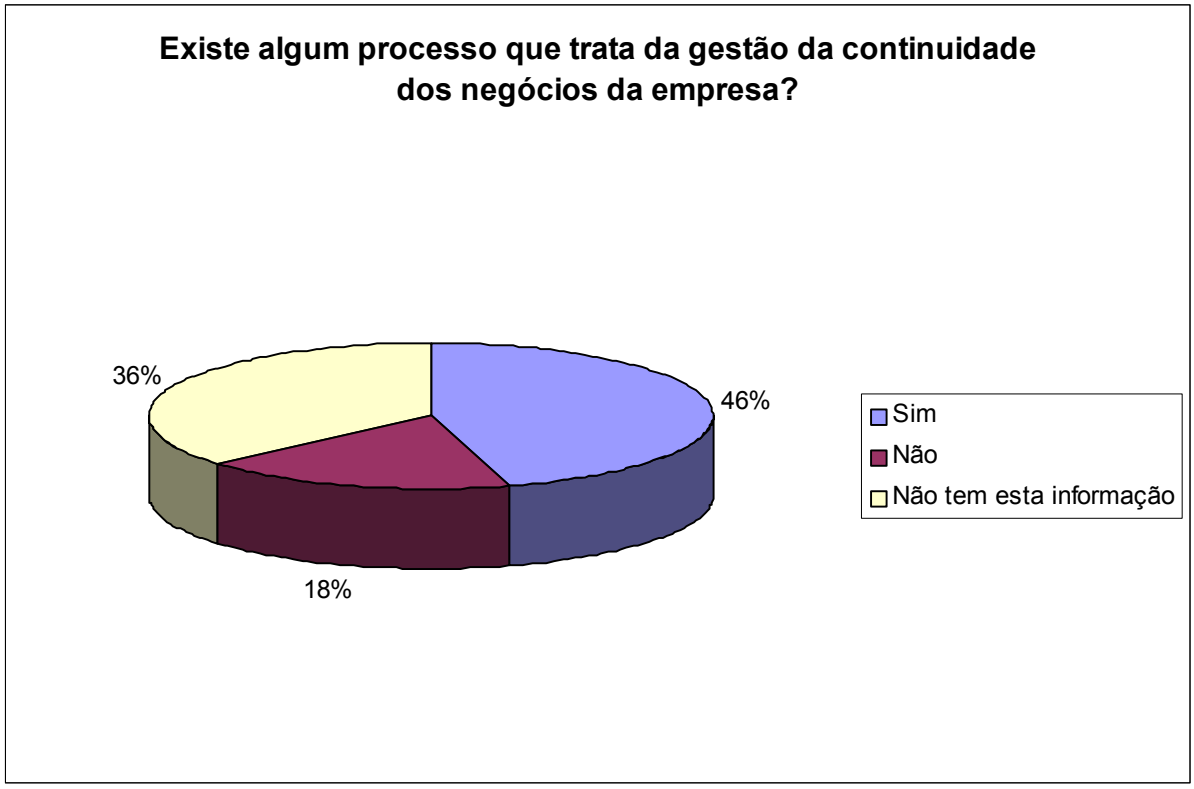


Gráfico 5.4 - Existência de processo de gestão da continuidade

Porém todas elas já possuem engatilhado algum tipo de procedimento ou planejamento que podem numa etapa posterior estar relacionado ao PCN. Isso demonstra que a preocupação com o tema vem crescendo a cada dia.

5.3 DESENVOLVIMENTO DO MODELO PARA ELABORAÇÃO DE UM PCN

A melhor forma de possibilitar a continuidade do negócio de uma organização após uma contingência é através de um bom planejamento. Com um planejamento bem elaborado,

preparado e periodicamente testado, a organização obterá sucesso na execução dos procedimentos de recuperação e continuidade necessários para manter a empresa em atividade.

Para auxiliar as organizações na elaboração deste planejamento, foi desenvolvido um modelo guia para a o desenvolvimento, implantação e manutenção de um PCN. Os formulários auxiliares do modelo guia poderão ser verificados no Anexo 2 deste trabalho.

5.3.1 Etapa 1 – Identificação

Nesta etapa serão desenvolvidas as seguintes atividades:

- Identificação do negócio
- Identificação dos processos que mantêm o negócio (processos críticos)
- Identificar a infra-estrutura que suporta os processos
- Identificar as ameaças que afetariam o desenvolvimento dos processos

Esta é a etapa mais importante de todo o processo, pois é nesta etapa que serão definidos quais os processos estarão sendo mantidos pelo PCN. O PCN não precisa necessariamente atender todos os processos de uma organização, ele estando preparado para prever ou dar suporte aos processos críticos já traz grandes resultados e minimiza a ocorrência de impactos negativos na operação da organização.

5.3.2 Etapa 2 – Análise

Nesta etapa serão desenvolvidas as seguintes atividades:

- Analisar as vulnerabilidades da infra-estrutura que mantêm os processos
- Definir as probabilidades de impacto
- Planejar ações imediatas, de contingência e de restauração
- Atribuir validade e responsáveis pelas ações

O sucesso de um PCN deve-se ao fato de um grande investimento de tempo e quantidade de informações levantadas na etapa de identificação e por conseguinte analisadas nesta etapa, a etapa de análise.

É nesta etapa que o PCN será definitivamente elaborado, ou seja, através das informações levantadas na primeira etapa, serão analisadas as ameaças que estas informações podem ter e quais ações para evitar, manter e recuperar no caso de uma ou mais destas ameaças se concretizarem.

5.3.3 Etapa 3 – Implementação

Nesta etapa serão desenvolvidas as seguintes atividades:

- Implantação das ações
- Treinamento com os responsáveis
- Divulgação dentro e fora da organização (funcionários, clientes e fornecedores)

Esta etapa é a responsável tanto pelo funcionamento correto do PCN elaborado, quanto pela conscientização e capacitação dos responsáveis pelas atividades do plano. É muito importante que todos tenham conhecimento e saibam como agir no caso de uma emergência, por isso que a divulgação se torna um dos fatores chave para o sucesso do seu funcionamento.

5.3.4 Etapa 4 – Manutenção

Nesta etapa serão desenvolvidas as seguintes atividades:

- Criação de atividades para atualização do PCN – integrado com atividades do dia-a-dia
- Testar o PCN através de simulações e registrar o resultado
- Reunião semestral para avaliar os processos críticos (mudança de estratégia ou negócio da organização)

O PCN não terá nenhuma utilidade se não estiver sempre atualizado e constantemente testado. Muitas vezes tanto durante o planejamento, quanto no momento de implantação, algumas características do ambiente ou até da capacitação de pessoas não são totalmente identificadas, podendo ser um ponto crítico que poderá caracterizar o mau funcionamento do plano no momento da sua execução.

A existência do PCN é a garantia que a organização não fique inativa em nenhuma situação, porém ele somente desempenhará a sua função corretamente se estiver de acordo com as características atuais das organizações.

5.4 CONCLUSÃO

Este capítulo teve como objetivo identificar a importância do PCN para as organizações atualmente. Como a dependência tecnológica vem crescendo gradualmente nos últimos anos, a existência de um PCN torna-se quase imprescindível para as organizações que não podem sofrer uma interrupção nas suas atividades.

Além disso, no decorrer deste capítulo, foi possível averiguar por meio da pesquisa de campo como está a preocupação das organizações em relação ao PCN. A preocupação vem crescendo, porém o investimento e a mudança de cultura são fatores que fazem com que as organizações deixem sua elaboração para um segundo momento.

Por fim, foi feito o desenvolvimento de um modelo guia capaz de auxiliar as organizações na elaboração do plano de continuidade do seu negócio.

6 CONSIDERAÇÕES FINAIS

Uma das motivações para o desenvolvimento deste trabalho foi o fato de que as organizações estão cada vez mais dependentes dos sistemas e de toda a tecnologia que as envolve. É quase impossível que uma organização não possua algum tipo de dependência tecnológica, mesmo se tratando de uma micro ou pequena empresa.

A tecnologia é fundamental para que a organização possa entrar no mercado e se manter de forma competitiva, pois por meio dela será oferecido mais qualidade em menos tempo. Porém é preciso avaliar até que ponto é bom estar totalmente atualizado. À medida que a organização expande seus negócios e começa a utilizar a rede mundial – Internet - por exemplo, aumenta a probabilidade de ameaças ao seu negócio.

Desta forma, é preciso que as organizações estabeleçam procedimentos de segurança para toda a sua infra-estrutura. Estes procedimentos vão desde medidas de segurança para os recursos de TI que geralmente suportam os processos da organização, até a segurança física de seus funcionários, clientes e fornecedores.

Com isso surge a necessidade da existência de um PCN dentro das organizações. Por meio dele, as organizações terão a garantia da prevenção, manutenção e recuperação do seu ambiente produtivo, independente dos eventos que ocorram e por conseqüência suspendam suas operações, ou dos danos causados nos seus recursos.

Por meio deste trabalho, foi possível analisar qual o impacto que um desastre ou a falta de um PCN poderia causar no processo produtivo das organizações. Os exemplos citados no tópico 5.1 do capítulo 5 comprovam este fato. Em todos os exemplos, houve muitas perdas tanto de informações quanto de equipamentos e até, no caso do World Trade Center de vidas humanas.

Neste caso então, o PCN auxiliaria na recuperação e contingência dos processos, possibilitando a continuidade da organização e rápido retorno ao seu desempenho padrão.

Assim, este trabalho confirmou que é muito importante a existência de um PCN dentro da organização para que a mesma continue sempre ativa.

6.1 CONTRIBUIÇÕES DO TRABALHO

Este trabalho trouxe contribuições importantes, tais como:

- Identificação do cenário atual do PCN no Brasil
- Estudo da importância de um PCN dentro das organizações
- Desenvolvimento de uma pesquisa de campo com empresas da região para averiguar como está o nível de conhecimento e aplicação do PCN
- Definição de um modelo guia para o desenvolvimento de um PCN dentro da organização

6.2 TRABALHOS FUTUROS

Por meio deste trabalho foi possível identificar a necessidade da existência de uma ferramenta com base nos padrões estabelecidos pelo DRI, que possibilite automatizar a elaboração e manutenção do PCN, pois todo este processo é ainda manual e muito complexo para controlar.

Assim fica como sugestão de trabalhos futuros a implementação desta ferramenta, com base no modelo proposto neste trabalho.

REFERÊNCIAS

1 BRASIL. Norma ISO/IEC 17799:2001. Estabelece critérios para a segurança da informação dentro das organizações.

2 BSI, British Standards Institute. BS 7799 Information Security. Artigo de acesso exclusivo por meio eletrônico. Disponível em: http://www.bsi-global.com/Global/bs7799.xalter. Acesso em: 21/08/2004.

3 CHESWICK, Bill. Firewalls in Internet Security: Reppling the Wily Hacker. Ed. Addison Wesley

4 DRI International. Disaster Recovery Institute. Apresenta informações sobre continuidade de negócios. Disponível em: http://www.drii.org. Acesso em: 01/10/2004.

5 FERREIRA, Aurélio Buarque de Holanda. Novo Dicionário Aurélio Século XXI: o dicionário da língua portuguesa. 3. ed. Rio de Janeiro: Nova Fronteira, 1999.

6 FERREIRA, Fernando N. F. Segurança da informação em ambientes informatizados. 1. ed. Rio de Janeiro: Ciência Moderna, 2003.

7 INFOWESTER. Firewall: conceitos e tipos. Disponível em: http://www.infowester.com/firewall.php. Acesso em: 30/12/2004.

8 MARINHO, Fernando. Como proteger e manter seus negócios. 1. ed. Rio de Janeiro: Campus, 2003.

9 MICROSOFT. Aplicando a Disciplina de Gerenciamento de Riscos de Segurança. Artigo de acesso exclusivo por meio eletrônico. Disponível em: http://www.microsoft.com/brasil/security/guidance/prodtech/win2000/secmod135.mspx. Acesso em: 30/08/2004.

10 MICROSOFT. Compreendendo a Disciplina de Gerenciamento de Riscos. Artigo de acesso exclusivo por meio eletrônico. Disponível em: http://www.microsoft.com/brasil/security/guidance/prodtech/win2000/secmod134.mspx. Acesso em: 30/08/2004

11 NAKAMURA, Emilio Tissato e GEUS, Paulo Lício de. Segurança de redes em ambientes cooperativos. São Paulo: Berkeley Brasil, 2002.

12 NBSO – NIC BR Security Office. Estatísticas dos Incidentes Reportados ao NBSO. Disponível em: http://www.nbso.nic.br/stats/incidentes/. Acesso em: 30/12/2004.

13 PMIMG. PMI Capítulo de Minas Gerais, 2002. PMBOOK 2000. Disponível em: http://www.pmimg.org.br. Acesso em: 02/09/2004.

14 RAMOS, F.F. Análise de Risco: O que se diz, o que se faz, e o que realmente é. Artigo de acesso exclusivo por meio eletrônico. Disponível em: http://www.axur.com.br. Acesso em: 30/08/2004.

15 SALDANHA, Fernando. Introdução a planos de continuidade e contingência operacional. 1. ed. Rio de Janeiro: Papel Virtual, 2000.

16 SANTOS, Luiz Carlos. Como funciona a criptografia? Artigo de acesso exclusivo por meio eletrônico. Disponível em: http://www.clubedasredes.eti.br/rede0009.htm. Acesso em: 21/08/2004.

17 UNIDADE VI – Segurança Física e Ambiental em Informática. Disponível em: http://www.geocities.com/ferujo/unidade-vi.htm. Acesso em: 30/12/2004.

18 US CERT. Statistics on Federal Incident Reports. Apresenta pesquisas sobre incidentes de segurança da informação. Disponível em: http://www.us-cert.gov/federal/statistics. Acesso em: 02/09/2004

19 VARGAS, Ricardo. Gerenciamento de Projetos: estabelecendo diferenciais competitivos. Rio de Janeiro: Brasport, 2003.

20 WIKIPEDIA – A enciclopédia livre. Ataques de 11 de Setembro. Disponível em: http://pt.wikipedia.org/wiki/Ataques_de_11_de_Setembro. Acesso em: 30/12/2004.

ANEXO

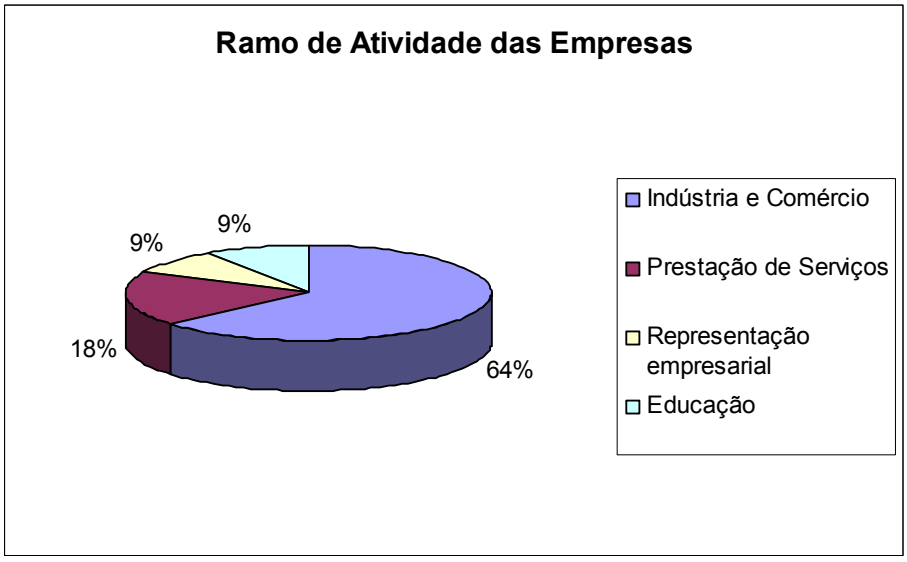
ANEXO 1 – Pesquisa de Campo com Empresas da Região

ANEXO 2 – Formulários auxiliares do Modelo Guia para elaboração do PCN

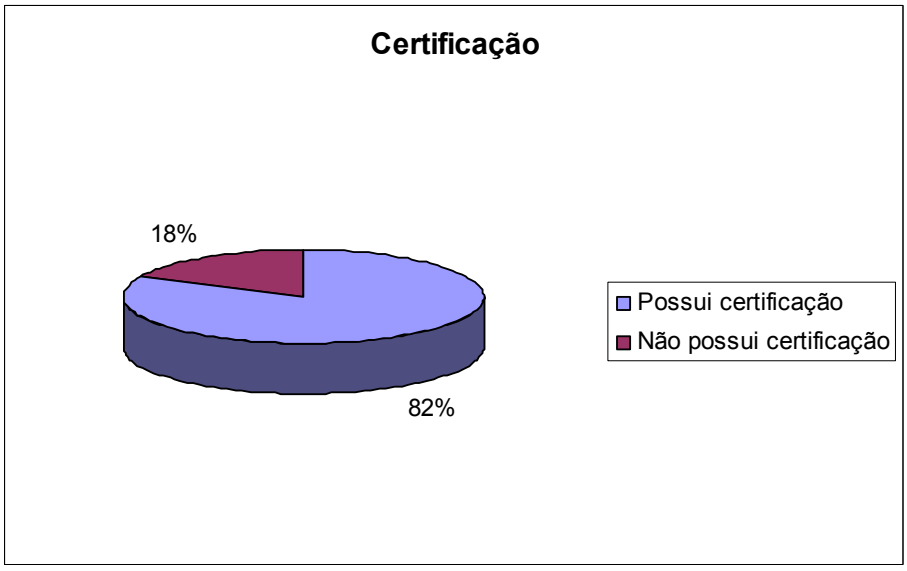
ANEXO 1 – PESQUISA DE CAMPO COM EMPRESAS DA REGIÃO

PERFIL DOS ESTREVISTADOS

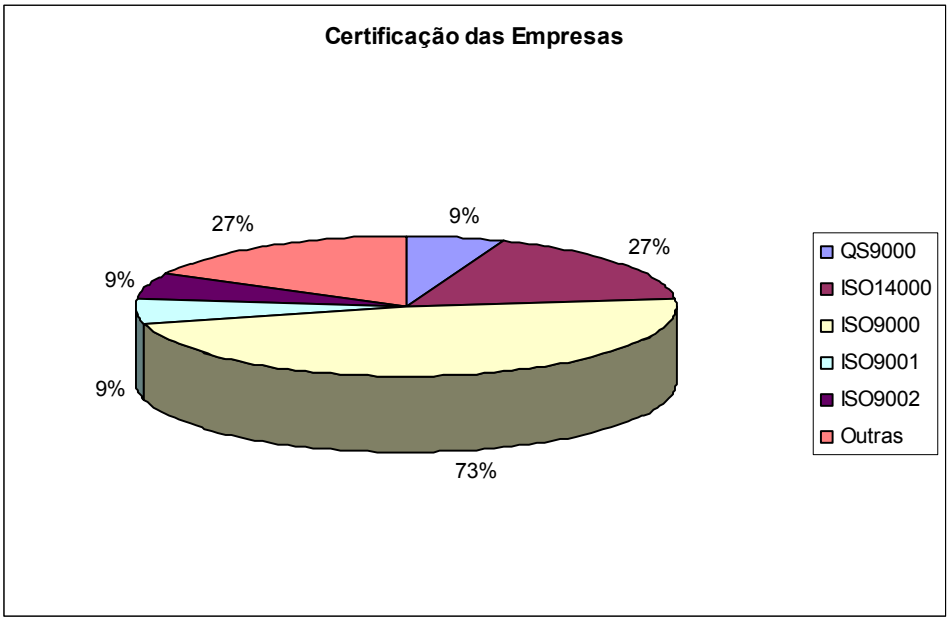
1. Qual é o ramo de atividade da empresa?



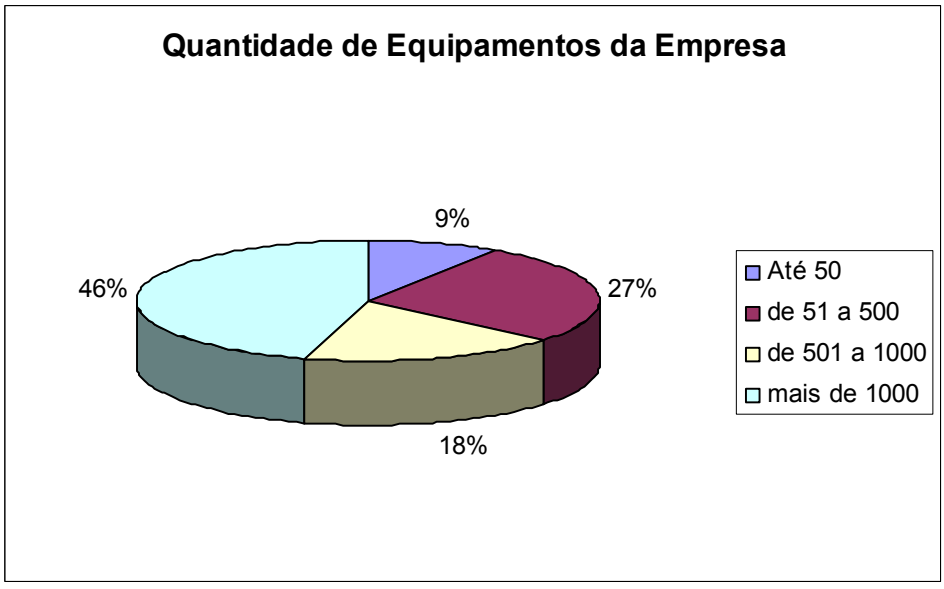
2. A empresa possui certificação?



3. Qual certificação a empresa possui?

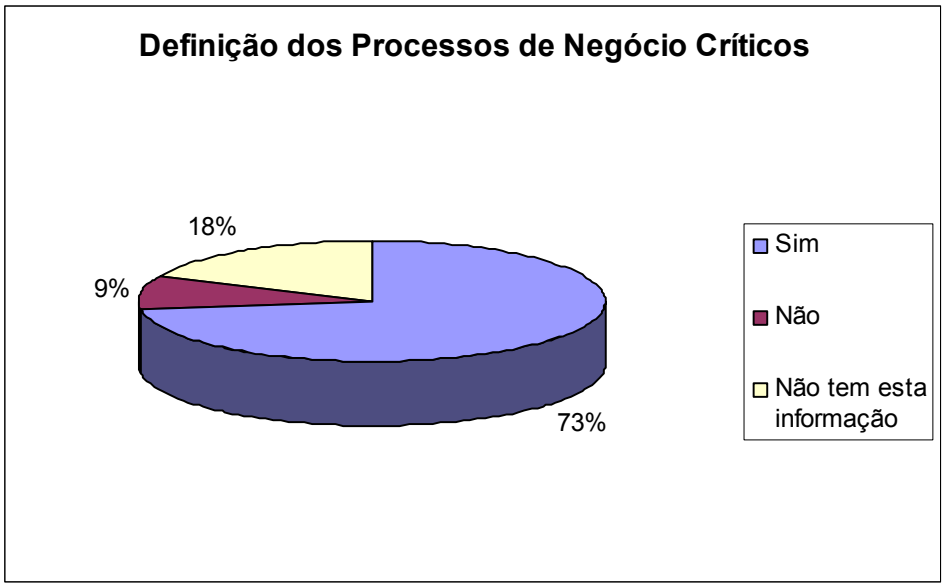


4. Quantos equipamentos a empresa possui?

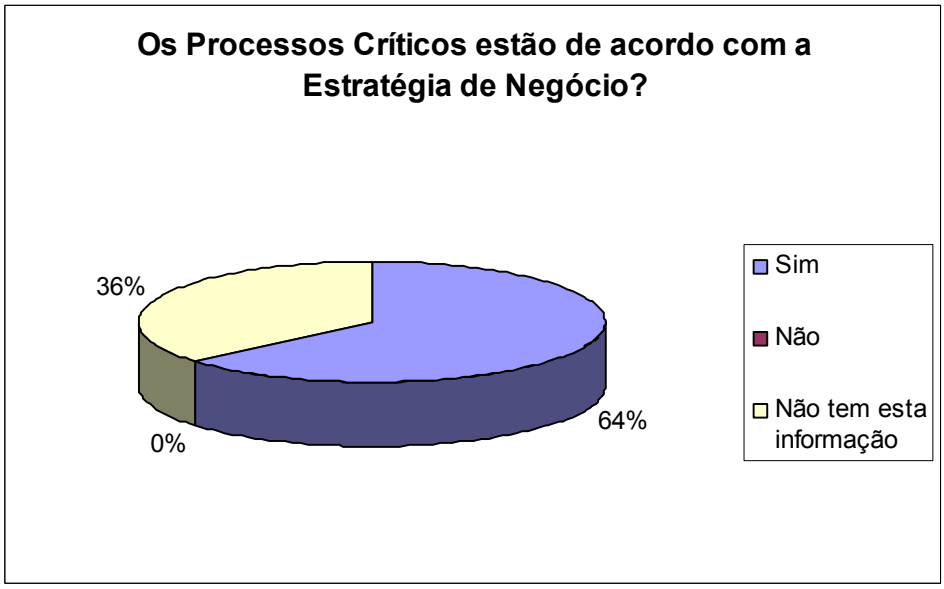


ESTRATÉGIA DE NEGÓCIO DA EMPRESA

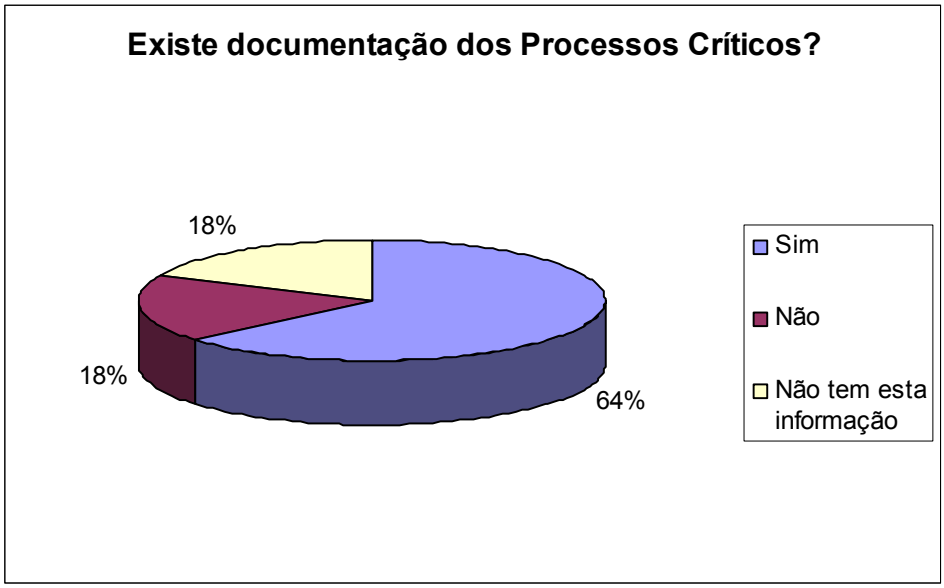
5. Existe uma definição bem clara de quais os principais processos de negócio da empresa? (Departamentos e atividades críticas)



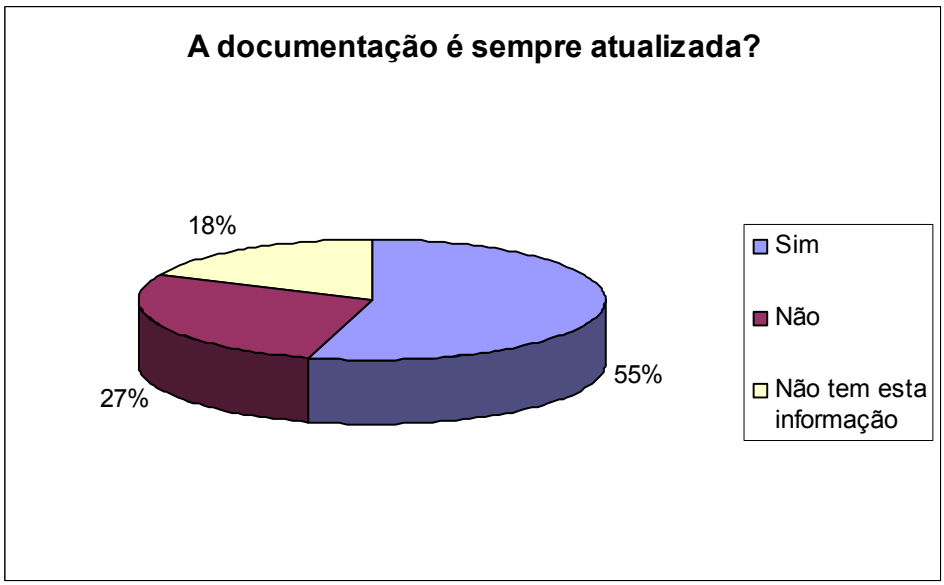
6. Estes processos críticos estão de acordo com a estratégia de negócio da empresa?



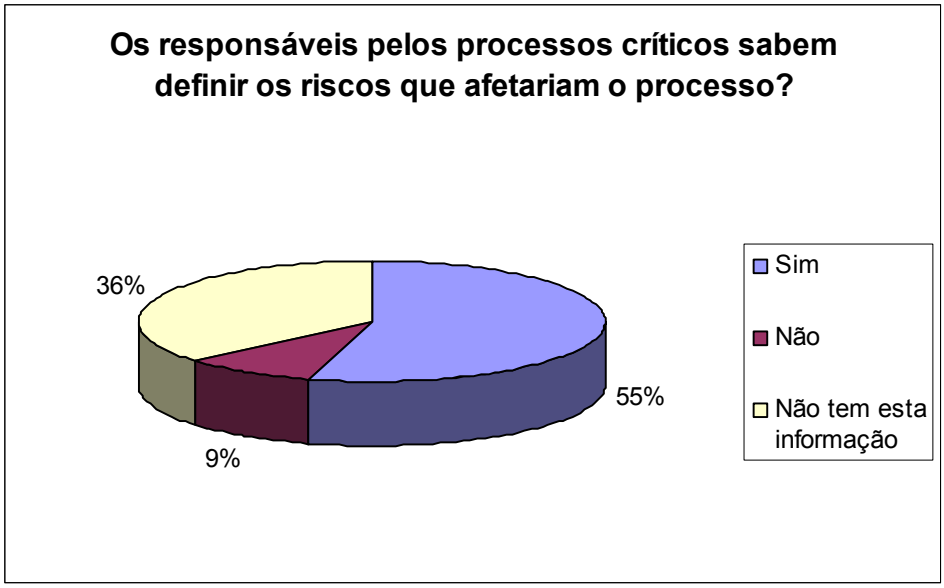
7. **Existe uma documentação das atividades e responsáveis pelos processos críticos?**



8. **Esta documentação é constantemente atualizada?**



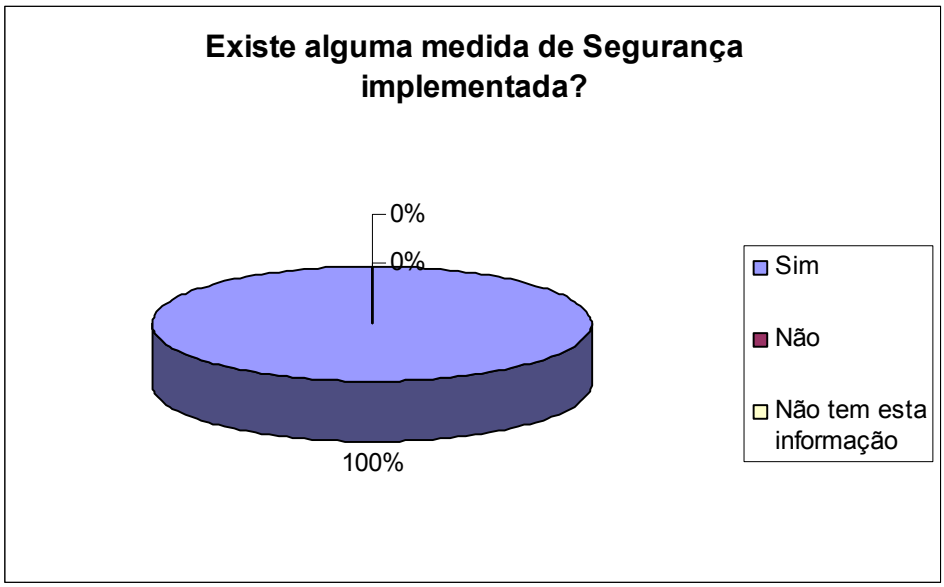
9. **Os responsáveis pelos processos críticos conhecem as atividades e sabem definir os riscos que afetariam sua realização com sucesso?**



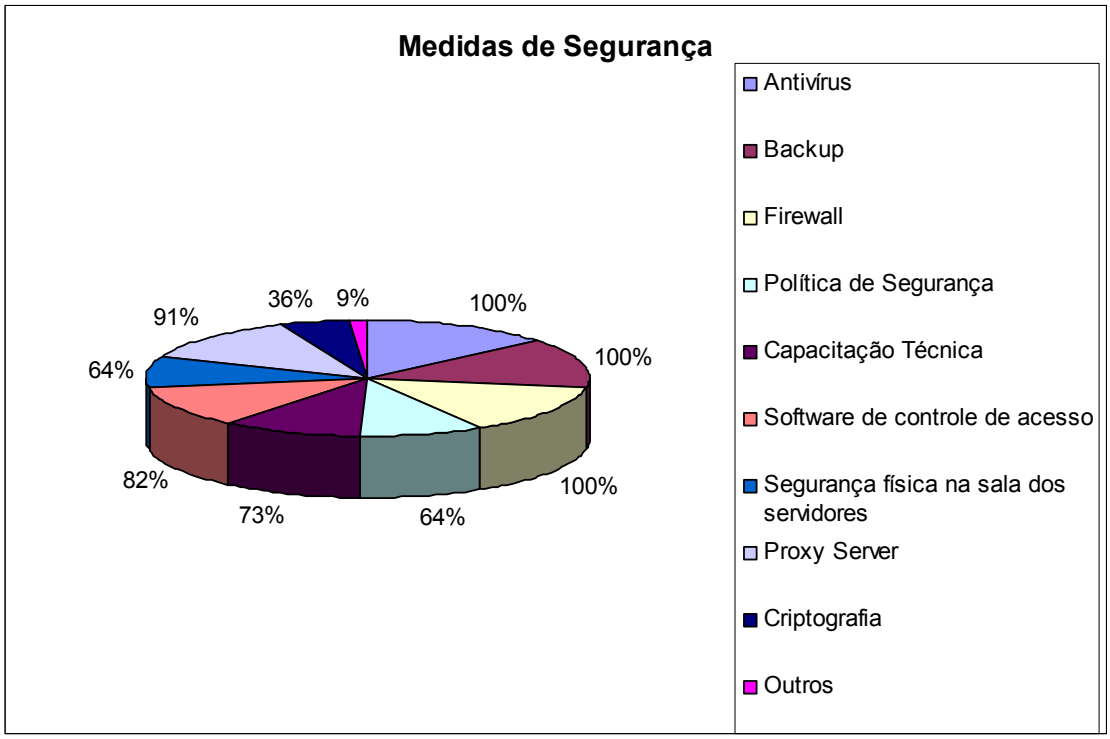
10. **Além dos recursos humanos, existem outros recursos que suportam os processos críticos da empresa?**

SEGURANÇA DA INFORMAÇÃO

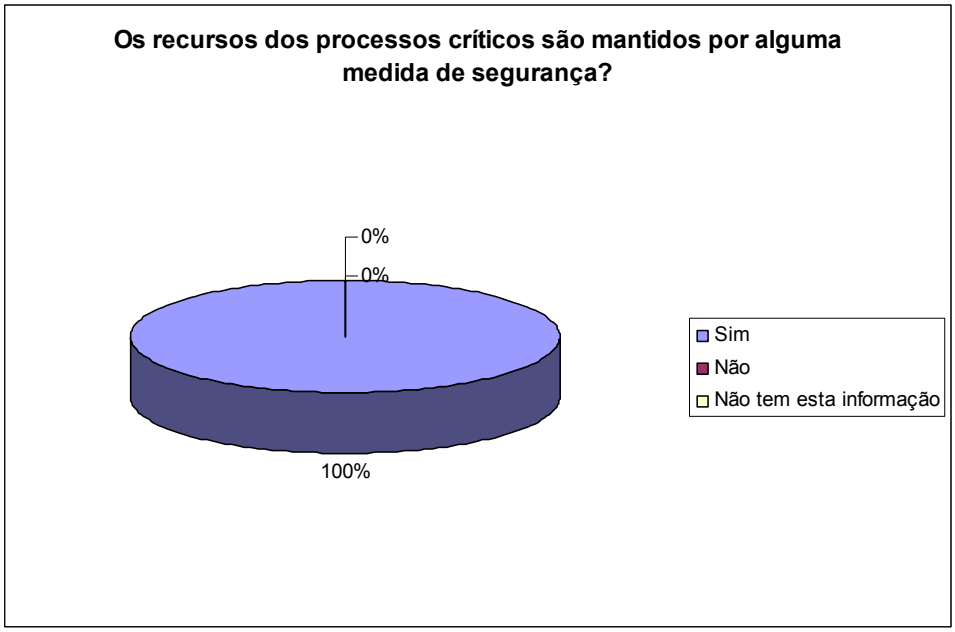
11. A empresa possui alguma medida de segurança implementada?



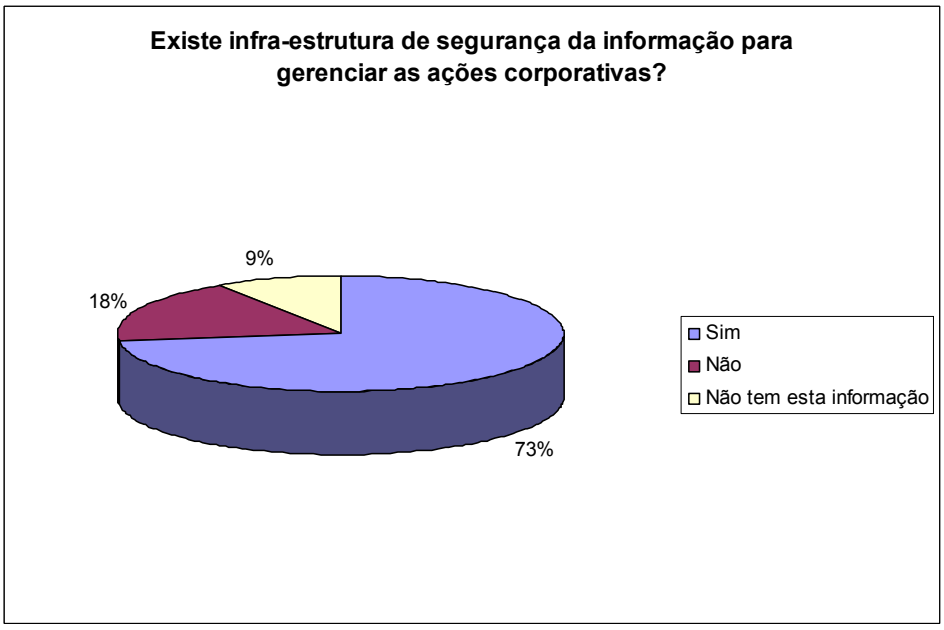
12. Quais são as medidas?



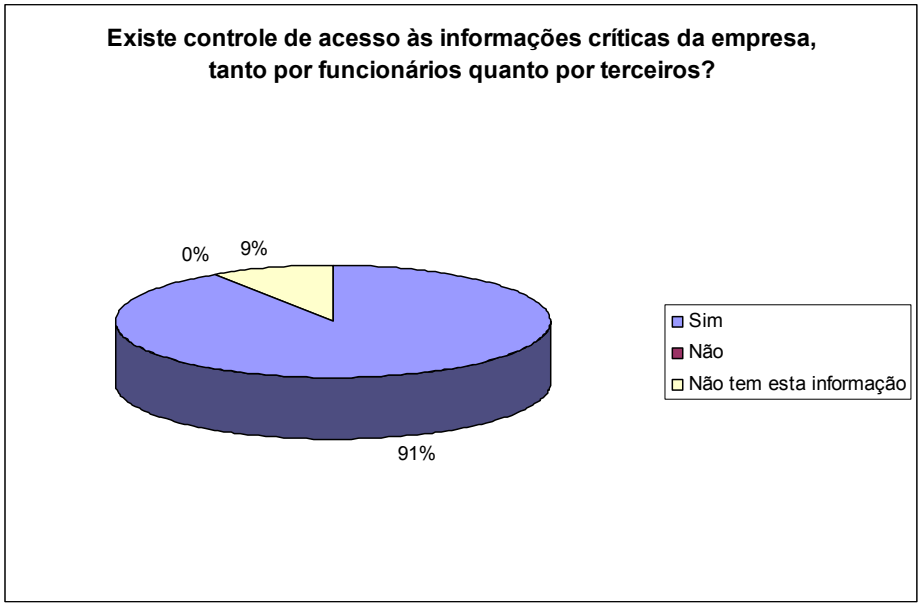
13. Os recursos que suportam os processos críticos da empresa são mantidos por alguma medida de segurança?



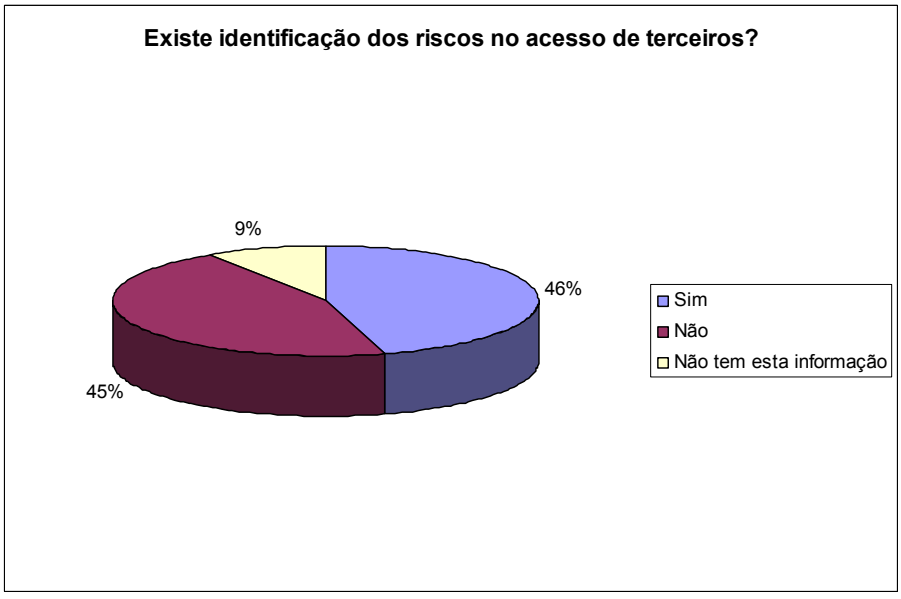
14. Existe infra-estrutura de segurança da informação para gerenciar as ações corporativas?



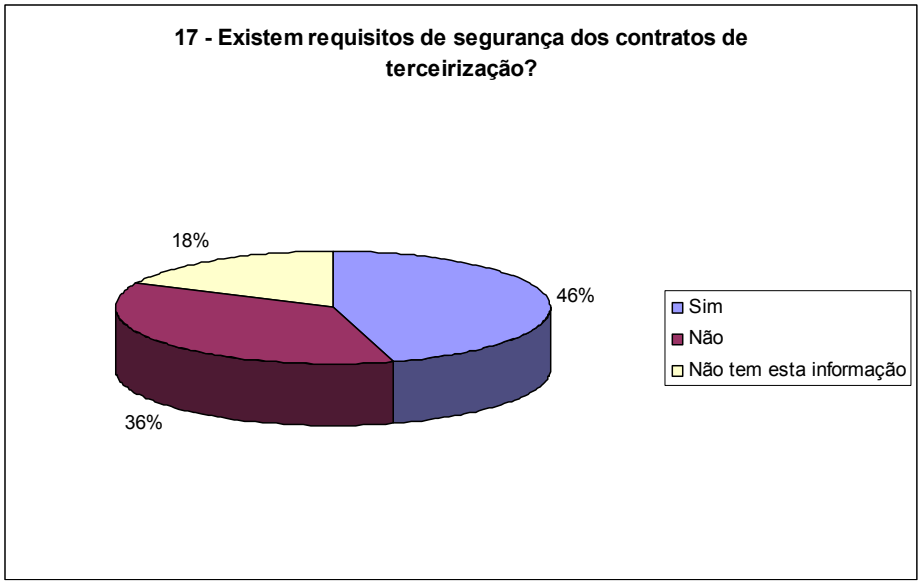
15. Existe controle de acesso às informações críticas da empresa, tanto por funcionários quanto por terceiros?



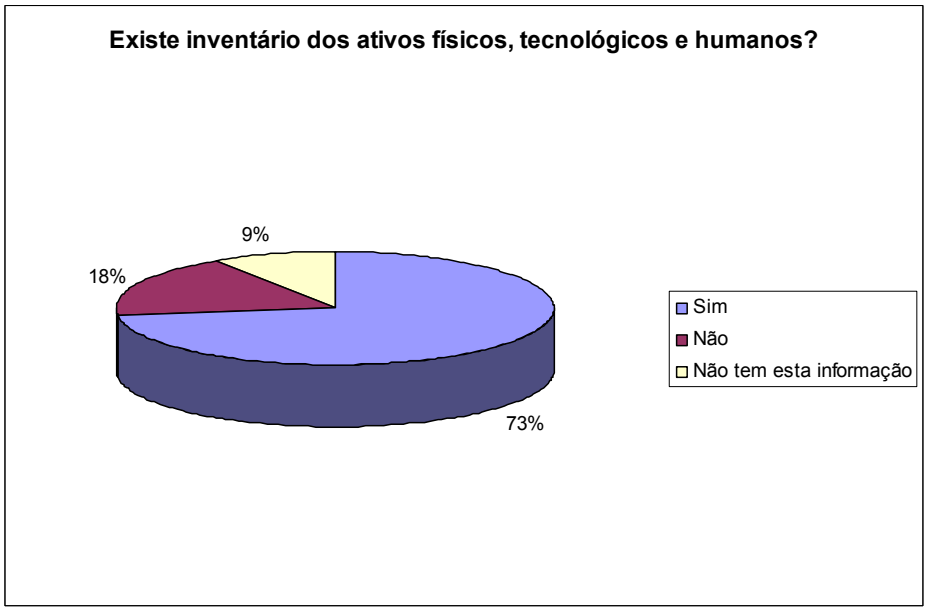
16. Existe identificação dos riscos no acesso de terceiros?



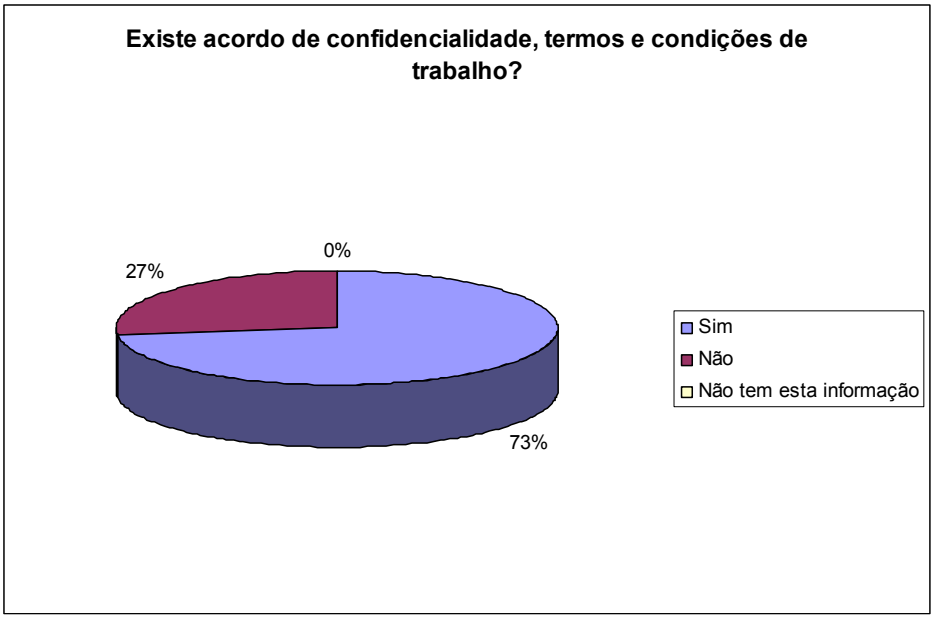
17. Existem requisitos de segurança dos contratos de terceirização?



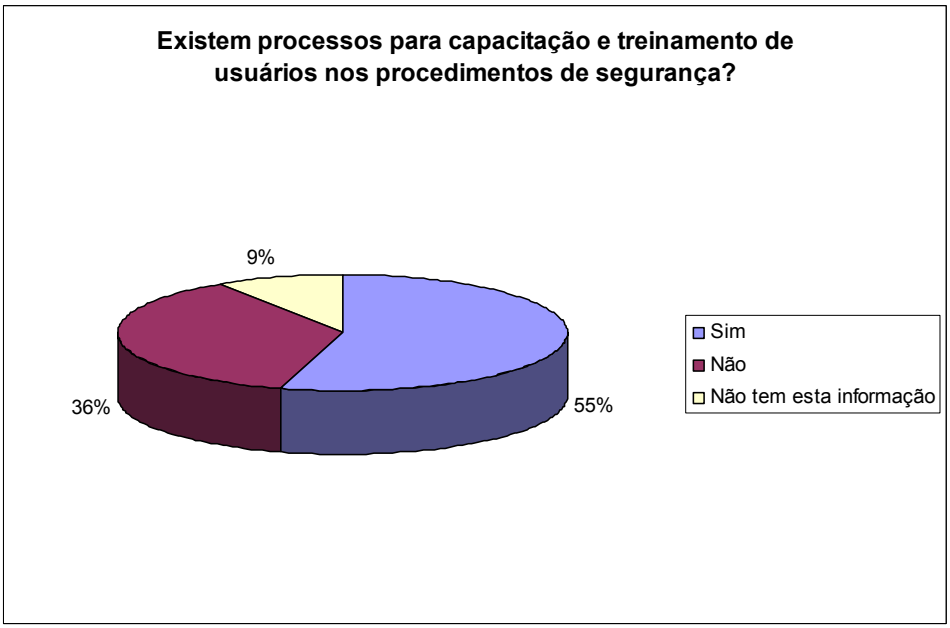
18. Existe inventário dos ativos físicos, tecnológicos e humanos?



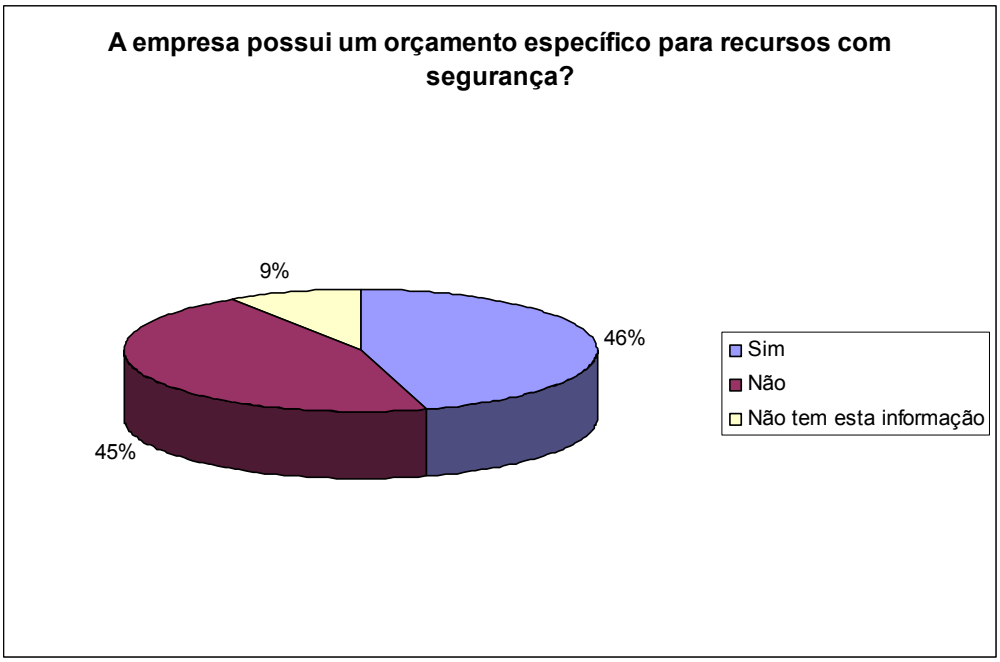
19. Existe acordo de confidencialidade, termos e condições de trabalho?



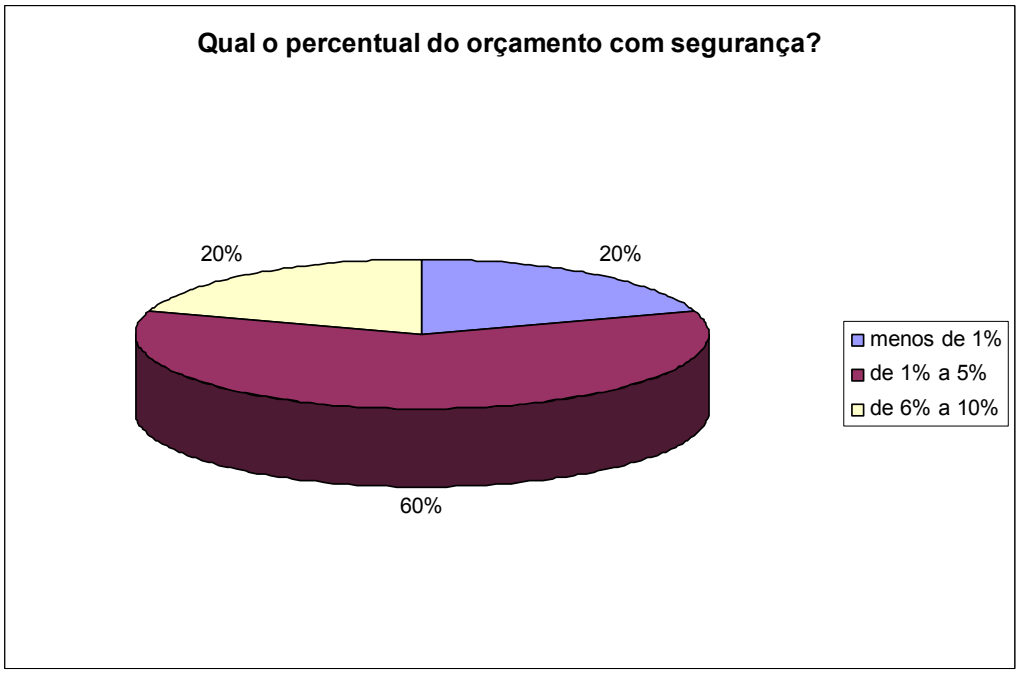
20. Existem processos para capacitação e treinamento de usuários nos procedimentos de segurança?



21. A empresa possui um orçamento específico para recursos com segurança?

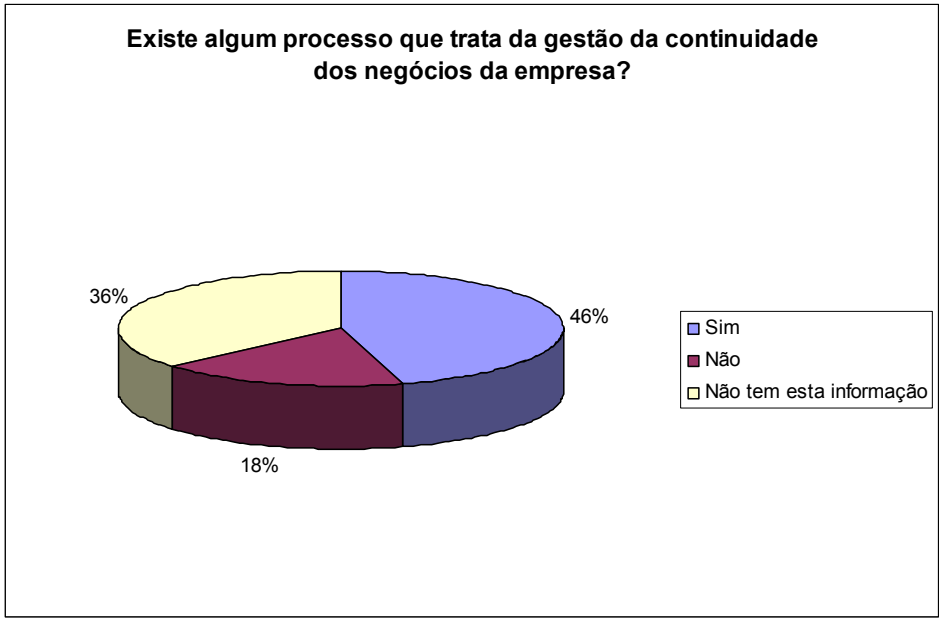


22. Qual o percentual do orçamento com segurança?

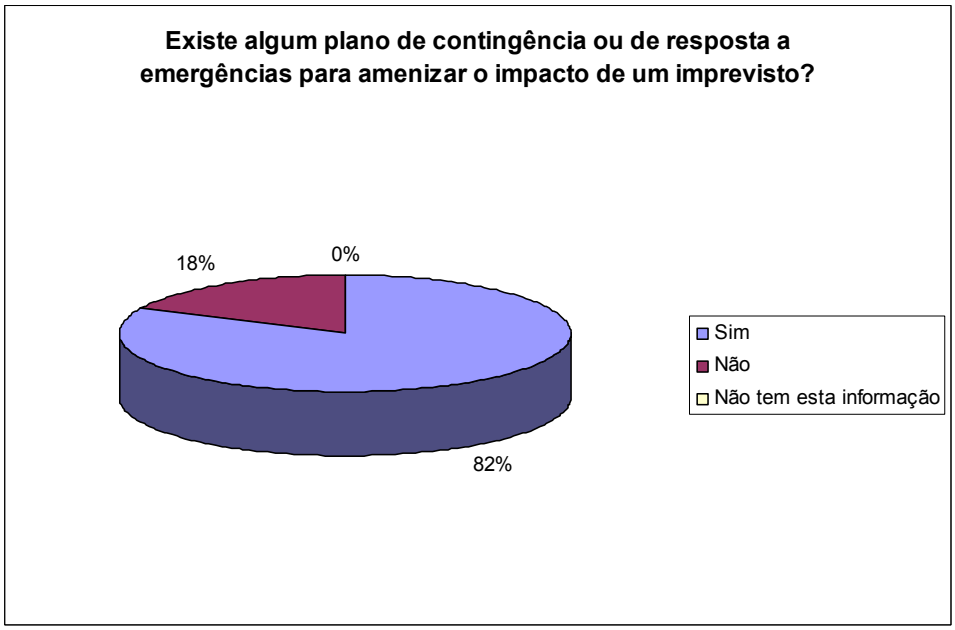


PLANO DE CONTINUIDADE DO NEGÓCIO

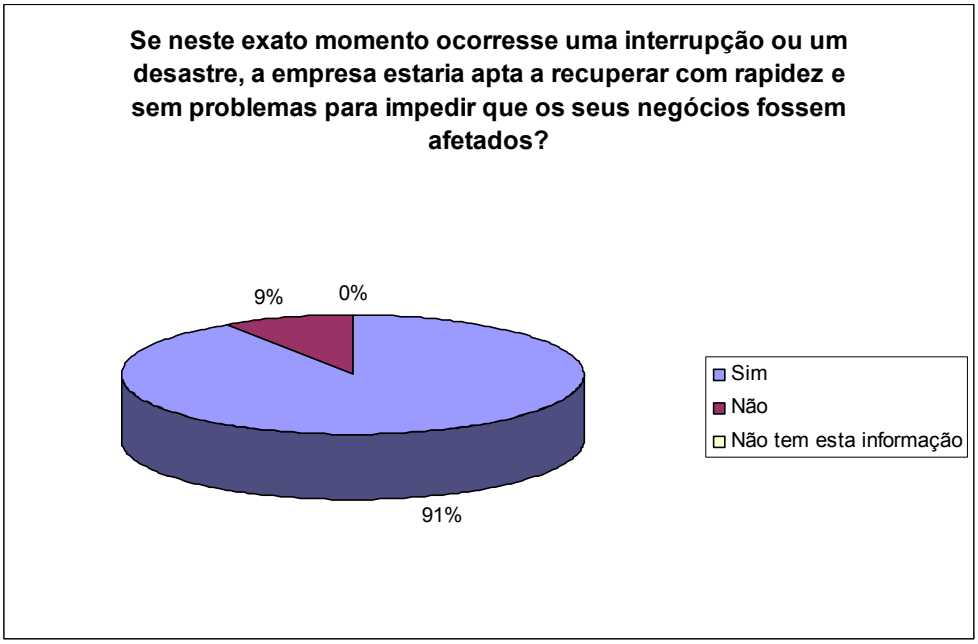
23. Existe algum processo que trata da gestão da continuidade dos negócios da empresa?



24. No caso da ocorrência de imprevistos, existe algum plano de contingência ou de resposta a emergências para amenizar o impacto deste imprevisto?

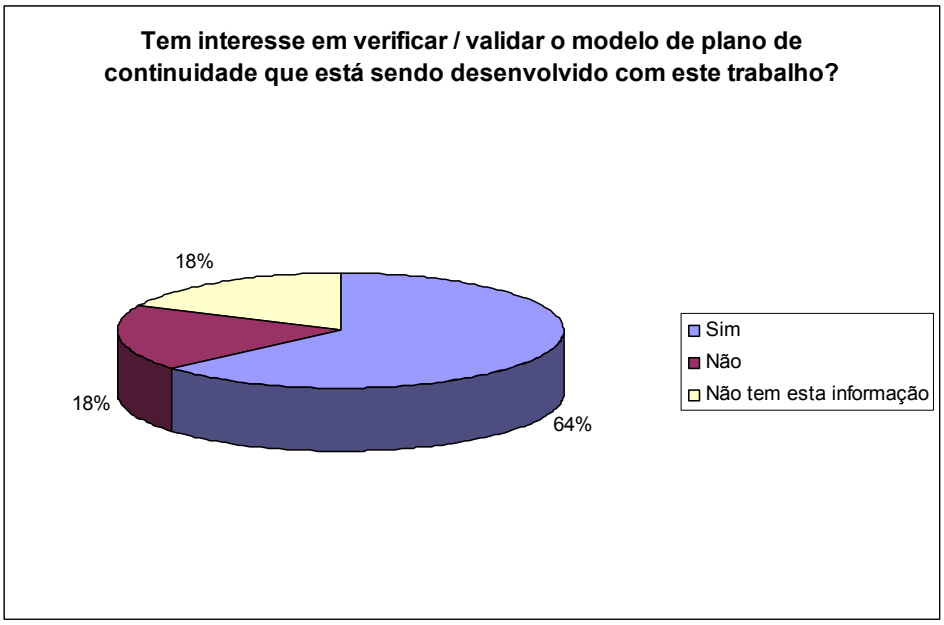


25. Se neste exato momento ocorresse uma interrupção ou um desastre, a empresa estaria apta a recuperar com rapidez e sem problemas para impedir que os seus negócios fossem afetados?



MODELO DE PCN

26. Tem interesse em verificar / validar o modelo de plano de continuidade que está sendo desenvolvido com este trabalho?



ANEXO 2 – FORMULÁRIOS AUXILIARES DO MODELO GUIA PARA ELABORAÇÃO DO PCN

1. IDENTIFICAÇÃO DO NEGÓCIO

Identificação da Empresa	
Razão Social	
Nome Fantasia	
CNPJ	
Endereço	
Inscrição Estadual	
Inscrição Municipal	
Data de Fundação	
Telefone	
Fax	
E-mail	
Site	

Identificação dos Sócios			
Nome	**Perfil**	**Atribuição**	**Participação Societária**

Definição do Negócio	
Segmento de Atuação	
Histórico	
Cenário Atual	
Tendências Futuras	
Visão	
Análise Estratégica (Oportunidades, Ameaças,	

Pontos Fortes e Pontos Fracos)	
Fatores Críticos de Sucesso	
Missão	
Metas	

Mercado	
Identificação do Público Alvo	
Identificação dos Clientes	
Segmentação	
Tamanho do Mercado Atual	
Concorrentes (Empresa, Porte, % do Mercado, Informações Operacionais)	
Tendências	
Participação Pretendida no Mercado	
Metas	

2. IDENTIFICAÇÃO DOS PROCESSOS DO NEGÓCIO

Processo de Negócio (Setor ou Unidade)	
Nome do Processo de Negócio:	
Localização:	
Nome do Responsável:	
Cargo:	Telefones:
E-mail:	Data de Admissão:
Nome do Substituto:	
Cargo:	Telefones:
E-mail:	Data de Admissão:
Função básica:	
Funcionários envolvidos (Nome / Cargo):	
Este processo de negócio é: ( ) Próprio ( ) Terceirizado pela empresa	
Gestor responsável:	

3. IDENTIFICAÇÃO DA INFRA-ESTRUTURA DOS PROCESSOS DO NEGÓCIO

Neste formulário serão relacionados todos os componentes utilizados para a execução de cada processo de negócio, indicando quais as respectivas quantidades e quais são consideradas como indispensável (críticas).

Componentes da Infra-Estrutura do Negócio			
Tipo	**Nome do Componente**	**Quantidades Utilizadas**	**É crítica? (S/N)**

Tempo de Inoperância Suportável **(sem que haja conseqüências para a empresa)**	Até ( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6 ( )12 ( )24 ( )30 ( )48 ( )90 Em ( ) horas ( ) minutos ( ) Não pode parar ( ) Não sabe

No formulário abaixo serão relacionados os processos de negócios que dependem das atividades realizadas por este processo de negócio.

Processos Dependentes			
Nome do Processo	**Unidade de Negócio (Setor)**	**Responsável**	**Telefones**

No formulário abaixo serão relacionados os processos de negócios dos quais este depende, sua execução, indicando em qual setor (unidade de negócio) é realizado e seus respectivos contatos.

Processos Dependentes			
Nome do Processo	**Unidade de Negócio (Setor)**	**Responsável**	**Telefones**

4. IDENTIFICAÇÃO DAS AMEAÇAS AOS PROCESSOS DO NEGÓCIO

Naturais

Descrição	Vulnerabilidade 0 – 1 – 2 – 3	Descrição	Vulnerabilidade 0 – 1 – 2 – 3
( ) Incêndio		( ) Inundação	
( ) Outra (Qual?)		( ) Outra (Qual?)	

Humanas

Descrição	Vulnerabilidade 0 – 1 – 2 – 3	Descrição	Vulnerabilidade 0 – 1 – 2 – 3
( ) Vírus de Computador		( ) Greves Externas	
( ) Manipulação indevida de dados e sistemas		( ) Erro humano (dano não-intencional)	
( ) Sabotagem de dados		( ) Ataque terrorista	
( ) Seqüestro de elemento-chave de processo		( ) Roubo e/ou furto de recursos	
( ) Falha do prestador de serviço/parceiro		( ) Seqüestro de dados e informações	
( ) Acesso indevido às instalações		( ) Sabotagem de instalações	
( ) Outra (Qual?)		( ) Outra (Qual?)	

Tecnológicas

Descrição	Vulnerabilidade 0 – 1 – 2 – 3	Descrição	Vulnerabilidade 0 – 1 – 2 – 3
( ) Falha em aplicativo (software)		( ) Falha no sistema de refrigeração	
( ) Falha em sistema operacional		( ) Falha em hardware	

( ) Falha em rede interna (LAN)		( ) Falha em rede externa (WAN)	
( ) Falha na entrada de dados		( ) Interrupção de energia	
( ) Falha em correio eletrônico		( ) Falha em instalação elétrica	
( ) Falha em telecom - voz		( ) Falha em telecom - dados	
( ) Outra (Qual?)		( ) Outra (Qual?)	

Físicas

Descrição	Vulnerabilidade 0 – 1 – 2 – 3	Descrição	Vulnerabilidade 0 – 1 – 2 – 3
( ) Queda de aeronave		( ) Problema estrutural ou de instalação	
( ) Falta d'água		( ) Proximidade de depósito de inflamáveis	
( ) Problema estrutural ou de instalação		( ) Rompimento de tubulação interna (água, esgoto, gás ou vapores)	
( ) Outra (Qual?)		( ) Outra (Qual?)	