Segurança da Informação

Plano de Contingência

Segurança da Informação

Plano de Contingência (1/2)

Consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização, no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não conseguiram evitar.

Segurança da Informação

Plano de Contingência (2/2)

Documento onde estão definidas as responsabilidades estabelecidas em uma organização, para atender a uma emergência e também contêm informações detalhadas sobre as características da área ou sistemas envolvidos.

É desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais.

Segurança da Informação

Objetivo (1/3)

O objetivo de um plano de contingência é servir como guia para esquematizar a execução de ações a serem tomadas para a continuidade dos serviços essenciais das áreas de negócios, que dependem da TI.

Segurança da Informação

Objetivo (2/3)

Para minimizar os esforços, reduzir os custos e tornar um plano de contingência factível, somente os serviços essenciais para dar continuidade aos negócios da organização devem ser contemplados;

Segurança da Informação

Objetivo (3/3)

Cada área de negócio da empresa, será responsável por definir o que é considerado como serviço essencial, levando em conta o grau de criticidade do(s) sistema(s) avaliado(s) para os negócios da organização.

Segurança da Informação

Conceitos utilizados para definição de escopo em um

Plano de Contingência

Segurança da Informação

Grau de Criticidade

Define-se como o grau de importância de uma rotina operacional/administrativa para a área de negócio.

(- valor financeiro envolvido; - dependência imperativa para continuidade dos serviços; - volume de informações que inviabilize controles alternativos; - outros;)

Segurança da Informação

Prioridade (1/2)

É definida em função da importância que os aplicativos têm para o fluxo organizacional, como os decorrentes de fluxo de atividades (folha de pagamentos, recolhimento de tributos, etc);

Segurança da Informação

Prioridade (2/2)

O critério de prioridade está subordinado ao critério de criticidade, isto é, em primeiro lugar será processado o aplicativo mais crítico;

No caso de dois sistemas com igual grau de criticidade, processa-se primeiro o aplicativo que naquele instante tiver mais prioridade.

Segurança da Informação

Período Crítico

É definido pelo tempo máximo que uma área de negócios pode conviver sem o auxílio dos serviços da Tecnologia da Informação;

Segurança da Informação

Sistema Crítico

Sistema sem o qual as atividades da organização sofrerão um impacto severo, correndo o risco pleno de paralização do negócio;

Segurança da Informação

Sistema Semicrítico

Sistema sem o qual as atividades da organização sofrerão um impacto sensível, porém não correndo o risco pleno de paralização do negócio;

Segurança da Informação

Sistema não crítico

Sistema sem o qual as atividades da organização não sofrerão impacto, não trazendo risco para o negócio;

Segurança da Informação

Fato gerador da Contingência

É o evento que desencadeou a situação de emergência, que por sua vez obrigou a ativação do plano de contingência.

Segurança da Informação

Características desejáveis de um Plano de Contingência (1/5)

O plano de contingência deve ser desenvolvido envolvendo todas as áreas sujeitas a catástrofes, tanto as de sistema de informática quanto as de negócio e não deve ser de exclusiva responsabilidade da área de Tecnologia da Informação.

Segurança da Informação

Características desejáveis de um Plano de Contingência (2/5)

Um plano de contingência não precisa necessariamente utilizar equipamentos iguais aos envolvidos no evento gerador da contingência;

Segurança da Informação

Características desejáveis de um Plano de Contingência (3/5)

Seus itens deverão estar todos documentados e a atualização desta documentação deve ser feita sempre que necessário.

Testes periódicos no plano também são necessários para verificar se o processo continua válido.

Segurança da Informação

Características desejáveis de um Plano de Contingência (4/5)

O detalhamento das medidas deve ser apenas o necessário para sua rápida execução, sem excesso de informações que podem ser prejudiciais numa situação crítica.

Segurança da Informação

Características desejáveis de um Plano de Contingência (5/5)

Por ser um caminho alternativo e temporário para dar continuidade aos negócios, deve-se escolher o mínimo de recursos para manter a disponibilidade necessária.

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (1/8)

- ***Identificar todos os processos** de negócio atendidos pela TI;*

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (2/8)

***- Avaliar os impactos no negócio**, ou seja, para cada processo identificado, avaliar o impacto que a sua falha representa para a organização, levando em consideração também as interdependências entre processos. Como resultado deste trabalho será possível identificar todos processos críticos para a sobrevivência da organização;*

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (3/8)

***- Identificar riscos e definir cenários possíveis de falha** para cada um dos processos críticos, levando em conta a probabilidade de ocorrência de cada falha, provável duração dos efeitos, conseqüências resultantes, custos inerentes e os limites máximos aceitáveis de permanência da falha sem a ativação da respectiva medida de contingência;*

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (4/8)

***- Identificar medidas para cada falha**, ou seja, listar as medidas a serem postas em prática caso a falha aconteça, incluindo até mesmo o contato com a imprensa;*

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (5/8)

***- Definir ações necessárias para operacionalização das medidas** cuja implantação dependa da aquisição de recursos físicos e/ou humanos (por exemplo, aquisição de gerador e combustível para um sistema de contingência de energia elétrica);*

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (6/8)

***- Estimar custos de cada medida*, comparando-os aos custos incorridos no caso da contingência não existir;**

- Definir forma de monitoramento após a falha;

Segurança da Informação

Elementos a serem utilizados para a concepção do Plano de Contingência (7/8)

***- Definir critérios de ativação do plano**, como tempo máximo aceitável de permanência da falha;*

***- Identificar o responsável pela ativação do plano**, normalmente situado em um alto nível hierárquico da companhia;*

Segurança da Informação

Elementos a serem utilizados para a concepção do

Plano de Contingência (8/8)

- Identificar os responsáveis em colocar em prática as medidas de contingência definidas, tendo cada elemento responsabilidades formalmente definidas e nominalmente atribuídas.

Segurança da Informação

Exercício

Plano de Contingência

Identifique 10 processos atendidos pela TI que você considera crítico para o negócio da sua empresa e pense num plano de contingência básico para eles.