TEMA 03
Planos de Contingência

Habilidades:

- Entender as estruturas dos documentos de contingência.
- Elaborar planos de contingência.
- Compreender e desenvolver relatórios de níveis de risco e prevenir riscos.

Planos de contingência na segurança da informação **são documentos que estabelecem diretrizes e procedimentos a serem seguidos em casos de incidentes ou situações de emergência que possam comprometer a segurança dos dados e sistemas de uma organização**. Estes planos visam minimizar os impactos dos eventos adversos, o que possibilita uma resposta rápida e eficiente para proteger a integridade, confidencialidade e disponibilidade das informações.
Os planos de contingência são **essenciais para garantir uma resposta adequada a incidentes de segurança da informação**. Eles permitem uma ação rápida e coordenada, o que minimiza os danos causados por incidentes e reduz a interrupção das operações da organização. Ao implementar e manter planos de contingência eficazes, as organizações demonstram seu compromisso com a segurança da informação e sua capacidade de lidar com situações adversas de forma eficiente.
Você pôde acompanhar no tema anterior que políticas de segurança são essenciais para a Segurança da Informação. A **prevenção** é um dos fundamentos mais importantes para evitar desastres com os ativos de informação.
O objetivo de um plano de contingência é traçar estratégias corretivas, ou seja, é definir as atitudes para incidentes correlativos com falhas de segurança, como vazamento de dados, ataques em aplicações e interrupções de serviço indesejadas que trarão prejuízo ao negócio. Do mesmo modo que a política de segurança é moldada para um negócio específico, um plano de contingência será feito na medida das preocupações compreendidas.
O **processo de desenvolvimento de planos de contingência** se dá, basicamente, por alguns passos básicos: o levantamento, organização e classificação, elaboração dos planos para cada ameaça encontrada, documentação e testes.

Um plano de contingência geralmente inclui as seguintes etapas:

- Identificação de ameaças: Nessa fase, são identificadas as ameaças potenciais que podem afetar a segurança da informação, como **ataques cibernéticos**, **desastres naturais**, **falhas de hardware ou software**, entre outros.
- Avaliação de riscos: Processo que envolve a análise das ameaças identificadas, considerando sua probabilidade de ocorrência e impacto potencial nos sistemas e dados. Com base nessa análise, **os riscos são classificados de acordo com sua criticidade**.
- Definição de estratégias de resposta: Com base na análise de riscos, são estabelecidas estratégias de resposta para cada tipo de ameaça. Isso pode incluir **ações de mitigação**, como a **instalação de firewalls ou sistemas de backup**, ou **medidas de resposta**, como a **interrupção de serviços** ou a **ativação de equipes de resposta a incidentes**.
- Elaboração dos procedimentos de resposta: Nessa etapa, são definidos os procedimentos detalhados que devem ser seguidos em cada tipo de incidente. Podemos apontar como a **designação de responsabilidades**, **comunicação de emergência**, **recuperação de sistemas e dados**, e **investigação e análise de incidente**s.
- Treinamento e conscientização: É fundamental que todos os envolvidos na organização sejam treinados e estejam cientes dos procedimentos de contingência. Isso engloba a **realização de exercícios de simulação e treinamentos regulares** para garantir que as equipes estejam preparadas para lidar com os incidentes.

- Testes e revisões: Os planos de contingência devem ser testados periodicamente para garantir sua eficácia. **Testes de simulação, como exercícios de resposta a incidentes**, ajudam a identificar falhas e ajustar os procedimentos, se necessário. Além disso, é importante **revisar os planos regularmente** para garantir que estejam atualizados e alinhados com as mudanças no ambiente de segurança.

Levantamento

Nesta etapa, será realizado todo o levantamento de todos os ativos que podem passar por algum momento de crise e impacte diretamente no ciclo de trabalho, como computadores, servidores, serviços e aplicações, rede de internet, etc. Aqui também é importante acrescentar os fatores humanos, e quais tarefas impactam o meio.

Classificação e Organização

Com todos os ativos críticos coletados, chegou a hora de organizá-los para definir quais são os mais propensos a serem interrompidos do que outros e definir o nível de risco para cada um, e priorizar as que demandam de mais atenção. Aqui também será descrito de que forma cada falha atua.
Uma das ferramentas mais utilizadas para mapearmos os riscos encontrados no cotidiano com os ativos de informação é a **matriz de risco**. Matriz de risco é uma ferramenta capaz de classificar o nível de risco em pontos, o que permite ao profissional de segurança priorizar cada problema e facilitar o desenvolvimento de um plano de contingência para cada risco identificado.
A matriz é definida a partir de 2 (dois) critérios: a **probabilidade**, que representa a possibilidade de o risco acontecer, e o **impacto**, que é a consequência causada por ele. Enquanto a probabilidade fica na coluna(x), o impacto fica na linha(x). Os atributos vão do nulo ao extremo, e cada um representa uma porcentagem de chance.

- Nulo/Insignificante – 10%
- Baixo – 20%
- Moderado – 50%
- Alto – 70%
- Extremo – 90/100%

A compreensão de riscos é diferente para cada empresa, por isso, cada organização deve fazer a sua e tirar as conclusões cabíveis perante os níveis de probabilidade e impacto.

Uma matriz de risco é uma ferramenta visual e analítica que ajuda a avaliar e priorizar riscos com base em suas probabilidades de ocorrência e seus impactos. Vamos criar um exemplo de matriz de risco e apresentar um esquema gráfico para melhor entendimento.

Exemplo de Matriz de Risco

Vamos supor que temos os seguintes riscos identificados em uma organização:

1. Falha no servidor principal
2. Vazamento de dados sensíveis
3. Ataque de ransomware
4. Interrupção de energia
5. Erro humano na operação

Para cada risco, determinamos a probabilidade de ocorrência e o impacto. Em seguida, utilizamos esses valores para plotar cada risco na matriz.

Probabilidade
- Nulo/Insignificante – 10%
- Baixo – 20%
- Moderado – 50%
- Alto – 70%
- Extremo – 90/100%

Impacto
- Nulo/Insignificante – 10%
- Baixo – 20%
- Moderado – 50%
- Alto – 70%
- Extremo – 90/100%

Valores de Exemplo

Risco	Probabilidade	Impacto
Falha no servidor principal	Moderado (50%)	Alto (70%)
Vazamento de dados sensíveis	Alto (70%)	Extremo (90%)
Ataque de ransomware	Moderado (50%)	Extremo (90%)
Interrupção de energia	Baixo (20%)	Moderado (50%)
Erro humano na operação	Alto (70%)	Moderado (50%)

Desenvolvimento dos planos de contingência

Agora que temos nossos ativos organizados e classificados, podemos iniciar o processo de desenvolvimento de ações necessárias para mitigar ou impedir que tais falhas aconteçam. Caso, por exemplo, ocorra uma falha que acarrete na exclusão de alguns dados do banco, quais as ações necessárias para que os desenvolvedores consigam realizar o procedimento de backup e retomam o serviço o mais rápido possível.

Documentação

Aqui, elaboramos um documento que abordará o passo a passo de resolução para cada problema classificado, ou seja, o que precisa ser feito se cada falha citada acima for iminente. É necessário que esta documentação seja muito clara para que cada setor compreenda perfeitamente o que fazer caso ocorra algo.

Testes

Nesta última etapa, realizaremos os testes para averiguar se os planos de contingência criados realmente funcionam. Normalmente, simulações das situações-problema são realizadas e os planos de contingência aplicados, analisando se todos os procedimentos, realmente, resolverão o problema.

RESUMO:

Os planos de contingência possuem um papel fundamental em todos os contextos institucionais. Eles são competentes para **projetar táticas que solucionarão ou ou irão atenuar circunstâncias críticas no dia a dia, que podem afetar diretamente a proteção dos dados**. As estratégias de contingência são absolutamente cruciais em qualquer esfera corporativa. São responsáveis por formular abordagens que enfrentarão ou irão suavizar eventos de crise na rotina, que podem

influenciar diretamente na segurança dos dados.

Desafio

Imagine uma situação em sua sala de aula/laboratório de informática, que pode ocasionar algum tipo de interrupção, prejudicando a você e seus colegas. Crie um plano de contingência para esta situação-problema utilizando os passos que você viu acima.

Desafio: Plano de Contingência para uma Interrupção no Laboratório de Informática

Situação-Problema

Imagine que em sua sala de aula/laboratório de informática, ocorra uma falha no servidor principal que gere a perda temporária do acesso aos arquivos e aplicações necessárias para o desenvolvimento das atividades acadêmicas. Essa interrupção pode prejudicar a realização de aulas práticas e o acesso a materiais de estudo importantes.

Plano de Contingência

1. Identificação de Ameaças

- Falha no servidor principal.
- Interrupção de energia elétrica.
- Ataque cibernético (ransomware).
- Erro humano ao manusear os sistemas do servidor.

2. Avaliação de Riscos

Risco	Probabilidade	Impacto
Falha no servidor principal	Moderado (50%)	Alto (70%)
Interrupção de energia	Baixo (20%)	Moderado (50%)
Ataque de ransomware	Moderado (50%)	Extremo (90%)
Erro humano	Alto (70%)	Moderado (50%)

3. Definição de Estratégias de Resposta

- **Falha no servidor principal:** Implementação de um servidor backup e realização de backups diários.
- **Interrupção de energia:** Instalação de no-breaks para garantir a continuidade temporária da energia e verificar a possibilidade de geradores de emergência.
- **Ataque de ransomware:** Utilização de software antivírus e firewalls, além de treinamentos regulares sobre segurança da informação.
- **Erro humano:** Desenvolvimento de um programa de treinamento para todos os usuários do laboratório.

4. Elaboração dos Procedimentos de Resposta

Falha no Servidor Principal

1. Notificar o administrador de TI imediatamente.
2. Ativar o servidor backup.
3. Restaurar os dados a partir do backup mais recente.
4. Verificar a integridade dos dados restaurados.
5. Informar aos usuários sobre a resolução do problema.

Interrupção de Energia
1. Utilizar no-breaks para manter a energia temporariamente.
2. Notificar a administração do campus sobre a falha.
3. Verificar a possibilidade de ativação de geradores de emergência.
4. Restaurar as operações normais assim que a energia for reestabelecida.

Ataque de Ransomware
1. Isolar o servidor infectado da rede.
2. Executar a ferramenta de remoção de malware.
3. Restaurar os dados a partir do backup mais recente.
4. Realizar uma análise pós-incidente para identificar e corrigir vulnerabilidades.

Erro Humano
1. Identificar a natureza do erro.
2. Restaurar o sistema ou dados a partir do backup mais recente, se necessário.
3. Realizar um treinamento adicional para o usuário envolvido.
4. Atualizar os procedimentos e documentações para evitar erros futuros.

5. Treinamento e Conscientização
- Realizar sessões de treinamento regular para todos os usuários do laboratório, cobrindo o uso correto dos sistemas, boas práticas de segurança da informação, e procedimentos de resposta a incidentes.

6. Testes e Revisões
- Realizar testes de simulação a cada seis meses para avaliar a eficácia do plano de contingência.
- Revisar e atualizar o plano de contingência anualmente ou sempre que houver mudanças significativas na infraestrutura do laboratório ou nos procedimentos de TI.

Documentação do Plano de Contingência

Plano de Contingência do Laboratório de Informática

1. Introdução
- Objetivo do plano: Garantir a continuidade das operações do laboratório de informática em caso de incidentes críticos.

2. Identificação de Ameaças
- Detalhamento das ameaças potenciais e seus impactos.

3. Avaliação de Riscos
- Tabela de classificação de riscos com probabilidade e impacto.

4. Estratégias de Resposta
- Descrição das estratégias para mitigação e resposta a cada ameaça.

5. Procedimentos de Resposta
- Passo a passo detalhado dos procedimentos a serem seguidos em caso de incidentes.

6. Treinamento e Conscientização
- Plano de treinamento e conscientização para todos os usuários.

7. Testes e Revisões

- Plano de testes e revisões periódicas para garantir a eficácia contínua do plano.

Testes

- Realizar simulações de falhas no servidor principal e interrupções de energia para garantir que os procedimentos de resposta sejam eficazes.
- Avaliar a resposta da equipe de TI e dos usuários do laboratório durante os testes.
- Ajustar o plano conforme necessário com base nos resultados dos testes.

Resumo

Este plano de contingência é projetado para minimizar os impactos de incidentes críticos no laboratório de informática, garantindo a continuidade das operações e a proteção dos dados e sistemas. Através da identificação de ameaças, avaliação de riscos, definição de estratégias de resposta, elaboração de procedimentos detalhados, treinamento e conscientização, e testes regulares, a organização estará preparada para lidar com situações adversas de forma eficiente e eficaz.

ATIVIDADES:

1. O que é um plano de contingência na segurança da informação e qual é o seu propósito principal?

Um plano de contingência na segurança da informação é um documento que estabelece diretrizes e procedimentos a serem seguidos em casos de incidentes ou situações de emergência que possam comprometer a segurança dos dados e sistemas de uma organização. Seu propósito principal é minimizar os impactos dos eventos adversos, possibilitando uma resposta rápida e eficiente para proteger a integridade, confidencialidade e disponibilidade das informações.

2. Quais são os elementos-chave que devem ser considerados ao desenvolver um plano de contingência eficaz?

Os elementos-chave que devem ser considerados ao desenvolver um plano de contingência eficaz incluem:

- **Identificação de ameaças:** Reconhecer potenciais ameaças que possam afetar a segurança da informação.
- **Avaliação de riscos:** Analisar a probabilidade e o impacto de cada ameaça identificada.
- **Definição de estratégias de resposta:** Estabelecer ações de mitigação e resposta para cada tipo de ameaça.
- **Elaboração dos procedimentos de resposta:** Definir procedimentos detalhados para serem seguidos em cada tipo de incidente.
- **Treinamento e conscientização:** Treinar e conscientizar todos os envolvidos sobre os procedimentos de contingência.
- **Testes e revisões:** Realizar testes periódicos e revisar o plano regularmente para garantir sua eficácia e atualização.

3. Por que é importante treinar e conscientizar as equipes sobre os procedimentos de um plano de contingência?

Treinar e conscientizar as equipes sobre os procedimentos de um plano de contingência é importante porque:

- **Preparação:** Garante que todos saibam exatamente o que fazer em caso de um incidente, permitindo uma resposta rápida e coordenada.
- **Redução de erros:** Minimiza o risco de erros durante a execução dos procedimentos, aumentando a eficácia da resposta.

- **Confiança:** Aumenta a confiança dos funcionários na capacidade da organização de lidar com incidentes, melhorando o moral e a cooperação.
- **Conformidade:** Assegura que a organização cumpra com regulamentações e padrões de segurança que exigem treinamento regular em segurança da informação.

4. Explique a importância de realizar testes e exercícios de simulação em um plano de contingência.

Realizar testes e exercícios de simulação em um plano de contingência é importante porque:
- **Validação:** Confirma que os procedimentos e estratégias definidos no plano são eficazes e funcionam conforme esperado.
- **Identificação de falhas:** Ajuda a identificar pontos fracos ou falhas no plano que precisam ser corrigidos.
- **Treinamento prático:** Proporciona uma oportunidade para que a equipe pratique os procedimentos em um ambiente controlado, melhorando sua preparação.
- **Ajustes:** Permite ajustar e melhorar o plano com base nos resultados dos testes e simulações.
- **Atualização:** Garante que o plano esteja sempre atualizado e alinhado com as mudanças no ambiente de segurança e nas operações da organização.

5. Cite três exemplos de situações de emergência que podem requerer a ativação de um plano de contingência na segurança da informação.

Três exemplos de situações de emergência que podem requerer a ativação de um plano de contingência na segurança da informação são:
- **Ataque de ransomware:** Um malware que criptografa dados e exige pagamento de resgate para a liberação.
- **Falha no servidor principal:** Uma interrupção no servidor que hospeda sistemas críticos, impedindo o acesso a dados e aplicações essenciais.
- **Vazamento de dados sensíveis:** Exposição não autorizada de informações confidenciais que podem prejudicar a privacidade e a segurança da organização e seus clientes.22