



CRIPTOGRAFIA E SEGURANÇA DE DADOS

Aula Teórica 13

SUMÁRIO:

Planeamento de segurança, estratégias de continuidade de
negócio


Docentes: S. Mavie & A. Covele

UEM, 2024

Planeamento de segurança, estratégias de continuidade de negócio

Objectivos:

- Definir a função do gestão no desenvolvimento, manutenção e aplicação de políticas, padrões, práticas, procedimentos e diretrizes de segurança de informações
- Descrever o que é um plano de segurança da informação, identificar seus principais componentes e explicar como ele suporta o programa de segurança da informação
- Discuta como uma organização institucionaliza suas políticas, padrões e práticas usando programas de educação, treinamento e conscientização
- Explicar o que é o plano de contingência e como ele se relaciona com plano de resposta a incidentes, planeamento de recuperação de desastre e planos de continuidade de negócios



Planeamento e Governança da Segurança da Informação

Planeamento e Governança da Segurança da Informação

- O planeamento estratégico define a direção de longo prazo a ser tomada por toda a organização e por cada uma de suas partes componentes. O planeamento estratégico deve orientar os esforços organizacionais e direcionar os recursos para objetivos específicos e claramente definidos.
- Depois que uma organização desenvolve uma estratégia geral, ela gera um plano estratégico geral, estendendo essa estratégia geral aos planos estratégicos para as principais divisões. Cada nível de cada divisão, então, traduz esses objetivos do plano em objetivos mais específicos para o nível abaixo. Para executar essa ampla estratégia e transformar a estratégia geral em ação, a equipe executiva deve primeiro definir as responsabilidades individuais. A conversão de metas de um nível estratégico para o próximo nível inferior talvez seja mais arte do que ciência.
- Ela depende da capacidade de um executivo de conhecer e compreender os objetivos estratégicos de toda a organização, de conhecer e apreciar as habilidades estratégicas e táticas de cada unidade dentro da organização e de negociar com colegas, superiores e subordinados. Essa combinação de habilidades ajuda a alcançar o equilíbrio adequado entre metas e capacidades.


Planeamento e Governança da Segurança da Informação

- Uma vez que o plano estratégico geral da organização é traduzido em planos estratégicos para cada divisão ou operação principal, o próximo passo é traduzir esses planos em objetivos táticos que se movam para alcançar realizações específicas, mensuráveis, realizáveis e vinculadas ao tempo.
- O processo de **planeamento estratégico** procura transformar declarações amplas, gerais e amplas em objetivos mais específicos e aplicados. Planos estratégicos são usados para criar planos táticos, que por sua vez são usados para desenvolver planos operacionais
- **Planeamento tático**, se concentra em empreendimentos de curto prazo que serão concluídos dentro de um ou dois anos. O processo de planeamento tático divide cada meta estratégica em uma série de objetivos incrementais. Cada objetivo em um plano tático deve ser específico e deve ter uma data de entrega dentro de um ano a partir do início do plano. Orçamento, alocação de recursos e pessoal são componentes críticos do plano tático. São frequentemente criados para projetos específicos.
- **Planos operacionais**, são derivados dos planos táticos, para organizar o desempenho contínuo das tarefas no dia-a-dia. Um plano operacional inclui as tarefas necessárias para todos os departamentos relevantes, bem como os requisitos de comunicação e relatório, que podem incluir reuniões semanais, relatórios de andamento e outras tarefas associadas. Esses planos devem refletir a estrutura organizacional, com cada subunidade, departamento ou equipe de projeto conduzindo seu próprio planejamento operacional e relatórios. A comunicação frequente e o feedback das equipes para os gerentes de projeto e / ou líderes de equipe e, em seguida, até os vários níveis de gerenciamento, tornarão o processo de planejamento como um todo mais gerenciável e bem-sucedido.

Planeamento e Governança da Segurança da Informação

Os cinco objetivos da governança de segurança da informação são:

- Alinhamento estratégico de segurança da informação com estratégia de negócios para suportar objetivos organizacionais;
- Gestão de riscos através da execução de medidas apropriadas para gerenciar e mitigar ameaças aos recursos de informação;
- Gestão de recursos utilizando conhecimento e infra-estrutura de segurança da informação de forma eficiente e eficaz;
- Medição de desempenho medindo, monitorando e relatando métricas de governança de segurança de informações para garantir que os objetivos organizacionais sejam alcançados;
- Entrega de valor otimizando os investimentos em segurança da informação em apoio aos objetivos organizacionais.




Programa de Educação, Treinamento e Conscientização sobre Segurança

Programa de Educação, Treinamento e Conscientização sobre Segurança

- Após a organização definir as políticas que orientarão seu programa de segurança e selecionar um modelo geral de segurança criando ou adaptando uma estrutura de segurança e um plano de implementação detalhado correspondente, é hora de implementar um programa de educação, treinamento e conscientização sobre segurança (ETCS).
- O programa ETCS é de responsabilidade do CISO e é uma medida de controle projetada para reduzir as incidências de violações acidentais de segurança pelos funcionários.
- Os erros dos funcionários estão entre as principais ameaças aos ativos de informação, por isso vale a pena gastar os recursos da organização para desenvolver programas para combater essa ameaça.

Programa de Educação, Treinamento e Conscientização sobre Segurança

- **Educação de Segurança** – Todos em uma organização precisam ser treinados e informados sobre segurança da informação, mas nem todos os membros da organização precisam de um diploma ou certificado formal em segurança da informação. Quando a gerência concorda que a educação formal é apropriada, um funcionário pode investigar cursos disponíveis em instituições locais de ensino superior ou educação continuada.
- **Treinamento de Segurança** – O treinamento de segurança fornece informações detalhadas e instruções práticas aos funcionários para prepará-los para executar suas tarefas com segurança. O gerenciamento da segurança da informação pode desenvolver treinamento interno personalizado ou terceirizar o programa de treinamento.
- **Conscientização sobre Segurança** – Um dos programas menos frequentemente implementados, mas mais benéficos, é o programa de conscientização de segurança. Um programa de conscientização de segurança é projetado para manter a segurança da informação na vanguarda das mentes dos usuários. Esses programas não precisam ser complicados nem caros. Bons programas podem incluir boletins informativos, cartazes de segurança, vídeos, quadros de avisos, panfletos e bugigangas. O boletim informativo de segurança é o método mais eficaz em termos de custo de divulgação de informações de segurança e notícias para o funcionário. Os boletins informativos podem ser distribuídos por meio de cópia impressa, e-mail ou intranet.



Política, Padrões e Práticas de Segurança da Informação

Política, Padrões e Práticas de Segurança da Informação

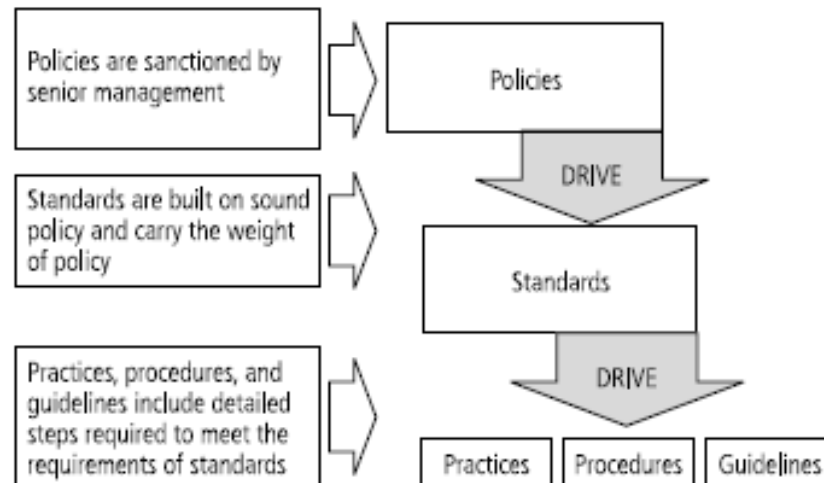
- A gestão de todas as comunidades de interesse, incluindo a equipe geral, a tecnologia da informação e a segurança da informação, deve fazer das políticas a base de todo o planejamento, projeto e implantação da segurança da informação.
 - Políticas direcionam como as questões devem ser abordadas e as tecnologias devem ser usadas. As políticas não especificam o funcionamento adequado do equipamento ou software, essas informações devem ser colocadas nos padrões, procedimentos e práticas dos manuais dos usuários e na documentação dos sistemas. Além disso, a política nunca deve contradizer a lei, porque isso pode criar uma responsabilidade significativa para a organização. Para uma discussão sobre esse problema.
 - Os programas de segurança de qualidade começam e terminam com a política. A segurança da informação é principalmente um problema de gestão, não técnico, e a política é uma ferramenta de gestão que obriga o pessoal a funcionar de maneira a preservar a segurança dos ativos de informação. Políticas de segurança são o controle mais barato para executar, mas o mais difícil de implementar corretamente. A sua criação e disseminação exigem apenas o tempo e o esforço da equipe de gerenciamento. Mesmo que a equipe de gestão contrate um consultor externo para ajudar a desenvolver políticas, os custos são mínimos comparados aos de controles técnicos. No entanto, a política de formatação é difícil porque a política deve:
 - Nunca entre em conflito com leis
 - Levante-se no tribunal, se desafiado
- Ser administrado adequadamente por meio de disseminação e aceitação documentada

Política, Padrões e Práticas de Segurança da Informação

- Política é um plano ou curso de ação que transmite instruções da alta gerência de uma organização para aqueles que tomam decisões, agem e cumprem outras tarefas. Políticas são leis organizacionais que ditam comportamento aceitável e inaceitável dentro da organização. Como as leis, as políticas definem o que é certo, o que está errado, quais são as penalidades por violar as políticas e qual é o processo de apelação.
- Padrões são declarações mais detalhadas do que deve ser feito para cumprir a política. Eles têm os mesmos requisitos para conformidade como políticas. Os padrões podem ser informais ou parte de uma cultura organizacional, como nos padrões de fato.

Política, Padrões e Práticas de Segurança da Informação

- A gerência deve definir três tipos de políticas de segurança, de acordo com o Instituto Nacional de Padrões e Publicações Especiais da Tecnologia 800-14 (uma publicação que será discutida com muito mais detalhes mais adiante neste capítulo):
 - Políticas de segurança da informação da empresa
 - Políticas de segurança específicas do problema
 - Políticas de segurança específicas de sistemas





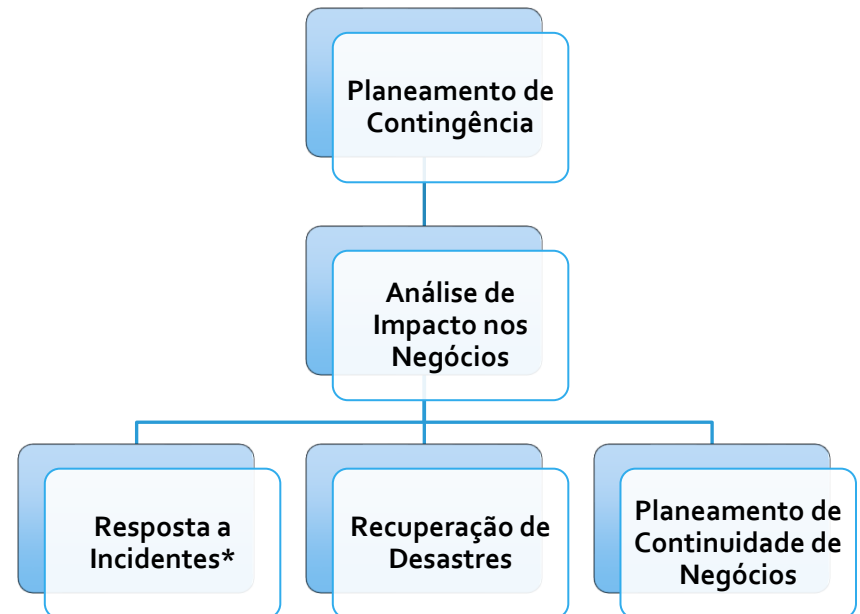
Estratégias de Continuidade

Estratégias de Continuidade

- Em caso de um ataque - interna ou externa, intencional ou acidental, humana ou não humana, chata ou catastrófica, os gestores de segurança de informação devem estar prontos para agir quando ocorrer um ataque bem-sucedido. Por isso, é fundamental que o gestor da segurança da informação tenha uma plano estratégico para assegurar a disponibilidade contínua dos sistemas de informação.
- Os planos de contingência podem ser: planos de resposta a incidentes, planos de recuperação de desastres e planos de continuidade de negócios. Em algumas organizações, elas podem ser tratadas como um único plano integrado.

Estratégias de Continuidade

- O plano de contingência é preparado pela organização para antecipar, reagir e se recuperar de eventos que ameaçam a segurança da informação e os ativos de informações na organização e, subsequentemente, para restaurar os modos normais de operações de negócios da organização.

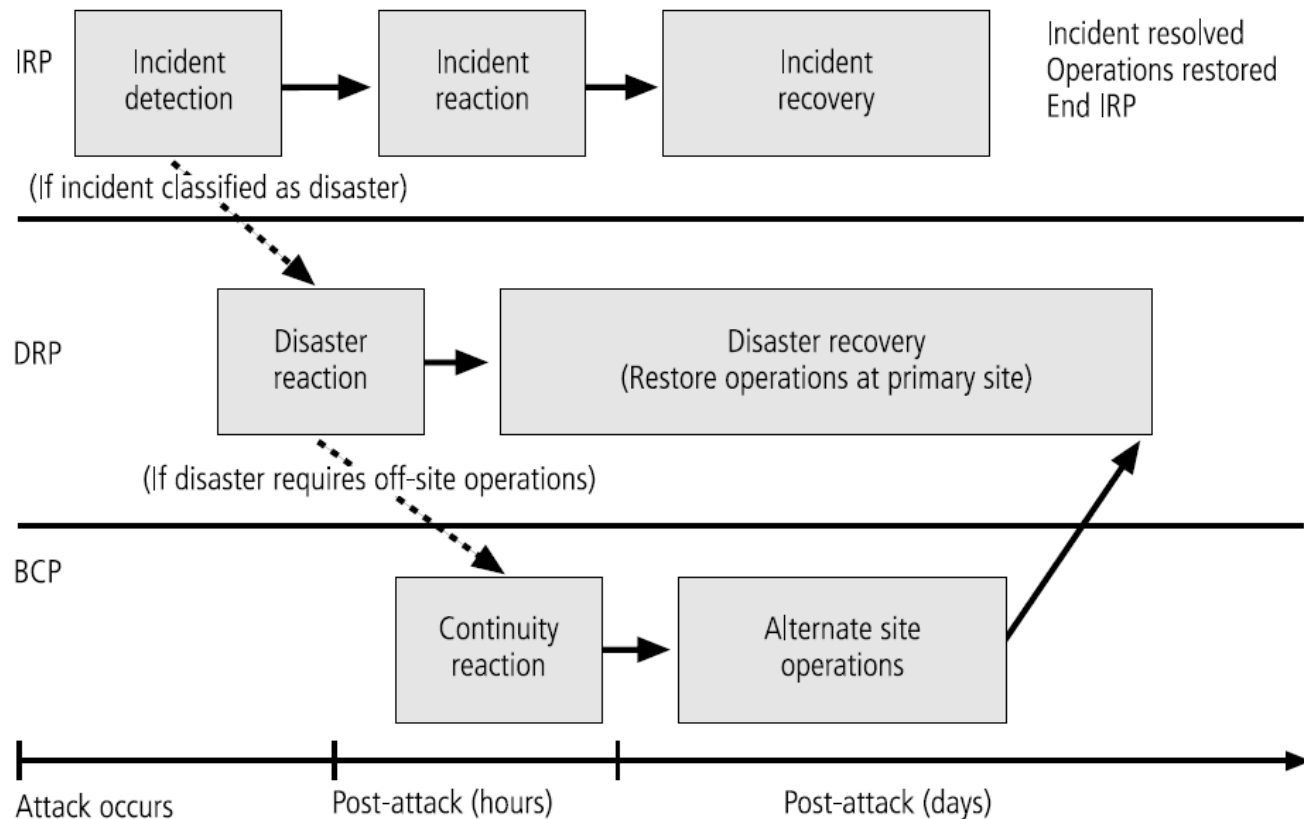


*Um incidente é qualquer ataque claramente identificado aos ativos de informações da organização que possam ameaçar a confidencialidade, a integridade ou a disponibilidade dos ativos.

Estratégias de Continuidade

- Um **Plano de Resposta a Incidentes (RI)** aborda a identificação, classificação, resposta e recuperação de um incidente. Se concentra na resposta imediata, mas se o ataque aumentar ou for desastroso (por exemplo, incêndio, inundação, terremoto ou apagão total), o processo avançará para a Recuperação de Desastres e o plano de Continuidade de Negócios.
- Um **Plano de Recuperação de Desastres (RD)** aborda a preparação e recuperação de um desastre, seja natural ou feito pelo homem. Normalmente se concentra na restauração de sistemas no local original após a ocorrência de desastres e está intimamente associada ao plano de Continuidade de Negócios.
- Um **Plano de Continuidade de Negócios (CN)** garante que as funções críticas de negócios continuem caso ocorra um incidente ou desastre catastrófico. Quando o dano é grande ou contínuo, exigindo mais do que a simples restauração de informações e recursos de informações, o plano de CN ocorre simultaneamente com o plano de Recuperação de Desastres .

Estratégias de Continuidade



Estratégias de Continuidade

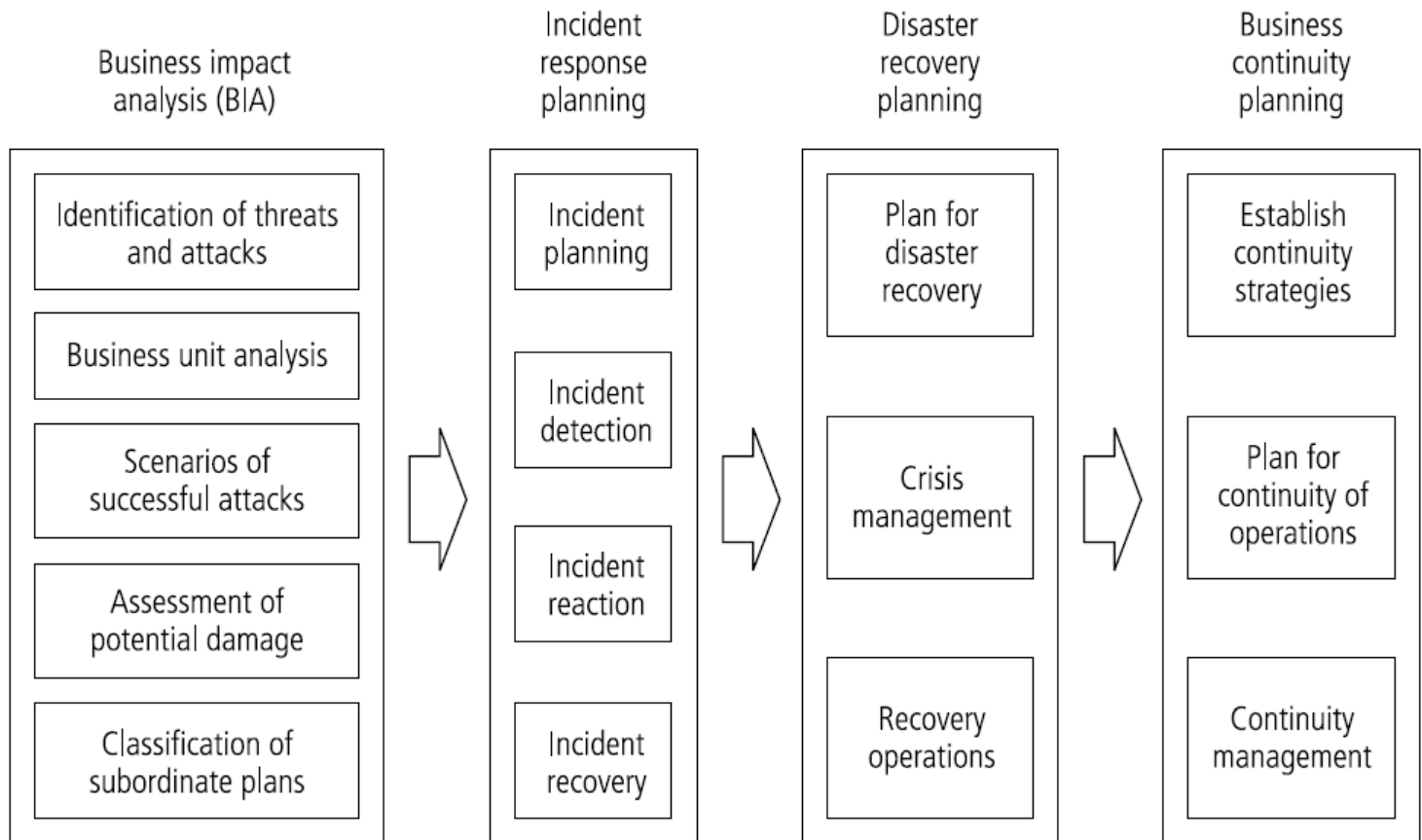
- Antes que qualquer planejamento possa começar, é necessário criar uma Equipe de Gestão de Planejamento de Contingência (EGPC), que pode consistir dos seguintes membros:
 - Campeão: O projeto de planejamento de contingência deve ter um gerente de alto nível para apoiar, promover e endossar os resultados do projeto. Este poderia ser o CIO ou, idealmente, o CEO.
 - Gerente de projetos: Um gerente de projeto, possivelmente um gerente de nível médio ou mesmo o CISO, deve liderar o projeto e garantir que um processo de planejamento de projeto sólido seja usado, um plano de projeto completo e útil seja desenvolvido e os recursos do projeto sejam administrados com prudência para atingir as metas do projeto.
 - Membros da equipe: Os membros da equipe devem ser gerentes ou seus representantes de várias comunidades de interesse: negócios, tecnologia da informação e segurança da informação.
 - Os gerentes de negócios representativos, familiarizados com as operações de suas respectivas áreas funcionais, devem fornecer detalhes sobre suas atividades e sua importância para a sustentabilidade geral dos negócios.
 - Os gerentes de tecnologia da informação da equipe do projeto devem estar familiarizados com os sistemas que podem estar em risco e com os planos de RI, RD e CN necessários para fornecer conteúdo técnico.
 - Os gerentes de segurança da informação devem supervisionar o planejamento de segurança do projeto e fornecer informações sobre as ameaças, vulnerabilidades, ataques e requisitos de recuperação necessários.

Estratégias de Continuidade

O EGPC é responsável por várias tarefas, incluindo as seguintes:

- Obtenção de compromisso e apoio do gestor senior
- Elaboração do documento do plano de contingência
- Realização da Análise de Impacto nos Negócios, que inclui:
 - Auxiliando na identificação e priorização de ameaças e ataques
 - Auxiliando na identificação e priorização de funções de negócios
- Organizando as equipes subordinadas, como:
 - Resposta ao incidente
 - Recuperação de desastres
 - Continuidade de negócios
 - Gerenciamento de crise

Estratégias de Continuidade



Análise de Impacto nos Negócios (AIN)

- É a primeira fase no desenvolvimento do processo de planejamento de contingência. Consiste em uma investigação e avaliação do impacto que vários ataques podem ter na organização.
- Inicia onde o processo de avaliação de risco termina. Começando com uma lista priorizada de ameaças e vulnerabilidades identificadas no processo de gestão de riscos e adiciona informações sobre a criticidade dos sistemas envolvidos e uma avaliação detalhada das ameaças e vulnerabilidades às quais eles estão sujeitos.
- É uma componente crucial dos estágios iniciais de planejamento, pois fornece cenários detalhados do impacto potencial que cada ataque poderia ter sobre a organização. Ajudando a determinar o que a organização deve fazer para responder o ataque, minimizar o dano do ataque, recuperar dos efeitos e retornar às operações normais.
- A gestão de risco abordagem de gerenciamento de riscos identifica ameaças, vulnerabilidades e ataques para determinar quais controles podem proteger as informações, enquanto a AIN assume que um ataque foi bem-sucedido apesar desses controles e tenta responder a pergunta, o que você faz agora.

Análise de Impacto nos Negócios (AIN)

- A equipe de planejamento de contingência conduz o Análise de Impacto nos Negócios nas seguintes etapas:
 - Identificação e priorização de ataques de ameaças
 - Análise da unidade de negócios
 - Atacar o desenvolvimento do cenário de sucesso
 - Avaliação potencial de danos
 - Classificação do plano subordinado

Planeamento de respostas a incidentes

- O planeamento de resposta a incidentes inclui a identificação, classificação e resposta a um incidente. O plano de RI é composto de atividades que devem ser executadas quando um incidente foi identificado.
- É um conjunto de atividades realizadas para planejar, detectar e corrigir o impacto de um incidente em ativos de informação. E consiste em quatro fases: Planeamento, detecção, reação e recuperação.

Planeamento de Recuperação de Desastres

- Um evento pode ser classificado como um desastre quando a organização não consegue mitigar o impacto de um incidente durante o incidente e o nível de dano ou destruição é tão grave que a organização não consegue se recuperar rapidamente.
- A diferença entre um incidente e um desastre pode ser sutil, a equipe de planeamento de contingência deve fazer a distinção entre desastres e incidentes, e pode não ser possível fazer essa distinção até que ocorra um ataque. Geralmente, um evento inicialmente classificado como incidente é determinado como desastre, quando isso acontece, a organização deve mudar como está respondendo e tomar medidas para proteger seus ativos mais valiosos para preservar valor a longo prazo, mesmo com o risco de mais perturbações a curto prazo.

Planeamento de Recuperação de Desastres

- O planeamento de recuperação de desastres (DR) é o processo de preparar uma organização para lidar e se recuperar de um desastre, seja natural ou causado pelo homem. A principal ênfase de um plano de DR é restabelecer as operações no local primário, o local em que a organização realiza seus negócios. O objetivo é tornar as coisas completas ou como eram antes do desastre.

Planeamento de continuidade de negócios

- O planeamento de continuidade de negócios prepara uma organização para restabelecer as operações comerciais críticas durante um desastre que afeta as operações no site primário.
- Se um desastre tornou o local atual inutilizável, deve haver um plano para permitir que o negócio continue funcionando. Nem toda empresa precisa desse plano ou de tais instalações. Pequenas empresas ou organizações sólidas do ponto de vista fiscal podem ter a latitude para cessar as operações até que as instalações físicas possam ser restauradas.

Planeamento de continuidade de negócios

- Uma vez que os planos de resposta a incidentes e recuperação de desastres estão em vigor, a organização precisa considerar a possibilidade de encontrar instalações temporárias para apoiar a viabilidade continuada do negócio no caso de um desastre.
- O desenvolvimento do plano de BC é um pouco mais simples do que o plano de RI ou o plano de RD, uma vez que consiste basicamente em selecionar uma estratégia de continuidade e integrar as funções de armazenamento e recuperação de dados externos a essa estratégia.

Planeamento de continuidade de negócios

- Uma vez que os planos de resposta a incidentes e recuperação de desastres estão em vigor, a organização precisa considerar a possibilidade de encontrar instalações temporárias para apoiar a viabilidade continuada do negócio no caso de um desastre.
- O desenvolvimento do plano de CN é um pouco mais simples do que o plano de RI ou o plano de RD, uma vez que consiste basicamente em selecionar uma estratégia de continuidade e integrar as funções de armazenamento e recuperação de dados externos a essa estratégia. Alguns dos componentes do plano de CN já podem ser parte integrante das operações normais da organização, como um serviço de backup externo.

Planeamento de continuidade de negócios

Há várias estratégias que uma organização pode escolher ao planar a continuidade dos negócios. O fator determinante na seleção entre essas opções geralmente é o custo. Em geral, existem três opções exclusivas: sites quentes, mornos e frios, e três funções compartilhadas: time-share, agências de serviços e acordos mútuos.

- Um site quente é uma instalação de computador totalmente configurada, com todos os serviços, links de comunicação e operações físicas da fábrica, incluindo aquecimento e ar condicionado. O site quente duplicam recursos de computação, periféricos, sistemas telefônicos, aplicativos e estações de trabalho. Podendo estar operacional em questão de minutos e, em alguns casos, pode ser criado para fornecer um processo que seja perfeito para os usuários do sistema, capturando a carga de processamento de um site com falha, portanto, a alternativa mais cara disponível, no entanto, se a organização precisar de um recurso 24 horas por dia, 7 dias por semana, para recuperação quase em tempo real, um hotsite é o caminho a ser seguido.

Planeamento de continuidade de negócios

- Há várias estratégias que uma organização pode escolher ao planar a continuidade dos negócios. O fator determinante na seleção entre essas opções geralmente é o custo.
- Em geral, existem três opções exclusivas: sites quentes, mornos e frios,
- Três funções compartilhadas: time-share, agências de serviços e acordos mútuos.

Gestão de crise

- Os desastres são, obviamente, maiores em escala e menos manejáveis do que os incidentes, mas os processos de planeamento são os mesmos e, em muitos casos, são conduzidos simultaneamente. O que pode realmente distinguir um incidente de um desastre são as ações das equipes de resposta. Uma equipe de resposta a incidentes geralmente corre para as estações de serviço ou para o escritório de casa.
- O primeiro ato é alcançar o plano de RI. Uma equipe de recuperação de desastres não pode se dar ao luxo de folhear um fichário para ver o que deve ser feito. O pessoal de recuperação de desastres deve conhecer suas funções sem qualquer documentação de apoio. Esta é uma função da preparação, treinamento e ensaio.
- As ações tomadas durante e após um desastre são chamadas de gerenciamento de crise. A gestão de crises difere drasticamente da resposta a incidentes, uma vez que se concentra em primeiro lugar nas pessoas envolvidas. A equipe de recuperação de desastres trabalha de perto com a equipe de gerenciamento de crises.

Bibliografia

- WHITMAN, M. & MATTORD, H (2012). Principles of Information Security, 4a Ed. Boston:Course Technology.