UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Auditoria e Segurança

Prof. Fred Sauer
http://www.fredsauer.com.br
fsauer@gmail.com

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Quem sou eu...

- Prof. Frederico Sauer (Fred)
  - Mestre e Doutor UFRJ com dissertação e tese em Segurança e Gerenciamento de Redes
  - Professor Adjunto UEZO desde 20/09/2013
  - Professor Convidado FGV Management
  - Gerente de TI de 90 a 2010
  - Auditor de SegInfo na Marinha de 99 a 2010

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

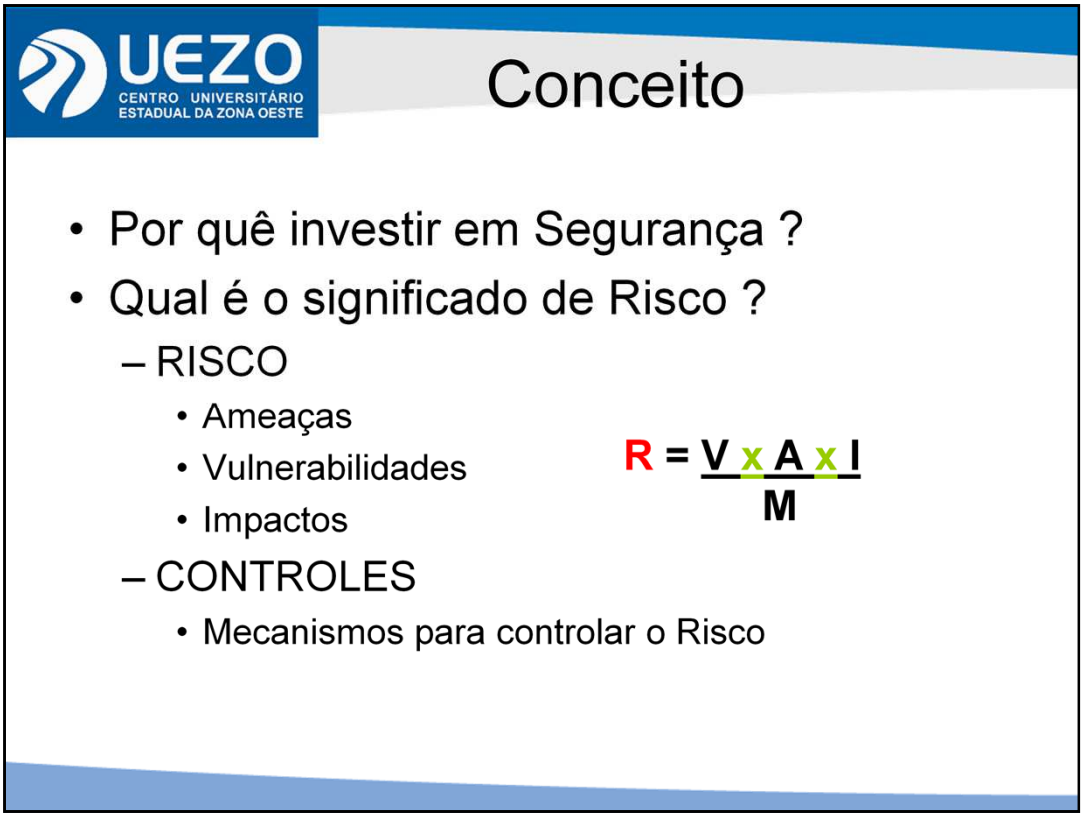
Aula 1

- **1) SEGURANÇA DAS INFORMAÇÕES**
  - 1.1 Plano de contingência e continuidade dos serviços de informática
  - 1.2 Política de Segurança das Informações
    - 1.2.1 Objetivos, legislação e definições de políticas
    - 1.2.2 Análise de riscos
    - 1.2.3 Serviços e mecanismos de segurança
    - 1.2.4 Ataques
    - 1.2.5 Gerência da segurança
    - 1.2.6 Violações da política de segurança
    - 1.2.7 Controles (acesso lógico e físico, controles ambientais)

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Plano de Contingências e Continuidade

- Perda do poder computacional → perda de negócios
- Vulnerabilidades existentes podem permitir incidentes inesperados
- Casos importantes:
  - Bug do milênio
  - Queda do WTC



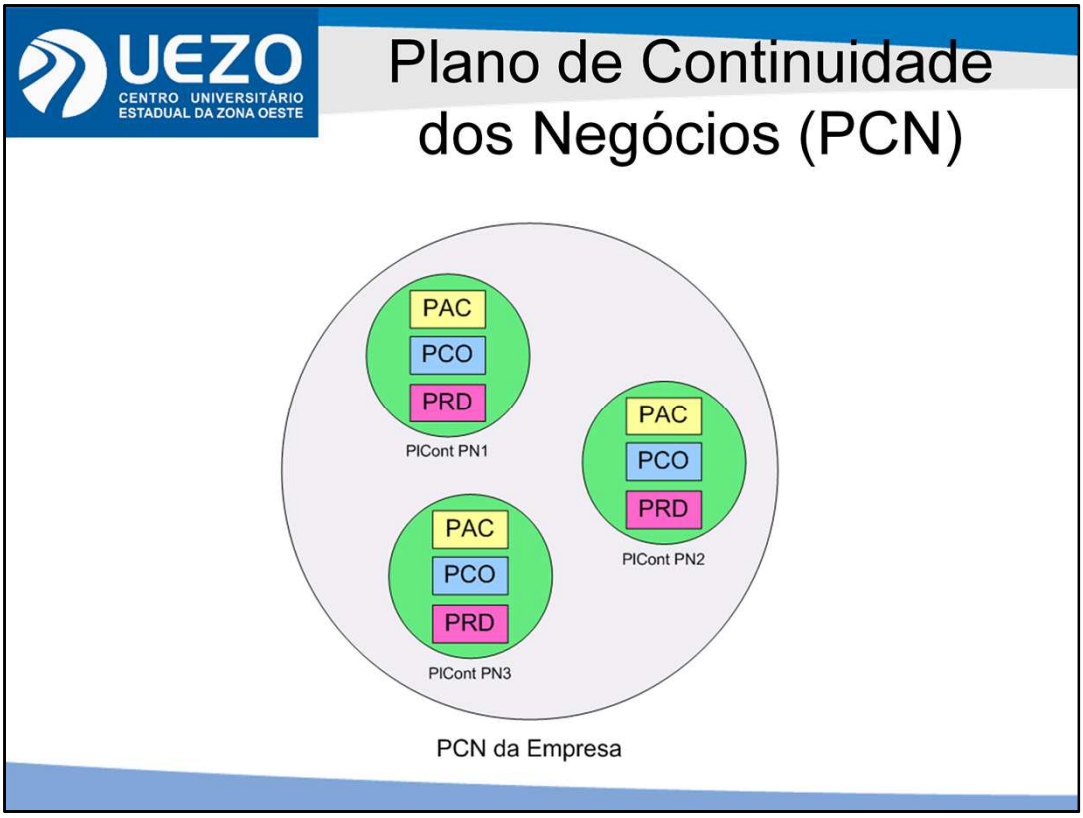
Investir em Segurança é um desafio, porque o empresariado tem dificuldade de visualizar o retorno do investimento. É importante informar os impactos em incidentes já ocorridos na própria empresa ou em empresas semelhantes, além de evidenciar casos de sucesso de empresas que investiram em ética e se v valorizaram no mercado, como a SIEMENS.

Ameaças são elementos ativos, que exploram vulnerabilidades causando impactos. Sem vulnerabilidades, as ameaças não atingiriam seu objetivos. As vulnerabilidades são elementos passivos, pertencentes ao sistema e que, sem a presença de ameaças, não representam risco. No entanto, as empresas convivem com as vulnerabilidades, ignorando-as ou as aceitando, tornando-se alvos fáceis para as ameaças. A combinação entre ameaças e vulnerabilidades pode ser substituída nesta fórmula pela probabilidade da ocorrência do incidente que está se analisando.

Incidente de Segurança é uma ocorrência caracterizada pelo potencial de comprometer o negócio da organização em análise.

Os impactos representam as consequências de um incidente de segurança (tangíveis e intangíveis) para o negócio.

Sempre que os Riscos forem inaceitáveis, são necessárias medidas voltadas para o controle deste risco (letra M na equação). Estas medidas envolvem ações preventivas e preditivas, descritas nas Políticas de Segurança, e medidas reativas descritas nos Planos de Contingência.



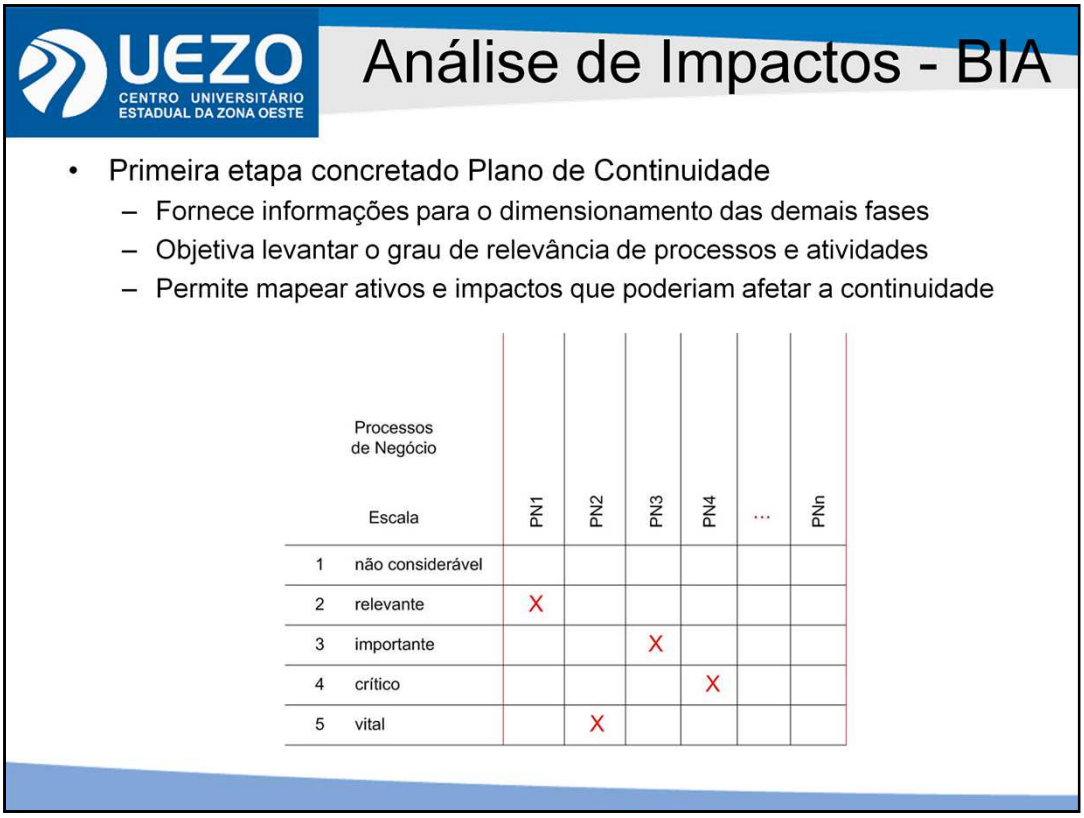
O desenho ilustra que um Plano de Continuidade de uma empresa é composto de vários Planos de Continuidade, um (ou mais) para cada processo de negócio. Estes, por sua vez, devem conter ações de Administração de Crise, de Continuidade Operacional e de Recuperação de Desastres, que podem ser realizadas em paralelo ou sequencialmente, de acordo com a disponibilidade de recursos materiais e humanos.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

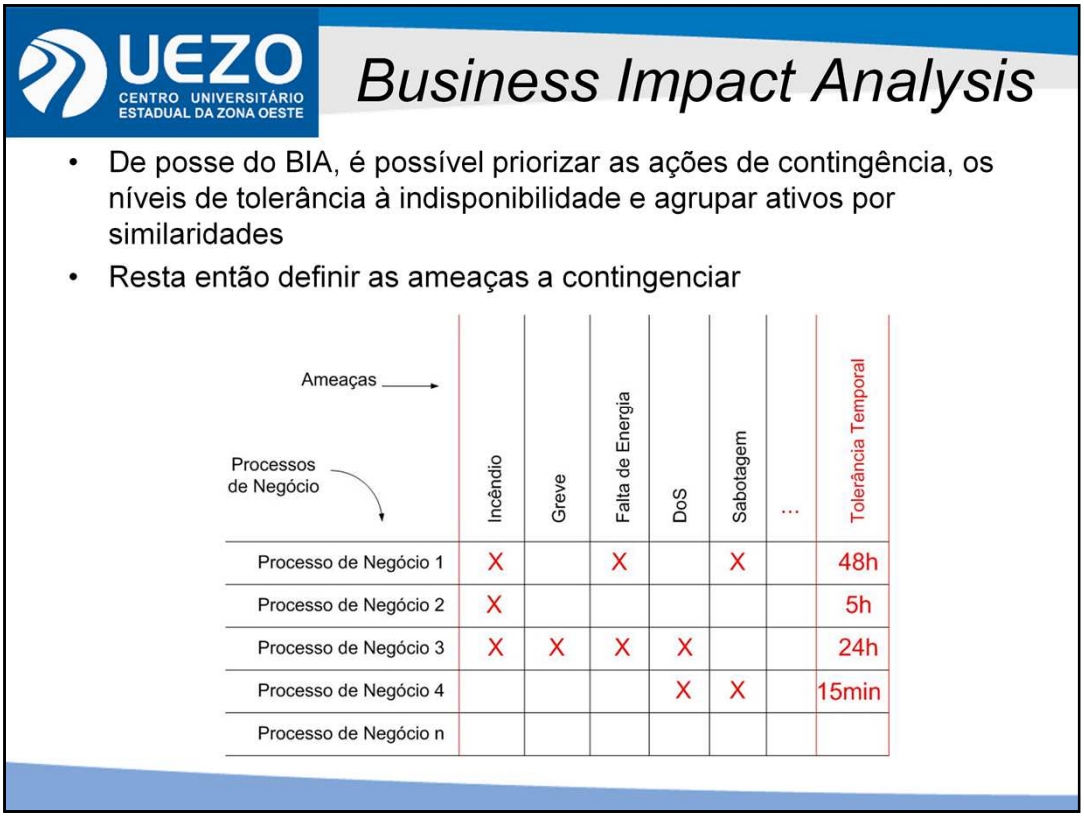
Planejamento

1. Conscientização e comprometimento da Direção
2. Análise, avaliação e proposta de tratamento do Risco
3. Desenvolvimento do Plano de Contingências
4. Treinamento e Teste do Plano
5. Avaliação e melhorias no Plano

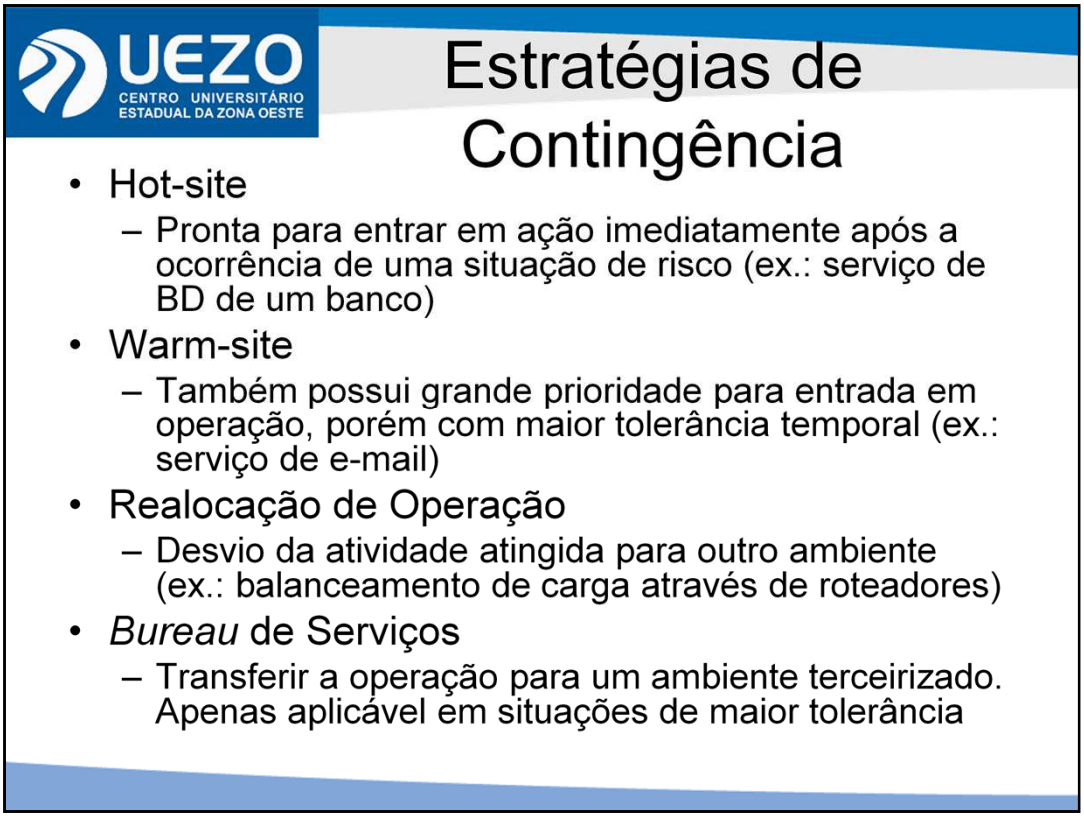
Essa figura ilustra a utilidade do Plano de Continuidade dos Negócios. Ele deve ser planejado para incidentes que não puderam ser evitados. Imagine a seguinte situação: um sabotador consegue entrar na empresa sem ser percebido. Enquanto ele não comete nenhum ataque, houve quebra de política de segurança, porque as ações de controle não foram eficazes. No entanto, sua presença no interior da empresa não causou impacto ao negócio até então. Estamos do lado esquerdo da seta do nível de risco da figura, cujo limite é a seta na vertical identificada como “nível aceitável”. O sabotador então se dirige para o setor de TI e pega um balde com água. O nível de risco está aumentando, ou seja, está próximo do nível aceitável. Ele entra na sala onde está o storage. Com isso, o nível de risco passa do aceitável, e para uma situação como essa apenas o uso de políticas não é suficiente, sendo conveniente a elaboração de um planejamento de contingência.



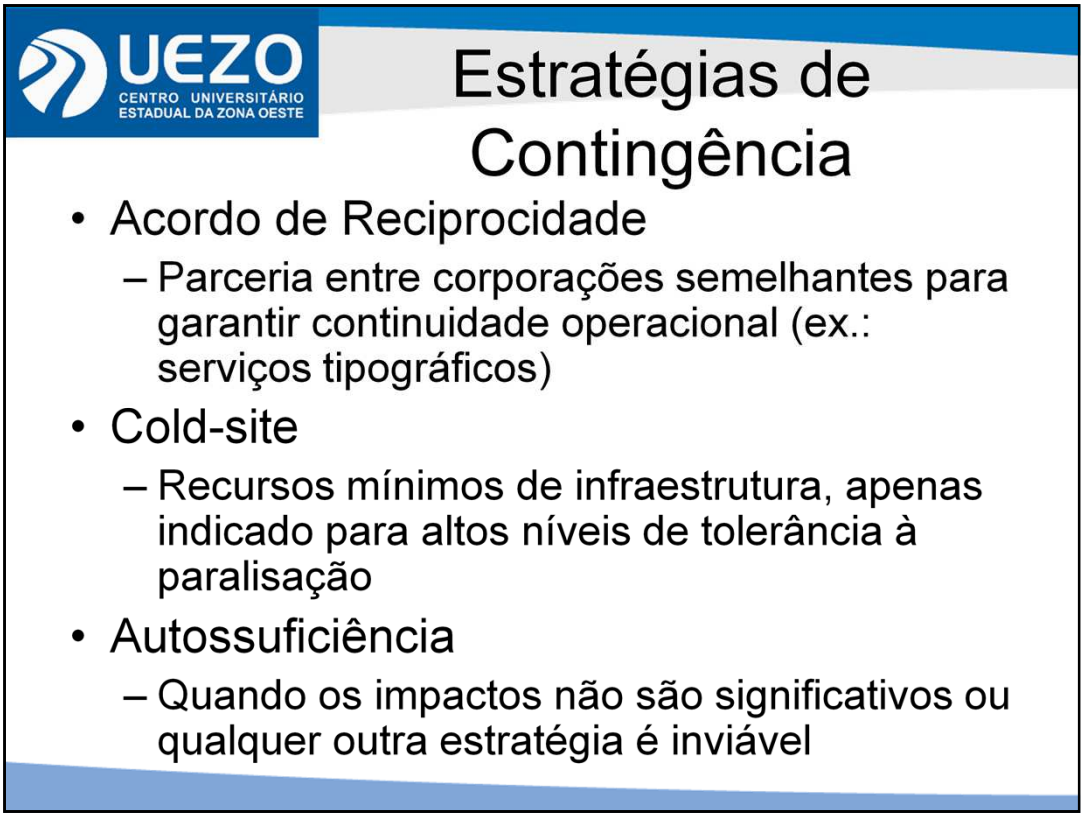
O BIA – *Business Impact Analysis* é um instrumento mundialmente conhecido que se destina a avaliar os impactos quantitativos que podem ser gerados com a paralisação total ou parcial de um determinado Processo de Negócio. Fornece informações para o perfeito e adequado dimensionamento do Plano de Continuidade. Com essa análise, pode-se definir prioridades de contingência, níveis de tolerância à indisponibilidade, agrupar os ativos de acordo com as suas similaridades. A figura a seguir ilustra a aplicação do BIA relacionada com as ameaças para o negócio, resultando num valor de tolerância para cada um dos PN ser contingenciado.



Essa tolerância se relaciona ao grau de criticidade de cada um dos PN.



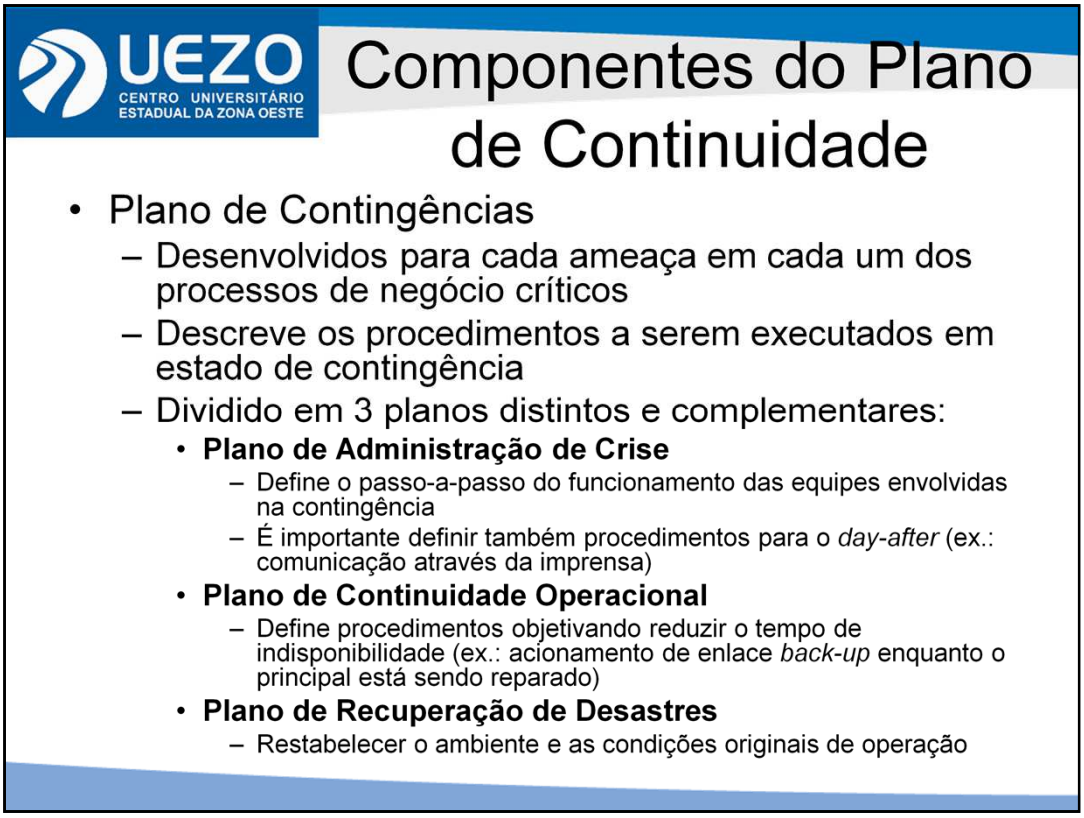
Para cada nível de tolerância há estratégias passíveis de adoção. A ***Hot-site***, por exemplo, é a mais imediata e está sempre prestes a entrar em ação, oferecendo um tempo mínimo ou até inexistente de paralisação.
A ***Warm-site***, aplicável a situações menos exigências que a anterior porém ainda com baixa tolerância à paralisação, oferece soluções prontas para contingenciar incidentes, porém que implicam em alguma latência de implementação. Esse exemplo do e-mail ilustra uma situação warm-site, em que se pode usar enlaces alternativos para o despacho de mensagens, porém a necessidade de reconfiguração demandaria algum tempo a mais para retorno a operação. A **Realocação de Operação** prevê o desvio da atividade atingida por um incidente para outra instalação, ambiente físico, enlace, equipamento, pertencentes à mesma empresa e disponíveis. Essa estratégia implica em algumas questões: a primeira é a necessidade de redundância que demanda recursos, nem sempre disponíveis. Um bom exemplo é a disponibilidade de um segundo roteador em rede para implementação de redirecionamento de carga em caso de indisponibilidade.
O Bureau de serviços é semelhante ao anterior, porém com o uso de infra-estrutura terceirizada. Se por um lado dispensa a necessidade de se manter recursos redundantes, por outro traz inconvenientes como o manuseio das informações da empresa por terceiros e requerer maior tempo de tolerância.



O **Acordo de Reciprocidade** é interessante quando a implementação das estratégias de contingência se apresentassem inviáveis pelos altos custos. A aproximação entre empresas com características semelhantes (físicas, tecnológicas e humanas) visa uma alocação da atividade atingida nessa outra empresa, através do compartilhamento de recursos. Apesar do benefício do baixo custo, continua-se com o problema da manipulação dos dados por terceiros, agravado pelo fato que empresas com características semelhantes tipicamente são concorrentes. Um exemplo é a impressão da tiragem de jornais.

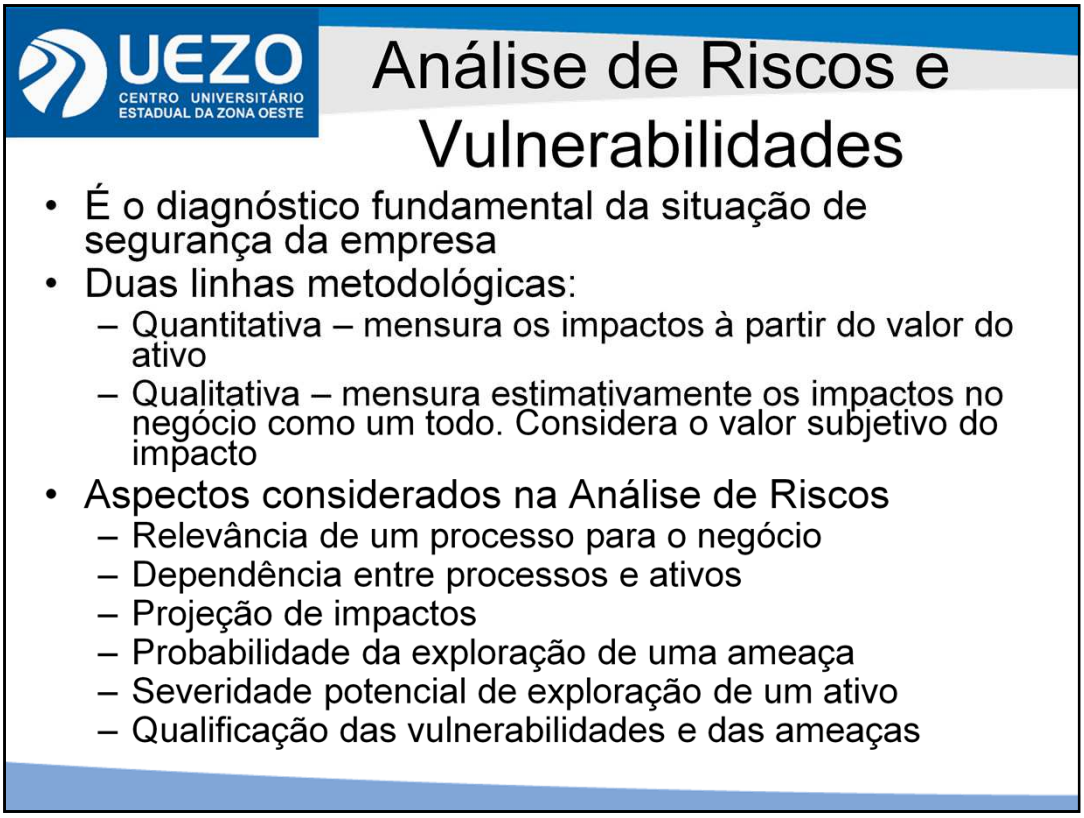
A estratégia ***Cold-site*** propõe uma alternativa viável apenas para instalações sem recursos de processamento de dados e recursos mínimos de infra-estrutura e telecom, ficando à mercê de soluções que serão implementadas para cada caso, de acordo com a disponibilidade de recursos e pessoal.

A **auto-suficiência** é o extremo oposto da hot-site, e é aplicável quando nenhuma das estratégias anteriores é adequada, ou porque os impactos não são significativos ou então estas estratégias não são economicamente viáveis.



Os Planos de Contingência são desenvolvidos de acordo com cada uma das ameaças para cada um dos PN relevantes e críticos, definindo detalhes operacionais para cada um dos incidentes de segurança possíveis. É dividido em 3 módulos distintos e complementares que tratam especificamente de cada momento vivido pela empresa.
O **Plano de Administração de Crises (PAC)** – Define o passo-a-passo do funcionamento das equipes envolvidas com o acionamento das contingências, antes, durante e depois do incidente. Também define procedimentos que devem ser realizados quando a empresa voltar à normalidade. Um exemplo é a estratégia de comunicação do fato ocorrido à imprensa. Também deve definir os insumos necessários para a sua implementação, como sobressalentes e ferramentas necessárias.
O **Plano de Continuidade Operacional (PCO)** – Define os procedimentos para o contingenciamento dos ativos que suportam cada um dos PN, para redução do tempo de indisponibilidade e consequentemente, a extensão dos impactos provocados pelo incidente. Um exemplo é a definição de ações a tomar no caso da queda da conexão principal com a Internet, e que pode ser substituída por outra de menor capacidade de forma indesejada porém satisfatória para o negócio. É objetivamente focado no negócio.
O **Plano de Recuperação de Desastres (PRD)** - Objetiva definir procedimentos de recuperação e restauração das funcionalidades dos ativos aos níveis originais de operação. É objetivamente focado nos ativos. Também deve possuir ações objetivas de análise das razões que causaram o incidente e proposição de alterações nos processos que possam reduzir as chances de uma nova ocorrência.
É fator crítico de sucesso definir precisamente os gatilhos para acionamento destes planos. Estes gatilhos são tipicamente parâmetros de tolerância, que se ultrapassados estão inferindo em perdas (impactos) para o negócio, e definidos através do BIA. Podem também ser usados outros parâmetros, como o percentual do recurso afetado, perdas financeiras, etc.
Este modelo deve ser dinâmico, testado e ajustado periodicamente para garantir a sua

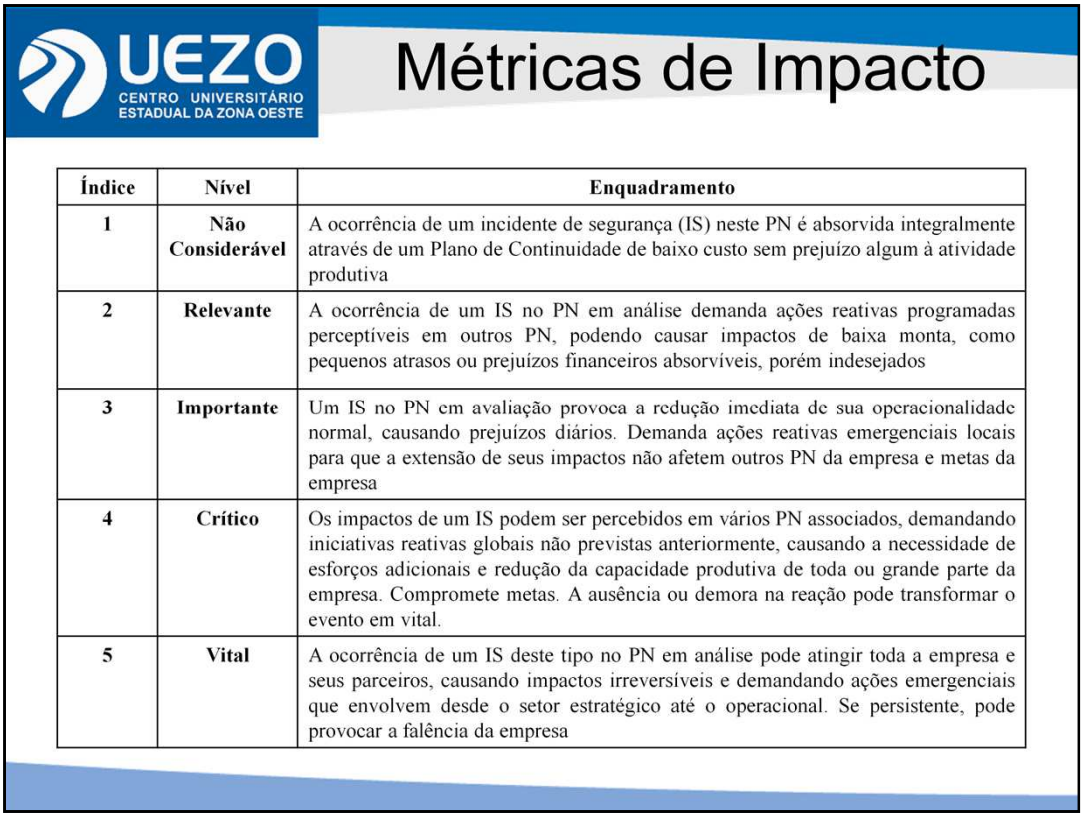
eficácia.



Por ser um procedimento crítico de sucesso para a SegInfo, a Análise de Riscos deve ser bem compreendida e corretamente executada. A maioria das iniciativas tende a concentrar o mapeamento de vulnerabilidades principalmente nos ativos tecnológicos, o que não é suficiente para diagnosticar com precisão os reais riscos que envolvem a operação da empresa. Processos, ambientes físicos, pessoas, sistemas, informações e equipamentos são pilares que sustentam os processos de negócio e conseqüentemente o próprio negócio. Há também variáveis exógenas que influenciam o nível de risco, como por exemplo as ameaças que surgem em função de mudanças estratégicas.

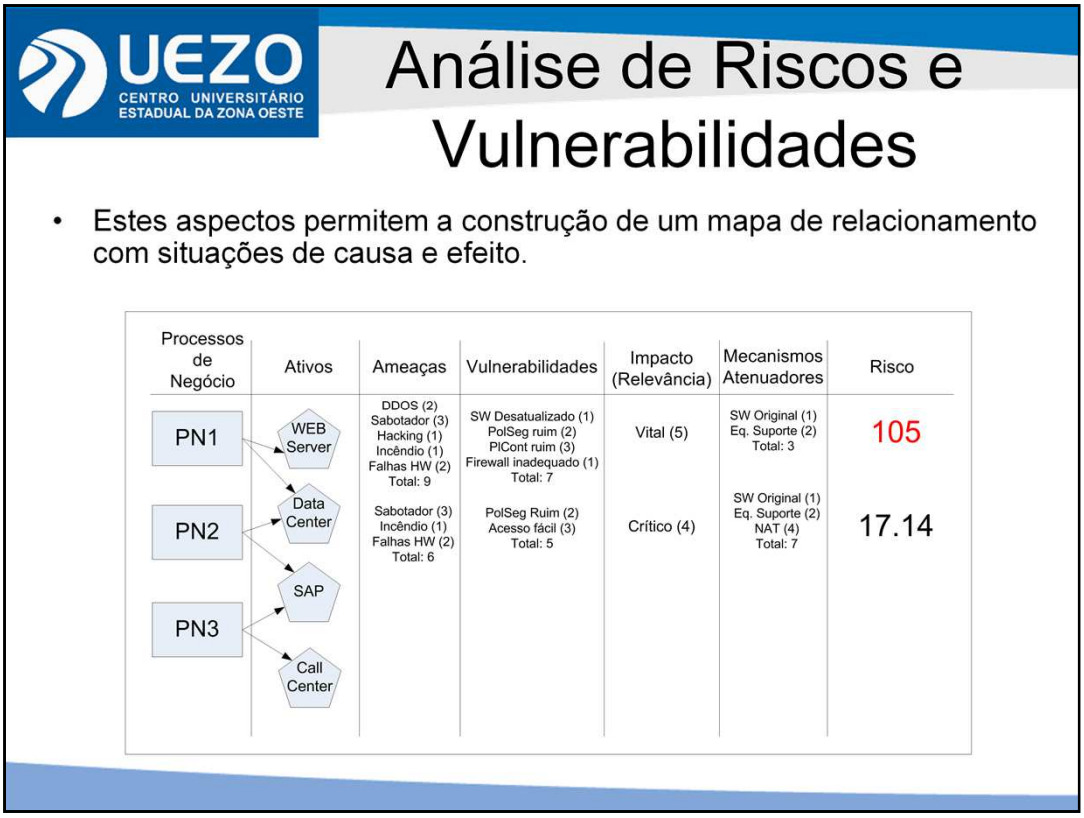
A Análise de Risco, portanto deve ser ampla e focada no negócio como um todo. Pode seguir a linha quantitativa, orientada a mensurar os impactos financeiros provocados por um incidente de segurança, calculado à partir do valor dos próprios ativos. A linha qualitativa usa critérios para estimar os impactos de um incidente de segurança causado por uma ameaça, mas tem uma componente mais subjetiva do que a quantitativa, permitindo a contabilização do aparentemente intangível.

Aplicando-se a metodologia para mapeamento de processos de negócio adotada no PDS, ou até mesmo “herdando” os resultados dessa atividade, tem-se o mapa de relacionamento e dependência dos ativos. Coleta-se evidências e identificação de ameaças e vulnerabilidades dos ativos, para o cálculo de risco.

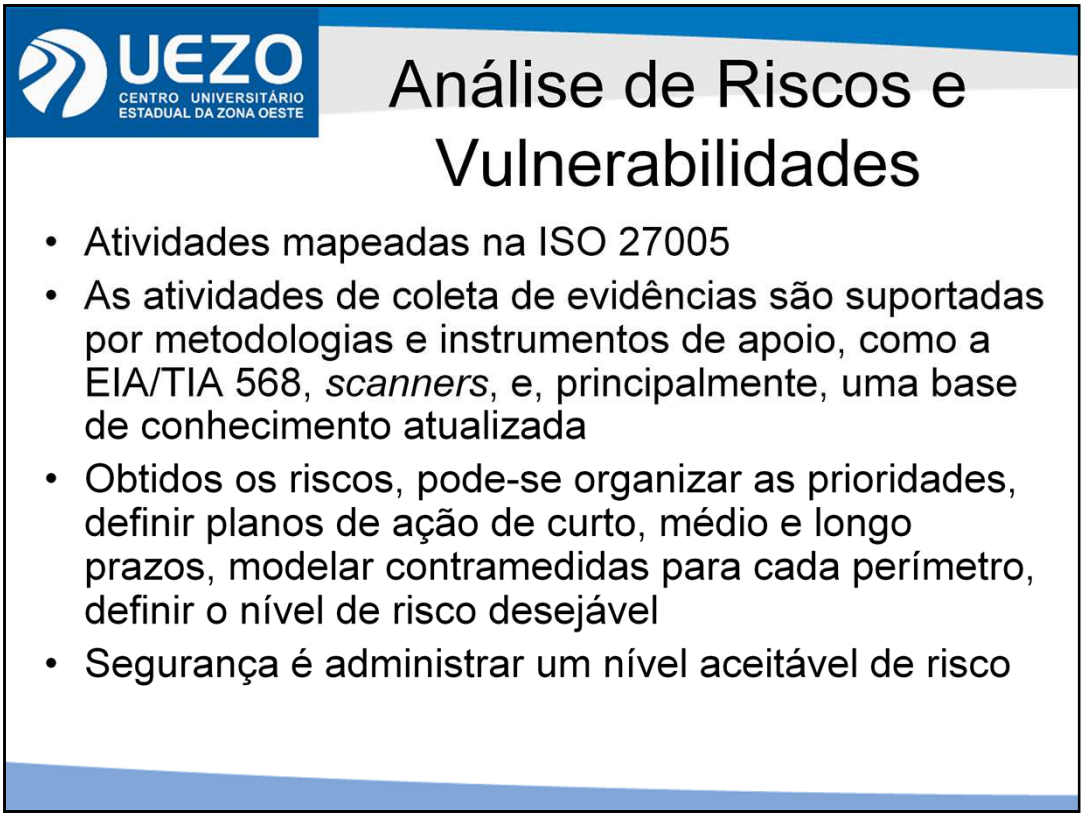


Índice	Nível	Enquadramento
1	**Não Considerável**	A ocorrência de um incidente de segurança (IS) neste PN é absorvida integralmente através de um Plano de Continuidade de baixo custo sem prejuízo algum à atividade produtiva
2	**Relevante**	A ocorrência de um IS no PN em análise demanda ações reativas programadas perceptíveis em outros PN, podendo causar impactos de baixa monta, como pequenos atrasos ou prejuízos financeiros absorvíveis, porém indesejados
3	**Importante**	Um IS no PN em avaliação provoca a redução imediata de sua operacionalidade normal, causando prejuízos diários. Demanda ações reativas emergenciais locais para que a extensão de seus impactos não afetem outros PN da empresa e metas da empresa
4	**Crítico**	Os impactos de um IS podem ser percebidos em vários PN associados, demandando iniciativas reativas globais não previstas anteriormente, causando a necessidade de esforços adicionais e redução da capacidade produtiva de toda ou grande parte da empresa. Compromete metas. A ausência ou demora na reação pode transformar o evento em vital.
5	**Vital**	A ocorrência de um IS deste tipo no PN em análise pode atingir toda a empresa e seus parceiros, causando impactos irreversíveis e demandando ações emergenciais que envolvem desde o setor estratégico até o operacional. Se persistente, pode provocar a falência da empresa

Esta tabela é um exemplo de métrica para atribuição qualitativa da intensidade do impacto para uma corporação. Trabalhos quantitativos dependem do acúmulo de amostras dentro da organização que possibilitem a definição de probabilidades de ocorrência de determinados incidentes, o que não é trivial e demanda tempo e maturidade (cultura de segurança) da organização.



Com a lista apresentada no *slide*, monta-se o mapa de relacionamento com a projeção de situações de causa e efeito, com ligações múltiplas, pontuações e qualificação de ameaças e vulnerabilidades, associadas a estudos de probabilidades e impactos que tornar-se-ão elementos subsidiadores do cálculo do risco.
A identificação de ameaças e vulnerabilidades é feita através de instrumentos como entrevistas, inspeção física e de documentos, análise técnica de ativos tecnológicos através de normas de certificação (EIA/TIA 568A), software especializado para varredura e *scanning*.



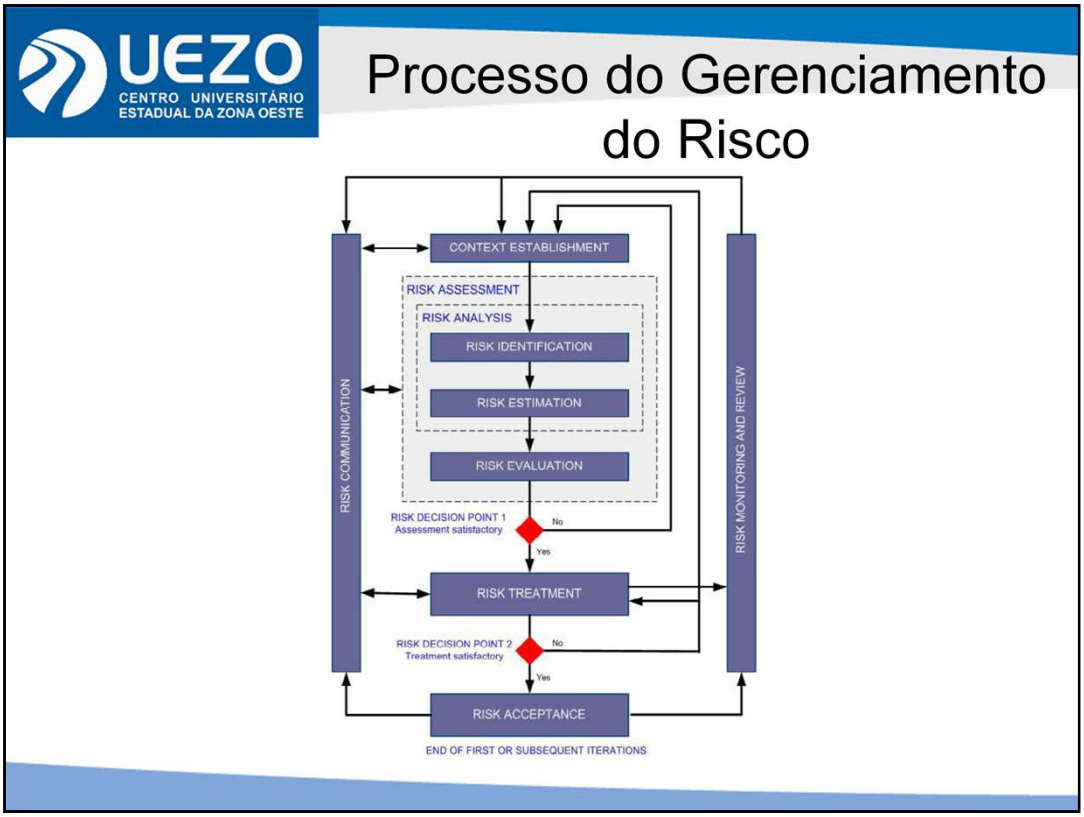
O nível de risco de um determinado PN é projetado à partir do nível de risco de cada ativo que o sustenta. O resultado permite a definição de prioridades, dimensionar plano de ação de curto médio e longo prazos, de acordo com o nível de risco de cada um. Pelo menos no início, convém alinhar os resultados da análise de riscos aos controles sugeridos pela norma ISO 27002 e identificar o nível de conformidade atingido pela empresa através da medição da aderência a cada um dos 127 controles de segurança.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

ISO 27005:2008

- O processo de Gerenciamento de Risco deve ser embasado no Plano Diretor de Segurança (ISO 27001 - PDCA).

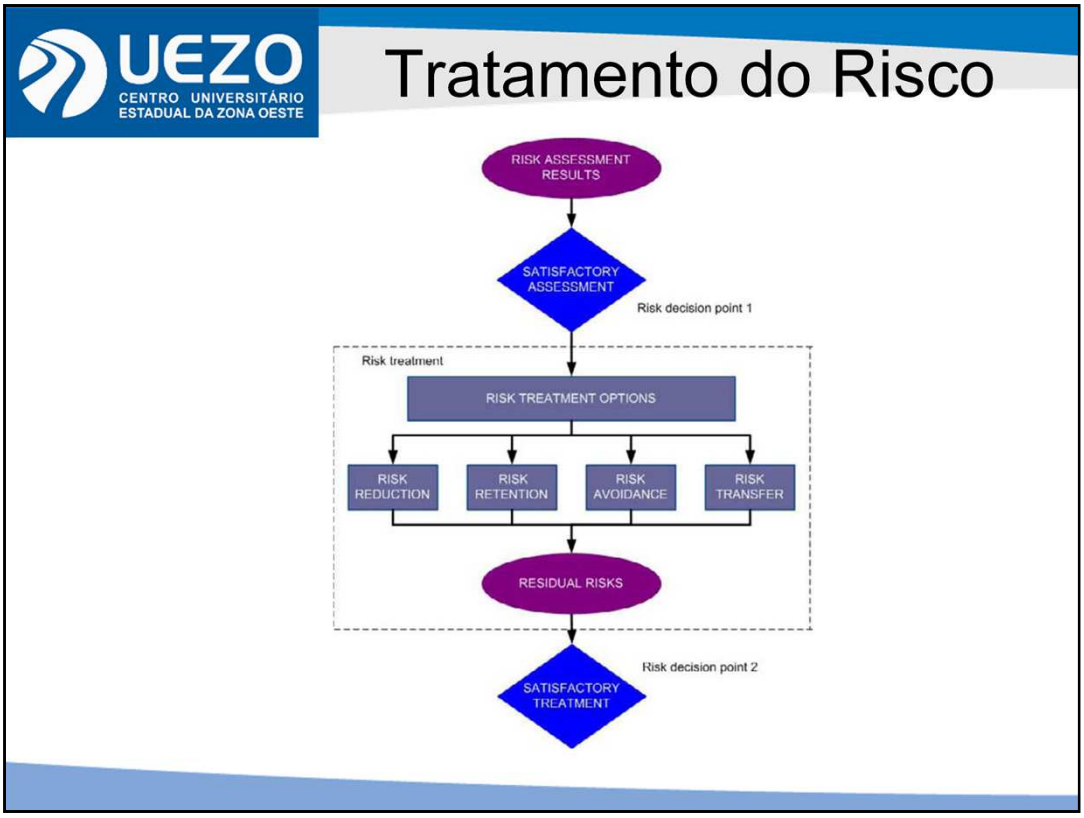
ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Risk treatment planning Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process



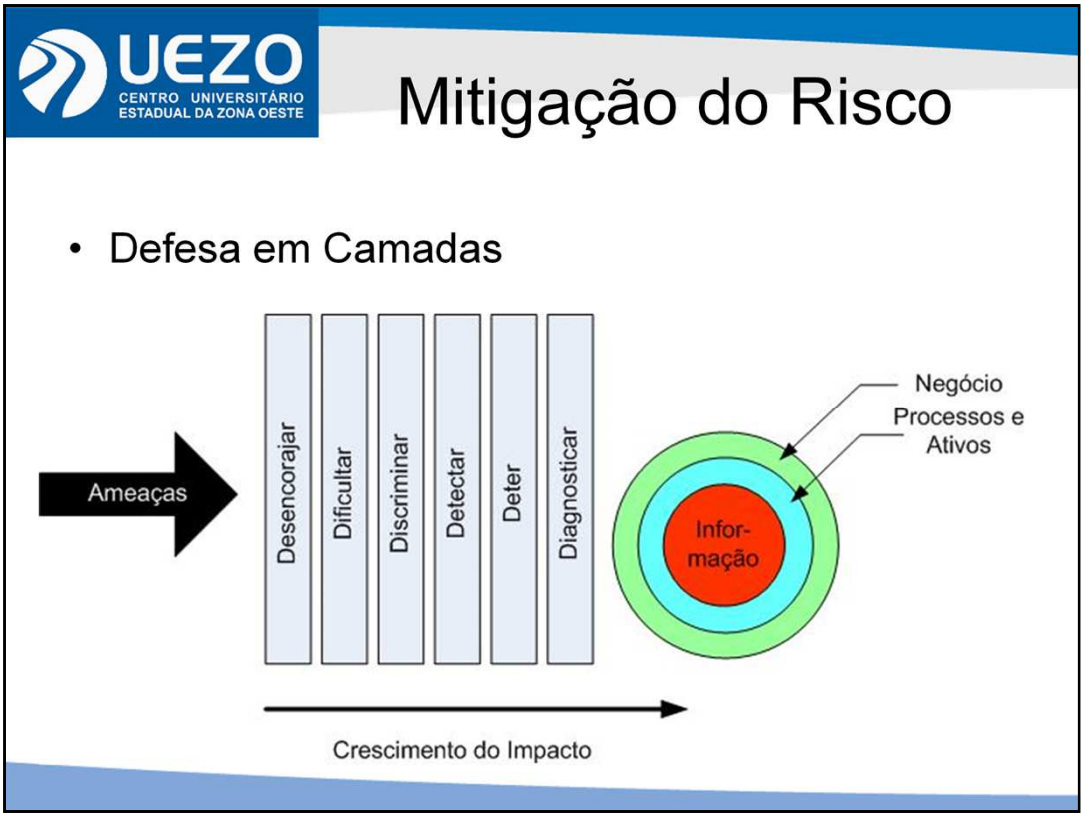
A IDENTIFICAÇÃO do risco é feita a partir da evidenciação da existência de vulnerabilidades específicas e de ameaças que as possam explorá-las. Uma vez identificados, os riscos precisam ser ESTIMADOS, que é a mensuração dos impactos causados ao negócio. Estes riscos então precisam ser AVALIADOS, que é a comparação objetiva dos resultados de mensuração com os critérios de aceitação de risco, que devem ser estabelecidos pela alta administração da empresa. Estes riscos então, de acordo com a avaliação anterior, serão TRATADOS, onde uma das estratégias deverá ser adotada: MITIGAÇÃO, que é a adoção de medidas para reduzir o risco, ELIMINAÇÃO, que é a desistência da atividade de negócio, em função do alto risco que ela envolve, MANUTENÇÃO, que é a implementação de medidas de monitoramento para garantir que o risco não se eleve de um patamar aceitável para outro superior, e a TRANSFERÊNCIA, que é o repasse de parte ou até mesmo o todo da atividade sob risco para um terceiro que possua maior competência para administrar este risco ou que assuma financeiramente os riscos envolvidos. Após o tratamento, nova avaliação deve ser feita para identificar os resíduos após a adoção das medidas. Estes resíduos devem ser apresentados à alta direção, que deve aceitá-los para que esta etapa se encerre. É importante ressaltar que todas estas etapas envolvem a comunicação com os stakeholders (partes interessadas) da organização.

A norma ISO 27005 detalha aspectos e requisitos para cada uma das fases deste processo, de forma que o mesmo possa ser metodologicamente aplicado a qualquer corporação. É relevante ressaltar a importância da definição de um objetivo critério para mensuração de impactos, nem sempre trivial de se fazer e que de forma alguma pode ser obtido através de experiências de outra empresa. Este critério será usado na avaliação do risco atual e aceitável, definindo controles a serem implementados, com

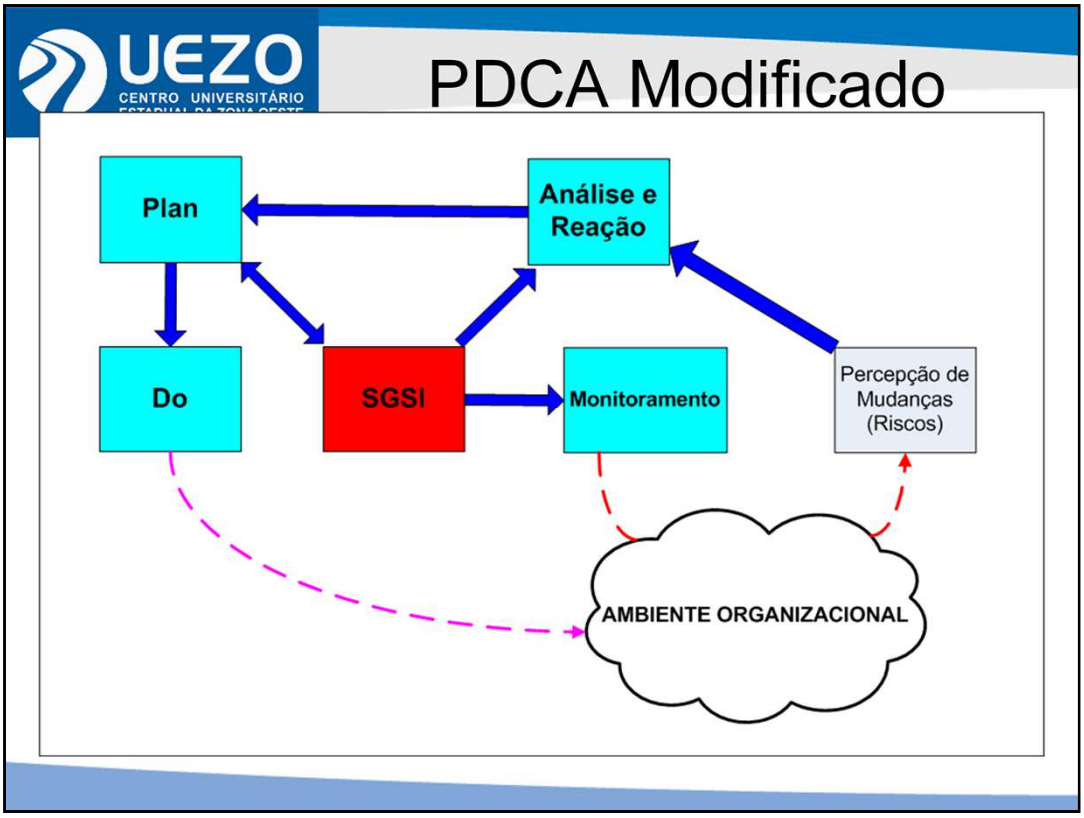
investimentos financeiros e pessoais. A Estratégia a ser adotada para tratamento deste risco e apresentada no próximo slide.



Após uma avaliação do risco, que pode ser qualitativa ou quantitativa, decisões precisarão ser tomadas. Estas decisões, para cada risco, poderão ser:
Redução do Risco (mitigação) – O nível aferido é superior ao desejado, demandando ações objetivas para reduzi-lo. Naturalmente, após a implementação destas ações, o monitoramento contínuo é necessário para avaliar se o risco residual está de acordo com as expectativas;
Retenção do Risco – O nível aferido é aceitável, mas precisa ser mantido, para não aumentar. Tipicamente, ações de monitoramento são suficientes para esta estratégia;
Afastamento do Risco – Estratégia complexa, uma vez que, para evitar o risco, um de seus componentes deve ser eliminado (ameaças, vulnerabilidades ou impactos); e
Transferência do Risco – Muito usado atualmente na área de TI, com a delegação de serviços de alto risco para outras empresas que já possuem expertise e infraestrutura preparada para combater o risco.



A defesa em camadas prevê a a implementação de fases com níveis de resistência crescentes. O **Desencorajar** visa exclusivamente fazer com que as ameaças percam seu estímulo inicial para exploração de vulnerabilidades. Isso pode ser feito através de mecanismos físicos, tecnológicos ou humanos, implementando-se câmeras de vídeo (mesmo falsas ! Hoje em dia são muito comuns placas "sorria, você está sendo filmado" sem que exista uma câmera sequer), campanhas de divulgação da Política de Segurança, informação sobre os procedimentos de auditoria e Forense Computacional, etc. **Dificultar** é a segunda barreira. É complementar à anterior e visa a adoção efetiva de controles para dificultar o acesso indevido. Exemplos são roletas, detectores de presença com alarmes, senhas, certificados digitais, etc. **Discriminar** é a ação de identificar e gerir os acessos identificados na fase anterior, permitindo acessos apenas para quem precisa e no nível necessário. A **Detecção** visa identificar uma situação de risco, ou seja, a tentativa de alguém de burlar as ações da fase anterior. Exemplos dessas ações são os antivírus, sistemas IDS entre outros. **Deter** objetiva impedir que a ameaça atinja os ativos, caso as barreiras anteriores não tenham sido eficazes. Ações administrativas, punitivas, bloqueio de acessos físicos e lógicos são exemplos. **Diagnosticar** não é simplesmente o último passo dessa segmentação, por representar o elo de ligação com a primeira barreira, sendo portanto a mais importante para o aprimoramento das estratégias de defesa dos ativos. Um bom diagnóstico é representado por uma detalhada análise de riscos, que deverá corrigir rumos e atualizar estratégias de acordo com todo o dinamismo que cerca o ambiente de negócios.



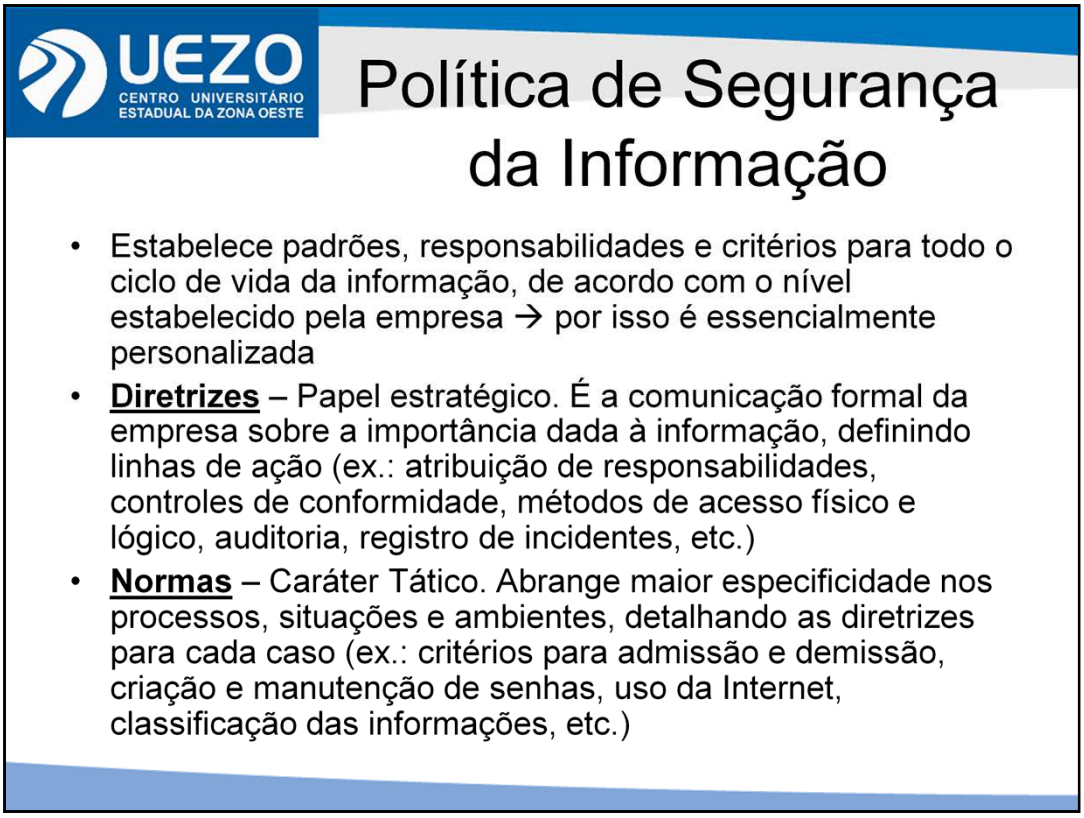
Essa figura ilustra a interação entre as fases, destacando a importância da fase de monitoramento, que interage com todas as outras permitindo a Gestão Dinâmica através da correção de rumos de acordo com a percepção do ambiente existente.
Na cronologia dos eventos, antes de tudo é importante **analisar**, e em função dessa análise gerar (**planejar**) a primeira versão do Plano Diretor de Segurança. **Implementam-se** os comitês de segurança, atribui-se responsabilidades, inicia-se um programa de divulgação, treinamento e conscientização. Inicia-se a tarefa de **monitoramento** desde então, realimentando a **análise** de riscos. Com essa realimentação, novamente se **planejam** ações, **implementam-se** controles e **monitoram-se** resultados, para que se possa realizar novas análises e assim por diante.

A Política de Segurança da Informação não um manual de procedimentos. É um conjunto de diretrizes, normas, procedimentos e instruções de grande abrangência, que se destinam a implementar e garantir o controle do nível de risco para a corporação. Seus objetivos são destinados a todos os setores da empresa, porém os documentos são direcionados para cada um dos setores, estratégico (executivo), tático e operacional, estabelecendo padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações de acordo com o nível de segurança estabelecido sob medida para a empresa. A Política de Segurança, então, é altamente particularizada para cada empresa.

As Diretrizes tem papel estratégico, expressando a importância que a empresa dá para a informação, além de comunicar aos seus funcionários seus valores e o seu comprometimento com os desafios de se incrementar a segurança na cultura organizacional. Por ser um conjunto de documentos da alta direção da empresa, serve como norteador das atividades táticas e operacionais. Definem responsabilidades dos elementos manipuladores da informação, estrutura do *Security Office*, métricas, índices e indicadores, controles de conformidade, requisitos de capacitação de usuários, mecanismos de controle de acesso físico e lógico, responsabilizações, auditoria do uso de recursos, registro de incidentes e gestão de continuidade do negócio.

As normas são usadas no nível tático para detalhas situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações. São naturalmente mais numerosas do que as diretrizes. Critérios para admissão e demissão, criação e manutenção de contas e senhas de usuários, descarte de informações, desenvolvimento e manutenção de sistemas, uso da internet, acessos remotos, notebooks, pendrives e câmeras digitais. Contratação de terceiros e classificação da sensibilidade da informação são bons exemplos de normas.

Procedimentos e Instruções aplicáveis ao nível operacional são bem mais numerosas e devem descrever meticulosamente cada uma das ações e atividades relacionadas com o uso das informações. Um bom exemplo é: enquanto a diretriz orienta estrategicamente para a necessidade de salvaguardar informações sigilosas, a norma define que as mesmas devem ser criptografadas com ferramentas de acordo com o grau de sigilo, e os procedimentos e instruções descrevem os passos necessários para executar tal criptografia caso-a-caso.



Para elaborar uma PolSeg, deve-se iniciar pela elaboração das diretrizes, envolver os executivos e conquistar apoio. Estabelecer responsáveis e gestores diretos pela manutenção da PolSeg. Elaborar um programa de divulgação das diretrizes, normas, procedimentos e instruções, como instrumento de disseminação da cultura e conscientização do pessoal. Buscar sempre o envolvimento de todos os funcionários, de forma a agregar responsabilidade pela continuidade do negócio, principalmente pela responsabilidade específica sobre as informações sob sua custódia.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Política de Segurança da Informação

- Procedimentos e Instruções
  - Descrição meticulosa de cada ação
  - Exemplo:
    - A **Diretriz** determina como estratégico a salvaguarda de assuntos sigilosos
    - A **Norma** define que assuntos sigilosos definidos por um determinado critério devem ser criptografado
    - O **Procedimento** descreve passo-a-passo como criptografar o arquivo
- Conclusões:
  - O processo deve ser *top-down* (iniciar pelas diretrizes)
  - Os executivos devem estar envolvidos e motivados
  - A ampla divulgação é fundamental
  - O funcionário também deve ser envolvido e motivado

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Elementos Construtivos

- ISO 27001 – Norma para construção de um SGSI
- ISO 27002 – Norma que descreve as Melhores Práticas para a segurança da Informação
- ISO 27005 – Norma para Gestão do Risco em Segurança da Informação

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

ISO 27002 - Seções

3.1 Seções

Cada seção contém um número de categorias principais de segurança da informação. As 11 seções (acompanhadas com o respectivo número de categorias) são:

a) Política de Segurança da Informação (1);

b) Organizando a Segurança da Informação (2);

c) Gestão de Ativos (2);

d) Segurança em Recursos Humanos (3);

e) Segurança Física e do Ambiente (2);

f) Gestão das Operações e Comunicações (10);

g) Controle de Acesso (7);

h) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6);

i) Gestão de Incidentes de Segurança da Informação (2);

j) Gestão da Continuidade do Negócio (1);

k) Conformidade (3).

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Fatores Críticos

0.7 Fatores críticos de sucesso

A experiência tem mostrado que os seguintes fatores são geralmente críticos para o sucesso da implementação da segurança da informação dentro de uma organização:

a) política de segurança da informação, objetivos e atividades, que reflitam os objetivos do negócio;

b) uma abordagem e uma estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível de todos os níveis gerenciais;

d) um bom entendimento dos requisitos de segurança da informação, da análise/avaliação de riscos e da gestão de risco;

e) divulgação eficiente da segurança da informação para todos os gerentes, funcionários e outras partes envolvidas para se alcançar a conscientização;

f) distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas;

g) provisão de recursos financeiros para as atividades da gestão de segurança da informação;

h) provisão de conscientização, treinamento e educação adequados;

i) estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

j) implementação de um sistema de medição[1], que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria.

Política de Segurança

5.1 Política de segurança da informação

Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

Diretrizes para implementação

Convém que o documento da política de segurança da informação declare o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a segurança da informação. Convém que o documento da política contenha declarações relativas a:

a) uma definição de segurança da informação, suas metas globais, escopo e importância da segurança da informação como um mecanismo que habilita o compartilhamento da informação (ver introdução);

b) uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação, alinhada com os objetivos e estratégias do negócio;

c) uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;

d) breve explanação das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização, incluindo:

   1) conformidade com a legislação e com requisitos regulamentares e contratuais;

   2) requisitos de conscientização, treinamento e educação em segurança da informação;

   3) gestão da continuidade do negócio;

   4) conseqüências das violações na política de segurança da informação;

e) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;

f) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

Convém que esta política de segurança da informação seja comunicada através de toda a organização para os usuários de forma que seja relevante, acessível e compreensível para o leitor em foco.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Violações de Regras

8.1 Antes da contratação[3]

Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.

Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.

Convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis.

Convém que todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação.

UEZ
CENTRO UNIVERSIT
ESTADUAL DA ZONA O

Produção de Registros para Auditoria

10.10.1 Registros de auditoria

Controle

Convém que registros *(log)* de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

Diretrizes para implementação

Convém que os registros *(log)* de auditoria incluam, quando relevante:

a) identificação dos usuários;

b) datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*log-on*) e saída (*log-off*) no sistema;

c) identidade do terminal ou, quando possível, a sua localização;

d) registros das tentativas de acesso ao sistema aceitas e rejeitadas;

e) registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;

f) alterações na configuração do sistema;

g) uso de privilégios;

h) uso de aplicações e utilitários do sistema;

i) arquivos acessados e tipo de acesso;

j) endereços e protocolos de rede;

k) alarmes provocados pelo sistema de controle de acesso;

l) ativação e desativação dos sistemas de proteção, tais como sistemas de antivírus e sistemas de detecção de intrusos.

Informações adicionais

Os registros (*log*) de auditoria podem conter dados pessoais confidenciais e de intrusos. Convém que medidas apropriadas de proteção de privacidade sejam tomadas (ver 15.1.4). Quando possível, convém que administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (*log*) de suas próprias atividades (ver 10.1.3).

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Próximo Tópico

- Auditoria