Neste documento constam a prova A (1a. Página) e a prova B (2a. Página) da 2a. prova presencial da disciplina Segurança e Auditoria de Sistemas.

PROVA A

Questão 1) (9 pontos)

A classificação das informações é um dos primeiros passos para se elaborar um plano de segurança. Uma classificação adotada amplamente define quatro níveis, dois deles são: pública e interna. Quando uma informação é classificada de acordo com cada nível citado anteriormente ?

Uma informação **pública** é aquela que pode ser divulgada para qualquer pessoa sem que haja implicações para a instituição. Uma informação **interna** é uma informação que não devem sair do âmbito da instituição. Entretanto, caso isso vem a ocorrer, as consequências não serão críticas.

Questão 2) (9 pontos)

Objetivos da segurança devem ser tratados cuidadosamente pela equipe de informática e pelos usuários de sistemas. Explique os objetivos indicados abaixo.

Privacidade: proteger informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação;**Integridade dos dados**: evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação; **Isolamento**: certificar que de que nada importante do sistema foi alterado ou adulterado em caso de acesso indevido.

Questão 2) (9 pontos)

Qual o objetivo da análise de riscos no contexto de segurança da informação ? Qual a sua relação com a Análise de Ameaças e Vulnerabilidades ?

O objetivo da análise de riscos é medir ameaças, vulnerabilidades e impactos em um determinado ambiente, de forma a proporcionar a adoção de medidas apropriadas tanto às necessidades de negócio de uma instituição, ao proteger seus recursos de informação, como aos usuários que necessitam utilizar esses recursos, levando em consideração justificativas de custos, nível de proteção e facilidade de uso.

A análise de riscos, então, engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, a qual identifica os componentes críticos e o custo potencial ao usuário do sistema.

Questão 3) (8 pontos)

Quais são as responsabilidades e a importância de um modelo de governança da segurança da informação para uma organização?

O modelo de governança de segurança da informação é responsável para que as organizações tenham proteção contra os riscos inerentes ao uso da infraestrutura de TIC ao mesmo tempo que obtenham indicadores dos benefícios de ter essa infra- estrutura segura e confiável. Em função do grande número de dados provenientes das mais diversas fontes da infraestrutura de TIC no cenário atual, é importante que boa parte das decisões seja tomada de forma estruturada e científica e não mais de forma sistêmica. No enfoque organizacional, de forma científica, o gestor pode utilizar modelos de governança organizacional apoiados por ferramentas disponíveis na teoria da decisão.

PROVA B

Questão 1) (9 pontos)

A classificação das informações é um dos primeiros passos para se elaborar um plano de segurança. Uma classificação adotada amplamente define quatro níveis, dois deles são: confidencial e secreta. Quando uma informação é classificada de acordo com cada nível citado anteriormente ?

Uma informação confidencial é aquela cujo acesso é realizado de acordo com estrita necessidade, isto é, os usuários só podem acessá-las se forem fundamentais para o desempenho de suas funções na instituição. O funcionamento da organização pode ficar seriamente comprometido, danos financeiros podem ocorrer ou perda de mercado para a concorrência se essas informações forem acessadas de forma não autorizadas. Uma informação secreta é aquela cujo acesso interno ou externo de pessoas não autorizadas é extremamente crítico para a organização.

Questão 2) (9 pontos)

Objetivos da segurança devem ser tratados cuidadosamente pela equipe de informática e pelos usuários de sistemas. Explique os objetivos indicados abaixo.

Confidencialidade: proteger informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação; **Disponibilidade**: proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização; **Confiabilidade**: garantir que, mesmo em condições adversas, o sistema atuará conforme o esperado.

Questão 3) (9 pontos)

O que se entende por controle de acesso lógico, controle de acesso físico e controle de acesso ambiental? Lista também duas verificações para cada um dos controles citados anteriormente.

O controle de acesso lógico tem como objetivo proteger dados e aplicações de software contra acesso indevido e malicioso. Verificações (Duas das listadas abaixo):

1. Conceder acesso, aos usuários, apenas aos recursos realmente necessários;
2. Restringir e monitorar o acesso a recursos críticos;
3. Utilizar softwares de controle de acesso lógico;
4. Utilizar criptografia
5. Revisar periodicamente as listas de controle de acesso;
6. Bloquear a conta do usuário após um certo número de tentativas frustadas de logon;
7. Restringir acesso a determinados periféricos.

O controle de acesso físico trata das medidas de proteção contra acesso físico não autorizado(Duas das listadas abaixo):

1. Instituir formas de identificação capazes de distinguir um funcionário de um visitante e categorias diferentes de funcionários, se for necessário;
2. Exigir devolução de bens de propriedade da instituição quando o funcionário é desligado ou demitido;
3. Controlar a entrada e a saída de equipamentos, registrando data, horário e responsável;
4. Controlar a entrada e saída de visitantes, registrando data, horários e local de visita, e dependendo do grau de segurança necessário, acompanhá-los até o local de destino;
5. Instituir vigilância no prédio, 24 horas por dia, 7 dias por semana.

O controle de acesso ambiental visa proteger os recursos computacionais contra danos provocados por desastres naturais, falhas na rede de fornecimento de energia, ou no sistema de ar condicionado dentre outros(Duas das listadas abaixo).

1. Instituir procedimentos de prevenção contra incêndios de acordo com as normas vigentes;
2. Na construção do prédio, usar materiais resistentes à ação do fogo e instalar para-raios;
3. Planejar a disposição dos equipamentos e móveis de forma a facilitar a circulação das pessoas, principalmente nas áreas próximas às saídas de emergência;
4. Adotar política anti-fumo nas dependências da organização;
5. Proibir o consumo de comidas e bebidas próximo aos equipamentos;
6. Manter as salas limpas, sem acúmulo de papéis ou outros materiais de fácil combustão.

Questão 3) (8 pontos)
Como o autor do artigo "Algumas recomendações para um modelo de governança da segurança da informação" define governança da Tecnologia da Informação e Comunicação (TIC) ?

Uma estrutura de relacionamentos entre processos para direcionar e controlar uma empresa para atingir seus objetivos corporativos, por meio da agregação de valor e controle dos riscos pelo uso da TIC e seus processos; ou

Capacidade organizacional exercida pela mesa diretora, gerente executivo e gerente ; de TIC, de controlar o planejamento e a implementação das estratégias de TIC e, dessa forma, permitir a fusão da TIC ao negócio ;ou

Especificação das decisões corretas em um modelo que encoraje o comportamento desejável no uso de TIC, nas organizações ; ou

Neste documento constam os gabaritos da 1a. prova presencial (Manhã), na página 1, e o da 1a. prova presencial (Tarde), na página 2, da disciplina de Segurança e Auditoria de Sistemas

1a. Prova Presencial Segurança e Auditoria de Sistemas (Manhã).

Questão 1)
A ISO/IEC 12207 agrupa os processos de ciclo de vida em processos fundamentais, em processos de apoio e em processo organizacionais. Descreva cada um deles e indique em qual processo a auditoria de computadores se enquadra.(9 pontos)
Processos fundamentais abrangem a contratação entre o adquirente e o fornecedor e a execução do desenvolvimento, da operação ou da manutenção de produtos de software durante o ciclo de vida do software. **Processos de apoio** são processos que auxiliam e contribuem para o sucesso e qualidade do projeto de software. Um processo de apoio é empregado e executado, quando necessário, por um dos seguintes processos. **Processos organizacionais** são processos que são empregados por uma organização para estabelecer e implementar uma estrutura constituída pelos processos de ciclo de vida e pelo pessoal envolvido no desenvolvimento de software. O processo de auditoria se enquadra nos processos de apoio.

Questão 2)
O processo de auditoria pode ser dividido em três grandes fases: planejamento, execução e fechamento. Com base nesta afirmativa, descreva o objetivo principal de cada uma destas fases (9 pontos)
A fase de planejamento ou pré-auditoria identifica-se os **instrumentos indispensáveis** à sua realização (recursos, área de verificação, metodologias, objetivos de controle e procedimentos a serem adotados). Ao longo da execução da auditoria, deve **reunir evidências suficientemente confiáveis**, relevantes e úteis para a realização da auditoria. Na finalização, o auditor normalmente apresenta seus achados e conclusões na forma de um relatório escrito.

Questão 3)
Ao longo da execução da auditoria, a equipe deve reunir evidências suficientemente confiáveis, relevantes e úteis para a realização da auditoria. Quais são estas evidências e como são descritas ? (9 pontos)
Evidência física: observações de atividades desenvolvidas pelos funcionários, gerentes, sistemas, equipamentos e etc. **Evidência documentária**: resultados de extração de dados, registros de transações e etc. **Evidência fornecida pelo auditado**: transcrições de entrevistas, cópias de documentos cedidos pelo auditado, fluxogramas, e-mails trocados com a gerência, relatórios e etc. **Evidência analítica**: comparações, cálculos e interpretações de documentos de entidades similares ou da mesma entidade em períodos de tempos diferentes.

Questão 4)
Quanto a forma de abordagem a auditoria pode ser horizontal ou orientada. Explique cada uma delas. (8 pontos)
Auditoria Horizontal: com tema específico realizada em várias entidades paralelamente; **Auditoria Vertical ou Orientada**: focada em uma atividade específica com fortes indícios de erros e fraudes.

1a. Prova Presencial Segurança e Auditoria de Sistemas (Tarde).

Questão 1)
Um sistema de informação pode ser definido como uma combinação organizada de pessoas, hardware, software, redes de computadores e dados que possibilita a coleta, transformação e a disseminação de informações em uma organização. Com base nessa definição, qual a função desempenhada por cada um dos elementos que fazem parte de um sistema de informação ?(9 pontos)
Um sistema de informação pode ser definido como uma combinação organizada de pessoas (especialistas e usuários finais), hardware (computadores e periféricos), software (sistemas operacionais, editores de texto, ferramentas de desenvolvimento, banco de dados e etc), rede de computadores (meios de comunicação, processadores de comunicações e etc) dados (descrição de produtos, banco de dados de estoque e etc) que possibilita a coleta, transformação e disseminação de informações em uma organização.

Questão 2)
Defina auditoria de computadores, campo, âmbito. Além disto, responda como área de verificação se relaciona com campo e âmbito ? (9 pontos)
Tipo de auditoria, essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança das informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências

Um campo engloba o **objeto** (entidade completa, uma parte selecionada ou uma função dessa entidade) a ser fiscalizado, o **período** a ser fiscalizado e **natureza** da auditoria. O âmbito engloba a **Amplitude** e **exaustão** dos processos de auditoria, incluindo uma limitação racional dos trabalhos a serem executados (**grau de abrangência**).A área de verificação é o conjunto formado pelo **campo** e pelo **âmbito** de auditoria. Delimita de **modo preciso** os temas da auditoria, em função da entidade a ser fiscalizada e da natureza da auditoria.

Questão 3)
Explique e exemplifique controle preventivo, controle detectivo e controle corretivo.(9 pontos)
Controles preventivos: são usados para prevenir erros, omissões ou atos fraudulentos. Exemplo: senhas de acesso a um determinado sistema. **Controles detectivos**: são usados para detectar erros , omissões ou atos fraudulentos, ou ainda relatar a sua ocorrência. Exemplo: softwares de controle de acesso e relatórios de tentativas de acesso não autorizado. **Controles corretivos**: são usados para reduzir impactos ou corrigir erros detectados. Exemplo: plano de contingência.

Questão 4)
Quais as evidências que podem ser encontradas durante uma auditoria ? E em qual fase elas são levantadas ?(8 pontos)
Evidência física: observações de atividades desenvolvidas pelos funcionários, gerentes, sistemas, equipamentos e etc;**Evidência documentária**: resultados de extração de dados, registros de transações e etc;**Evidência fornecida pelo auditado**: transcrições de entrevistas, cópias de documentos cedidos pelo auditado, fluxogramas, e-mails trocados com a gerência, relatórios e etc.**Evidência analítica**: comparações, cálculos e interpretações de documentos de entidades similares ou da mesma entidade em períodos de tempos diferentes. Estas evidências são levantadas na fase de execução.

Neste documento constam a 1a. prova presencial (A), na página 1, e a 1a. prova presencial (B), na página 2, da disciplina de Segurança e Auditoria de Sistemas

1a. Prova Presencial Segurança e Auditoria de Sistemas (A).

Questão 1)(12 pontos)

Defina auditoria de computadores, campo, âmbito. Além disto, responda como área de verificação se relaciona com campo e âmbito ?

Tipo de auditoria, essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança das informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências

Um campo engloba o **objeto** (entidade completa, uma parte selecionada ou uma função dessa entidade) a ser fiscalizado, o **período** a ser fiscalizado e **natureza** da auditoria. O âmbito engloba a **amplitude** e **exaustão** dos processos de auditoria, incluindo uma limitação racional dos trabalhos a serem executados (**grau de abrangência**). A área de verificação é o conjunto formado pelo **campo** e pelo **âmbito** de auditoria. Delimita de **modo preciso** os temas da auditoria, em função da entidade a ser fiscalizada e da natureza da auditoria.

Questão 2)(12 pontos)

Conceitue controle e descreva três tipos de controles estudados na disciplina.

Fiscalização exercida sobre as atividades de pessoas, órgãos, produtos, para que tais atividades **não se desviem** das normas preestabelecidas.

Preventivos:são usados para prevenir erros, omissões ou atos fraudulentos. **Detectivos**: são usados para detectar erros , omissões ou atos fraudulentos, ou ainda relatar a sua ocorrência. **Corretivo**s: são usados para reduzir impactos ou corrigir erros detectados.

OU

Pré-controle: rotinas e resultados embutidos e obtidos no início de um processamento, com o objetivo de garantir às rotinas operacionais a qualidade dos dados de elas são alimentadas. **Corrente**: rotinas e informações de controle que acompanham o processamento ou que validam e dão o aval às informações operacionais geradas a cada sequência de rotinas operacionais. **Pós-controle**: rotinas que fazem cruzamentos entre diversas informações operacionais finais geradas, ou entre informações finais e informações iniciais.

Questão 3)(11 pontos)

Quanto a abordagem como podemos classificar uma auditoria ? Descreva todas as categorias citadas.

Auditoria Horizontal: com tema específico realizada em várias entidades paralelamente; **Auditoria Vertical ou Orientada**: focada em uma atividade específica com fortes indícios de erros e fraudes.

1a. Prova Presencial Segurança e Auditoria de Sistemas (B).

Questão 1)(12 pontos)

Um sistema de informação pode ser definido como uma combinação organizada de pessoas, hardware, software, redes de computadores e dados que possibilita a coleta, transformação e a disseminação de informações em uma organização. Com base nessa definição, qual a função desempenhada por cada um dos elementos que fazem parte de um sistema de informação ? **(12 pontos)**

Um sistema de informação pode ser definido como uma combinação organizada de pessoas (especialistas e usuários finais), hardware (computadores e periféricos), software (sistemas operacionais, editores de texto, ferramentas de desenvolvimento, banco de dados e etc), rede de computadores (meios de comunicação, processadores de comunicações e etc) dados (descrição de produtos, banco de dados de estoque e etc) que possibilita a coleta, transformação e disseminação de informações em uma organização.

Questão 2)(12 pontos)

A engenharia de software é um disciplina da engenharia que engloba três elementos básicos: processos, métodos e ferramentas. Explique cada um deles e, responda também, como eles se relacionam.

Engenharia de software é um ramo da engenharia que engloba processos, métodos e ferramentas e cujo foco é o desenvolvimento dentro de custos adequados de sistemas de software de alta qualidade. Os processos englobam as atividades que deve ser realizadas e o resultados associados para se produzir um software, os métodos indicam abordagens estruturadas(notações, regras e procedimentos) para se executar cada atividades e as ferramentas fornecem o apoio automatizado aos métodos e atividades do processo.

Questão 3)(11 pontos)

Quais as evidências que podem ser encontradas durante uma auditoria ? E em qual fase elas são levantadas ?

Evidência física: observações de atividades desenvolvidas pelos funcionários, gerentes, sistemas, equipamentos e etc;Evidência documentária: resultados de extração de dados, registros de transações e etc;Evidência fornecida pelo auditado: transcrições de entrevistas, cópias de documentos cedidos pelo auditado, fluxogramas, e-mails trocados com a gerência, relatórios e etc. Evidência analítica: comparações, cálculos e interpretações de documentos de entidades similares ou da mesma entidade em períodos de tempos diferentes.

Disciplina: Segurança e Auditoria de Sistemas

Prof. Carlos Barreto Ribas
ribas@pucminas.br

Unidade 1- Gestão da Segurança da Informação

Segurança da Informação

Motivação para se praticar a Gestão da Segurança da Informação

***Dados** e **informações** podem ser:*

- perdidos; - roubados; - adulterados;

- processados errados; - acessados indevidamente;

Segurança da Informação

Podendo causar sérios impactos sobre:

- a continuidade dos processos;

- a imagem das pessoas / organizações;

- credibilidade; - competitividade;

- finanças; - etc.

Segurança da Informação

Foco dos modelos de segurança, inclusive os aplicados à Segurança da Informação:

- todo e qualquer modelo de segurança possui como objetivo central a palavra

"Continuidade".

Segurança da Informação

- Segurança da informação é a proteção da informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizando os riscos, maximizando o retorno sobre os investimentos e oportunidades para as organizações.

Segurança da Informação

De acordo com a Norma ISO-17799, que hoje tem o número de ISO-27002,

Segurança da Informação é a preservação da confidencialidade, integridade e disponibilidade da informação.

Segurança da Informação

Confidencialidade

- Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Segurança da Informação

Integridade

- Salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

Segurança da Informação

Disponibilidade

- Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessários.

Segurança da Informação

- A segurança da informação é obtida a partir da implementação de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Segurança da Informação

Fontes de requisitos de

Segurança da Informação:

-Análise / Avaliação de Riscos;

-Legislação e normas vigentes;

-Princípios e objetivos de negócio.

Segurança da Informação

Grandes classes de problemas:

- sinistros; - fraudes e sabotagens;

- erros operacionais; - falhas de hardware;

- falhas em comunicações;

- erros em entrada de dados;

Segurança da Informação

Sinistros

- enchentes; - explosões; - desabamentos;

- curtos-circuitos; - descargas atmosféricas;

- furacões; - terremotos; - incêndios;

- atentados terroristas;

- quedas e picos de energia;

Segurança da Informação

Fraudes e Sabotagens

- cópias não autorizadas de projetos, processos, sistemas, programas e dados;

- roubo de informações; - adulteração de dados;

- espionagem industrial/comercial; - etc;

Segurança da Informação

Erros Operacionais

- perda de dados históricos; - apagar arquivos indevidos; - uso equivocado de versões de sistemas, programas e dados;

- não realização de rotina de backup;

- outros;

Segurança da Informação

Falhas de Hardware

- falhas em conexões físicas; - problemas em componentes; - problemas em mídias móveis como HD externo, pen drive, cd, fita;

- falhas intermitentes em equipamentos;

- etc;

Segurança da Informação

Falhas em Comunicações

- problemas em provedores de acesso;

- problemas em equipamentos (roteadores, switch, modem, ..) e em componentes de rede; - falhas nos meios de transmissões de dados (antenas, satélite, cabos, fibras, etc);

Segurança da Informação

Erros em Entrada de Dados

- todo e qualquer processo que pode levar a uma falta de consistência na entrada de um dado.

Segurança da Informação

Conceitos básicos para se pensar segurança na prática

Proprietário da Informação

Pessoa que tem o poder e a responsabilidade total sobre um conjunto de dados e sistemas a ele vinculado.

Segurança da Informação

Usuário da Informação

Pessoa autorizada pelo proprietário a acessar e utilizar dados e sistemas para a realização do seu trabalho.

Unidade 1- ISO/IEC-27001

Segurança da Informação

ABNT NBR ISO/IEC 27001:2013

Tecnologia da informação

Técnicas de segurança – Sistemas de Gestão da Segurança da Informação Requisitos

Segurança da Informação

Escopo

Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação (SGSI) dentro do contexto da organização.

Segurança da Informação

Sistemas de Gestão de Segurança da Informação – (SGSI)

A organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação (SGSI).

Determinando o escopo do SGSI (1/2)

Deve-se considerar:

- as questões internas e externas que são relevantes para o seu propósito;

Segurança da Informação

- os requisitos das partes interessadas, incluindo os legais e regulamentares, bem como as obrigações contratuais;

- as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas desempenhadas por outras organizações; (2/2)

Liderança (1/5)

Liderança e Comprometimento

A alta direção deve demonstrar sua liderança e comprometimento em relação ao SGSI pelos seguintes meios:

Segurança da Informação

Liderança (2/5)

- assegurando que a política de segurança e os objetivos de segurança da informação estejam estabelecidos e que são compatíveis com a direção estratégica da organização;

Segurança da Informação

Liderança (3/5)

- garantindo a integração dos requisitos do SGSI dentro dos processos da organização;

- assegurando que os recursos necessários para o SGSI estejam disponíveis;

Segurança da Informação

Liderança (4/5)

- comunicando a importância de uma gestão eficaz de segurança da informação e da conformidade com os requisitos do SGSI;

- assegurando que o SGSI alcance os seus resultados pretendidos;

Segurança da Informação

- orientando e apoiando pessoas que contribuam para a eficácia do SGSI;

- promovendo a melhoria continua;

- apoiando outros papéis relevantes da gestão para demonstrar como sua liderança aplica às áreas sob sua coordenação; (5/5)

Política (1/3)

A alta direção deve estabelecer uma política da informação que:

- seja apropriada ao propósito da organização;

- inclua os objetivos de segurança da info;

Política (2/3)

- inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;

- inclua o comprometimento com a melhoria contínua do SGSI;

Segurança da Informação

A política da informação deve: (3/3)

- estar disponível como informação documentada;

- ser comunicada dentro da organização;

- estar disponível para as partes interessadas, conforme apropriado;

Segurança da Informação

Autoridades, responsabilidades e papeis organizacionais

A alta direção deve atribuir responsabilidade e autoridade aos papeis relevantes para:

Segurança da Informação

- assegurar que o SGSI está em conformidade com as normas e regras;

- relatar sobre o desempenho do SGSI para a mesma;

Segurança da Informação

Planejamento

Quando do planejamento do SGSI, a organização deve considerar as questões internas e externas que são relevantes, os requisitos das partes interessadas e determinar os riscos e oportunidades que precisam ser consideradas.

Segurança da Informação

Objetivos da Segurança da Informação e planejamento para alcança-los (1/2)

Os objetivos devem:

- ser consistentes com a política de segurança da informação;

- ser mensuráveis (quando aplicável);

Segurança da Informação

(2/2)

- levar em conta os requisitos aplicáveis e os resultados da avaliação e tratamento dos riscos;

- ser comunicados;

- ser atualizados;

Segurança da Informação

Para o planejamento, a organização deve determinar:

- o que será feito; - quem será responsável;

- quais recursos serão necessários;

- quando estará concluído;

- como os resultados serão avaliados;

Apoio ao SGSI (1/4) - Recursos

- a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação;

Apoio ao SGSI (2/4) - Competência

- a organização deve determinar a competência necessária das pessoas envolvidas com a segurança da informação;

- assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência adquirida;

Apoio ao SGSI (3/4) - Conscientização

As pessoas que realizam trabalhos na organização devem estar cientes da:

- política de segurança;

- suas contribuições para a eficácia do SGSI;

- implicações com as não conformidades com os requisitos do SGSI;

Apoio ao SGSI (4/4) - Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o SGSI incluindo:

Segurança da Informação

- o que comunicar;

- quando comunicar;

- quem comunicar;

- quem será comunicado; e

- o processo pelo qual a comunicação será realizada;

Operação (1/3)

Planejamento operacional e controle (1/2)

- a organização deve planejar, implementar e controlar os processos necessários para atender aos requisitos de segurança da informação e implementar as ações previstas;

Planejamento operacional e controle (2/2)

- deve assegurar também, que os processos terceirizados estão determinados e são controlados;

Operação (2/3)

Avaliação de riscos de segurança da infor.

- a organização deve realizar avaliações de riscos de segurança da informação em intervalos planejados, ou quando mudanças significativas forem propostas ou ocorrerem;

Operação (3/3)

Tratamento de riscos de segurança da informação

- a organização deve implementar o plano de tratamento de riscos de segurança da informação;

Avaliação de Desempenho (1/3)

Monitoramento, medição, análise e avaliação (1/2)

- a organização deve avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão de segurança da informação;

Segurança da Informação

(2/2)

Para tal deve determinar:

- o que precisa ser monitorado e medido;

- os métodos para monitoramento, medição, análise e avaliação;

Avaliação de Desempenho (2/3)

Auditoria Interna

- a organização deve conduzir auditorias internas em intervalos planejados para prover informações sobre o quanto o SGSI está em conformidade e o quanto está efetivamente implementado e mantido;

Avaliação de Desempenho (3/3)

Análise crítica pela Direção

- A alta direção deve analisar criticamente o SGSI em intervalos planejados, para assegurar a contínua adequação, pertinência e eficácia.

Melhoria (1/2)

Não conformidade e ação corretiva

Quando uma não conformidade ocorre, a organização deve:

Segurança da Informação

- reagir a não conformidade;

- avaliar a necessidade de ações para eliminar as causas de não conformidade para evitar a repetição da mesma;

- implementar quaisquer ações necessárias, analisar criticamente as mesmas e realizar as mudanças quando necessário;

Melhoria (2/2)

Melhoria Contínua

A organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação – SGSI.

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.

Plano de Continuidade de Negócios

Plano de Continuidade de Negócios

É o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte. **(Norma ABNT-NBR 15999)**

Plano de Continuidade de Negócios

É um processo de gestão que da capacidade a uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de negócios críticos.

Plano de Continuidade de Negócios

Visa prevenir a ocorrência de desastres e preparar a empresa para minimizar o impacto de uma crise com a rápida ativação de processos alternativos, quando da indisponibilidade dos processos usuais.

Plano de Continuidade de Negócios

O **propósito** é permitir que uma organização se recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios.

Plano de Continuidade de Negócios

Descreve como a organização responde a um evento para garantir que as funções críticas do negócio, retornem a um nível de operação **aceitável** dentro de um prazo considerado razoável.

Provê uma descrição detalhada das ações a serem tomadas em resposta a uma interrupção inaceitável dos serviços críticos da organização.

Plano de Continuidade de Negócios

Deve ser desenvolvido preventivamente a partir de um conjunto de estratégias e planos táticos capazes de permitir o planejamento e a garantia dos serviços essenciais, devidamente identificados e preservados.

Este processo orienta e define como e quais ações devem ser executadas para que se construa uma resiliência organizacional capaz de responder efetivamente e salvaguardar os negócios da organização.

Plano de Continuidade de Negócios

O **objetivo** do **Plano de Continuidade de Negócios (PCN)** é garantir que os sistemas críticos para o negócio de uma empresa sejam retornados a sua condição operacional normal em um prazo aceitável, por ocasião da ocorrência de um incidente de segurança.

O PCN visa, com isso, tornar possível o funcionamento da organização em um nível aceitável nas situações de contingência, resguardando os interesses, a reputação, a imagem da organização e suas atividades fim de significativo valor agregado.

Plano de Continuidade de Negócios

Ameaças a Continuidade de Negócios

Todas as atividades de negócios de uma organização estão sujeitas a interrupções pelos mais diversos motivos.

Ter um PCN propicia a organização a capacidade de reagir adequadamente às interrupções operacionais enquanto preserva a vida e protege o bem estar e a segurança dos envolvidos.

Plano de Continuidade de Negócios

Ameaças potenciais (sinistros)

Falhas sistêmicas;
Pandemias;
Terrorismo /Sabotagem;
Catástrofes Naturais;
Fraudes;
Sabotagem;
Roubo/assalto;
Incêndio.

Plano de Continuidade de Negócios

Um **Plano de Continuidade** deve responder algumas questões, dentre elas:

Quais são os processos críticos para o negócio da organização?

Quais são os riscos e ameaças existentes?

Quais são os recursos necessários para enfrentar e superar os riscos existentes?

Qual é a estratégia de recuperação adequada?

O que devemos monitorar e controlar?

Plano de Continuidade de Negócios

A **elaboração do PCN** é algo especifico e singular a cada organização e riscos envolvidos.

Um plano PCN deverá conter os seguintes tópicos:

- Objetivo e Escopo;
- Instruções sobre como usar o plano;
- Mapeamento de potenciais cenários de perda;
- Identificação, análise e avaliação dos Riscos;
- Definição das ações a serem tomadas;
- Definição de responsabilidades e deveres;
- Roteiro de simulação de teste de funcionamento;
- Mecanismo de ativação do Plano.

Plano de Continuidade de Negócios

O **PCN** resume em três etapas simples:

- **Análise de risco**: o que de ruim pode vir a acontecer?
- **Análise de impacto**: de que forma eventuais ameaças podem impactar o negócio?
- **Plano de ação**: se um risco se concretizar, quais atitudes e ações são necessárias para a retomada das operações prejudicas pelos efeitos do evento ocorrido.

A elaboração de um plano de continuidade de negócios envolve a preparação, teste, e manutenção de ações específicas para proteger os processos críticos da organização.

Plano de Continuidade de Negócios

Benefícios do PCN

- Identificação de processos críticos e do impacto de sua paralisação para toda a organização;
- Conhecimento do grau de exposição aos riscos;
- Resposta eficiente às interrupções, sobretudo em função de um planejamento das ações necessárias;
- Treinamento do pessoal envolvido na resposta a ocorrências de impactos negativos relevantes;

Plano de Continuidade de Negócios

Benefícios do PCN

- Preservação da reputação da organização no que tange a uma administração profissional na gestão, em caso de crise;
- Minimização de possíveis impactos às partes interessadas e ao patrimônio;
- Significativo aumento da probabilidade de sobrevivência da entidade ou do negócio em caso de uma crise, quaisquer que sejam as suas causas;
- Promoção de entendimento mais claro e amplo do “modus operandi” da organização, permitindo a oportunidade de melhorias.

Política de Segurança da Informação

Política de Segurança da Informação

A Política de Segurança da Informação tem como objetivo estabelecer **normas**, **diretrizes e procedimentos** que assegurem a **segurança das informações** em uma organização.

Política de Segurança da Informação

Para tal, ela busca garantir:

Política de Segurança da Informação

- A **confiabilidade das informações** através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;

- O **compromisso da empresa** com a proteção das informações de sua propriedade e/ou sob sua guarda;

- A **participação e cumprimento** por todos os colaboradores em todo o processo.

Política de Segurança da Informação

Porque a Política de Segurança tem que ser para todos os **colaboradores** em todos **os níveis hierárquicos** ?

Política de Segurança da Informação

"Uma corrente é tão forte quanto seu elo mais fraco".

Não adianta a área da **Tecnologia da Informação** impor controles e medidas técnicas se não existir a **participação dos colaboradores**, por exemplo, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico se um funcionário que tem acesso legítimo a determinada área restrita, resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área.

Política de Segurança da Informação

A área de **Tecnologia da Informação** é a responsável pela salvaguarda dos dados da organização, mas o processo de segurança da informação deve envolver **todos os colaboradores**, **independente do nível hierárquico**, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação **não autorizada**.

Política de Segurança da Informação

Diante do exposto, a **Política da Segurança da Informação** vem propor uma **Gestão de Segurança da Informação** baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: **entender o negócio e aplicar segurança a ele.**

Política de Segurança da Informação

ALTA DIREÇÃO

A efetividade Política de Segurança da Informação depende estritamente do **comprometimento da alta direção**.

É essencial que os responsáveis por liberar recursos, aplicar sanções, criar regras e portarias, apoiem a PSI e demonstrem seu comprometimento para que os colaboradores se sintam motivados e obrigados a cumpri-la.

Política de Segurança da Informação

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações devem ser classificadas e identificadas por rótulos, considerando níveis, como exemplo:

- Pública;
- Interna;
- Confidencial;
- Confidencial restrita;

Política de Segurança da Informação

– Pública

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

Política de Segurança da Informação

- **Interna**

São informações disponíveis aos colaboradores da organização para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

Política de Segurança da Informação

– Confidencial

São informações de acesso restrito a um colaborador ou grupo de colaboradores.

Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.

Política de Segurança da Informação

– Confidencial restrita

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa.

Política de Segurança da Informação

Entendido a importância e os objetivos da **Política de Segurança da Informação**, a quem se destina, tipos de informações a serem protegidas, cabe a área responsável pela mesma, identificar todos os processos a serem normatizados e dar ciência a todos de como os mesmos devem ser trabalhados.

Política de Segurança da Informação

Alguns exemplos de **orientações** que podem constar em uma

Política de Segurança da Informação

Política de Segurança da Informação

Responsabilidades das partes envolvidas:

- colaboradores;
- gestores de pessoas e processos;
- comitê gestor da segurança;
- setor de Tecnologia da Informação;
- outros atores;

Política de Segurança da Informação

UTILIZAÇÃO DA REDE

O ingresso à rede corporativa deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados.

Assim, é preciso que sejam instauradas algumas regras, listadas a seguir: (listar as regras)

Política de Segurança da Informação

POLÍTICA DE SENHAS

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

(listar as regras)

Política de Segurança da Informação

E-MAIL

O e-mail é uma das principais formas de comunicação.

No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

Política de Segurança da Informação

USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operacionais durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas.

Assim, algumas medidas de segurança devem ser tomadas, são elas: (listar as medidas)

Política de Segurança da Informação

USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, contando com todos os recursos de equipamentos disponíveis, mas não pode deixar de considerar os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis. (listar as regras)

Política de Segurança da Informação

USO DE IMPRESSORAS

O uso de impressoras deve seguir algumas regras: (listar as regras)

Política de Segurança da Informação

BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança).

Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer.

Assim, estabelecem-se as regras:

(listar as regras)

Política de Segurança da Informação

VIOLAÇÃO DA POLÍTICA E PENALIDADES

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades: (listar as penalidades)

Política de Segurança da Informação

Anexos

São documentos de outros temas específicos que são gerados de forma incremental e anexados para grupos e processos que vão sendo identificados que a política deva atingir.

Política de Segurança da Informação

Sugestão Final

É fundamental que o documento oficial da **Política de Segurança da Informação**, seja redigida com uma visão técnica, mas que tenha uma redação também na **ótica jurídica**, para que a mesma possa ser utilizada em questões que envolvam a justiça.

Segurança da Informação

PUC Minas

Segurança Física

A segurança física é feita nas imediações da empresa e leva em consideração a prevenção de danos causados por desastres locais ou ambientais, como terremotos, inundações e incêndios.

Por isso, investigar a ocorrência de eventos climáticos passados é importante ao se planejar os métodos de segurança física para proteção de funcionários, equipamentos, dados e do local.

Segurança da Informação

PUC Minas

Segurança Física

Ela trata de métodos para evitar o acesso de pessoas **não autorizadas** a áreas em que se encontram dados e informações críticas da empresa.

Uma das formas de fazer isso é implantar recursos de identificação de funcionários, como o uso de crachás, senhas e cadastro de digitais.

Segurança da Informação

PUC Minas

Segurança Física

A segurança física também deve controlar a entrada e saída de equipamentos, materiais e pessoas da empresa por meio de registros de data, horário e responsável.

Quando há a entrada de visitantes na empresa, eles não devem andar sozinhos, o ideal é que sejam acompanhados por algum funcionário até o local de destino e registrados no sistema.

Segurança da Informação

PUC Minas

Segurança Física

Outro tipo de reforço para a segurança local é usar mecanismos, como fechaduras eletrônicas, câmeras e alarmes, para controlarem o acesso aos ambientes que guardam backups e computadores com dados confidenciais.

Segurança da Informação

PUC Minas

Segurança Física

Para desenvolver uma boa segurança física é preciso analisar qual é o perfil da empresa, o tipo de proteção necessária, os investimentos possíveis e definir uma política de controle de acesso físico que se encaixe ao modelo de negócio.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

A segurança física perimetral corresponde à constituição de barreiras de forma a evitar, ou retardar, intrusões e garantir uma resposta mais eficaz às mesmas.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

É o ramo da segurança que visa prevenir acessos não autorizados a equipamentos, instalações, materiais ou documentos.

Este tipo de segurança pode ser concretizado através de uma simples porta ou envolver complexos sistemas de segurança onde a tecnologia de ponta é uma constante.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

Os sistemas de segurança física têm sofrido uma evolução significativa nos últimos anos, nomeadamente devido à incorporação nos sistemas mais modernos de tecnologias como:

- utilização de detectores de infravermelhos;
- mecanismos de controle de acesso eletrônico;
- video-vigilância;
- entre outros.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

Quando se pretende garantir a segurança física de um espaço é fundamental realizar uma análise eficiente e conclusiva dos **riscos existentes**.

São definidos quatro **graus de risco** que devem ser considerados:

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

Grau 1 – Baixo Risco: Utilizado para definir instalações em que se considera pouco provável a existência de intrusões.

Neste grau, considera-se que as intrusões existentes neste tipo de edifícios não são planejadas e caracterizam-se pela tentativa de forçar portas ou janelas de forma arbitrária.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

Grau 2 – Risco Baixo a Médio: Categoria onde se situam a maioria dos sistemas residenciais ou instalações comerciais de baixo risco.

Considera-se que os intrusos não possuem grandes conhecimentos acerca dos sistemas de segurança e que têm recursos limitados. A estratégia de intrusão passa por ter acesso às instalações através de pontos desprotegidos.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

Grau 3 – Risco Médio a Elevado: É nesta categoria que está inserida a maioria das instalações comerciais e industriais.

Ao contrário das categorias anteriores, espera-se que os intrusos tenham experiência a lidar com sistemas de detecção de intrusão e que possuam o equipamento necessário para lidar com os sistemas de proteção mais simples.

Segurança da Informação

PUC Minas

Segurança Física - Perimetral

Grau 4 – Risco Elevado: Engloba as instalações de alta segurança e de risco elevado.

Nesta fase já não se espera que possíveis intrusões sejam realizadas por um único intruso. Ao invés, a expectativa é que a intrusão seja realizada por um grupo de indivíduos com elevado conhecimento sobre mecanismos de segurança, que preparou detalhadamente o plano de ação e que tem disponíveis recursos tecnológicos muito avançados.

Segurança da Informação

PUC Minas

Segurança Física

Tecnologias e Recursos Utilizadas

- **câmeras;**
- **catracas;**
- **fechaduras eletrônicas;**
- **porteiros físicos;**
- **Detectores de presença;**

Segurança da Informação

PUC Minas

Segurança Física

Tecnologias e Recursos Utilizadas

- detectores de fumaça;
- condicionadores de ar;
- salas cofre;
- no-break;
- estabilizadores de energia;

Segurança da Informação

PUC Minas

Segurança Física

Tecnologias e Recursos Utilizadas

- aterramento;
- pára-raios;
- firewall;
- cabeamento certificado;
- protetores anti-surto elétricos;
- back-up;
- etc.

Segurança Lógica

Segurança Lógica

Segurança Lógica é a forma como um sistema é protegido, seja por softwares ou regras de restrições de acesso. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação.

Segurança Lógica

As principais ameaças no que diz respeito a segurança lógica estão ligadas aos acessos indevidos, erros provocados e a perda de dados decorrente a esses erros, falhas na rede provocadas por software estranho, fraudes e sabotagens.

Segurança Lógica

Os principais mecanismos de proteção que podemos trabalhar na segurança lógica são:

1. Classificação da informação em níveis de segurança;
2. Classificação de usuários pela necessidade de acesso;

Segurança Lógica

3. Senhas;
4. Listas de controle de acesso;
5. Criptografia;
6. Firewall;
7. Sistemas de detecção de intrusão;
8. Redes virtuais privadas;
9. Assinatura digital;
10. Consistência em entrada de dados;
11. Etc;

Segurança da Informação

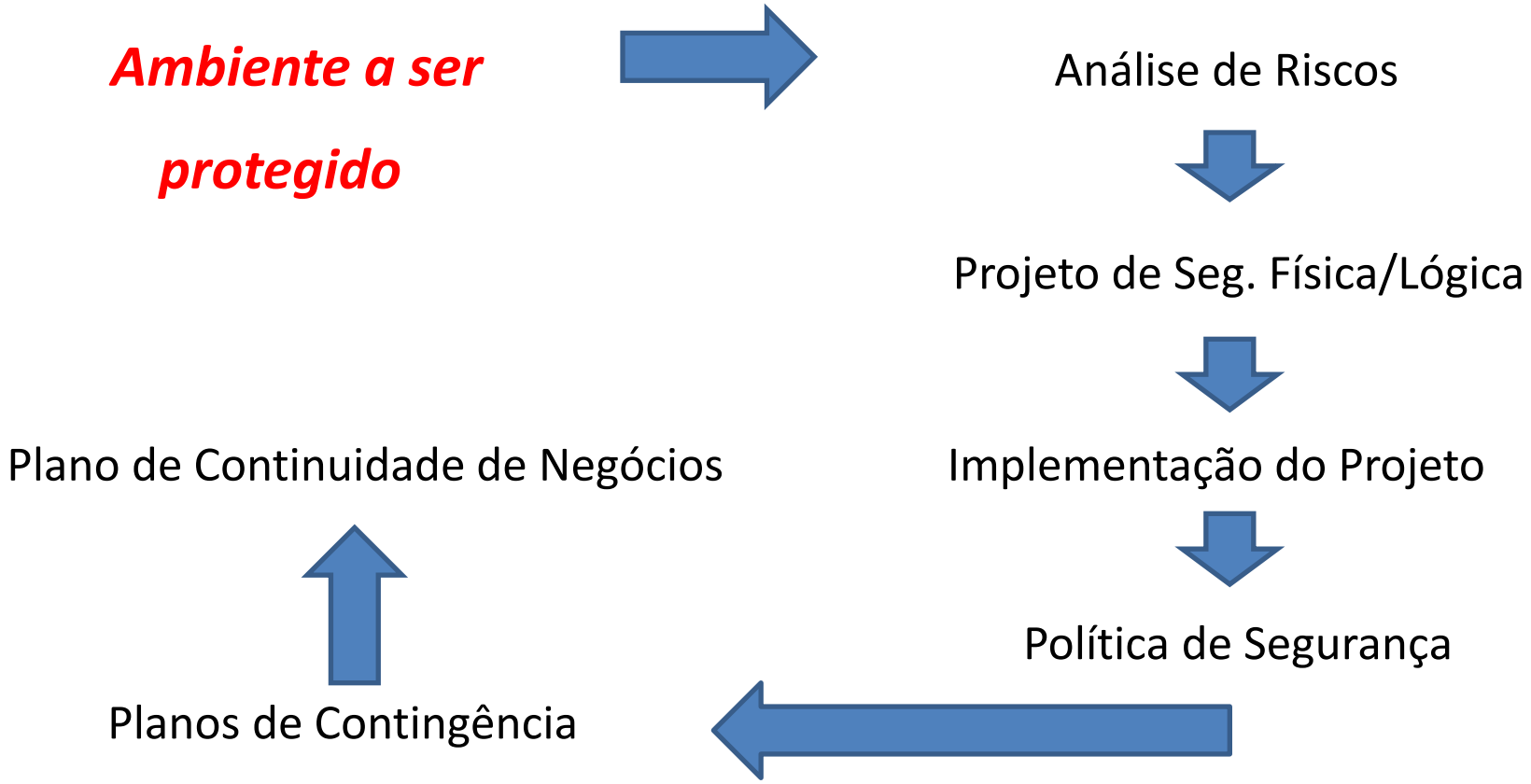
PUC Minas

Algoritmo da

Segurança da Informação

Segurança da Informação

PUC Minas



PUC Minas

Análise de Riscos

Segurança da Informação

Análise de Riscos

PUC Minas

O termo **Risco** é utilizado para designar o resultado objetivo da combinação entre a **probabilidade de ocorrência** de um determinado evento, aleatório, futuro e que independa da vontade humana, e o **impacto resultante** caso ele ocorra.

É também ligado à probabilidade de ocorrência de um determinado evento que gere prejuízo econômico.

Análise de Riscos

PUC Minas

Não existe risco "zero"

As empresas devem decidir qual o nível de risco estão dispostas a aceitar.

Análise de Riscos

PUC Minas

Quando tratamos de gerenciamento de risco, no final das contas, estamos tratando de segurança da informação.

Quando estamos implementando controles de segurança da informação, estamos buscando mitigação de riscos.

Análise de Riscos

PUC Minas

Análise de Riscos de Segurança da Informação é um método de identificação de riscos e avaliação dos possíveis danos que podem ser causados, a fim de justificar os controles de segurança.

Possui três objetivos principais:

- identificar riscos; - quantificar o impacto de possíveis ameaças; - conseguir um equilíbrio financeiro entre o impacto do risco e o custo da contramedida;

Análise de Riscos

PUC Minas

Um dos desafios da área de Segurança da Informação, ou até mesmo do departamento de Tecnologia da Informação, é integrar os objetivos do programa de segurança aos objetivos e requisitos de negócios.

Para que todos os requisitos de negócios sejam atendidos, a empresa deve alinhar os objetivos de segurança com os objetivos de negócios. Apenas dessa forma o programa de segurança será bem sucedido.

Análise de Riscos

PUC Minas

A análise de risco ajuda a empresa a delinear um orçamento adequado para um programa de segurança e os componentes de segurança que formam esse programa.

Quando a empresa souber o valor dos ativos e entender as possíveis ameaças a que eles estão expostos, a alta direção poderá tomar decisões inteligentes sobre o quanto investir na proteção desses ativos.

Análise de Riscos

PUC Minas

Objetivos: (1/2)

- Identificar ameaças em potencial à segurança de TI (Tecnologia da Informação) e sua probabilidade aproximada;

- Identificar o valor dos ativos, inclusive seu valor indireto, caso sejam danificados ou violados;

- Usar esses valores quantificados para identificar as atividades mais adequadas e econômicas para proteger o ambiente;

Análise de Riscos

PUC Minas

Objetivos: (2/2)

- Definir e gerenciar uma diretiva formal de gerenciamento de riscos de segurança;
- Integrar o gerenciamento de riscos de segurança ao ciclo de vida da infra-estrutura de TI;
- Definir processos para aprimorar a especialização em gerenciamento de riscos na empresa por meio de iterações do ciclo do gerenciamento de riscos.

Prova Global

Segurança e Auditoria de Sistemas

Escolher 3 questões para responder:

1. **Cite 10 formas de segurança física e 10 de segurança lógica.**

Segurança física:

processos de segurança física; rede elétrica; sala cofre; criptografia

Segurança Lógica:

controle de acesso; segurança de banco de dados

2. **Defina Política de Segurança.**

É a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

Proposito:

1. Informar aos usuários, equipes e gerente as suas obrigações para a proteção do tecnologia e do acesso à infraestrutura
2. Outro proposito é oferecer um ponto de referencia a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes para que sejam adequados aos requisitos propostos.

Objetivos:

1. Os objetivos devem ser determinados a partir das seguintes análises:
    1. Serviços oferecidos x Segurança Fornecido;
    2. Facilidade de Uso x Segurança
    3. Custo da Sequencia x Riscos da Perda

3. **Comente sobre a ISSO 17799 e as áreas onde ela atua.**

A norma ISO-17799 foi criada para orientar as empresas quanto as melhores praticas a serem implementadas quanto a segurança da TI.
Apresenta-se de forma totalmente flexivel, não definindo o modelo tecnologico a ser utilizado e não condicionada ao tamanho da empresa.
São 10 as áreas de controle que ela destaca que deviam ser implementadas

1. Politica de Segurança
    - Controlar a conduta das pessoas
    - Conduta de aquisição de hardware
2. Organização da Segurança
3. Classificação e Controle do Patrimônio

4. Segurança dos Funcionários
    - O correto seria: postura de segurança dos funcionarios
5. Segurança física e ambiental
    - De controle de acesso até problemas em geral
6. Gerenciamento de Operações e Comunicações;
    - Gerenciar instalações, operações, etc...
7. Controle de Acesso;
    - gerenciar acesso
8. Manutenção e Desenvolvimento de Sistemas;
    - As vezes é mexer no código, projetos.
9. Gerenciamento da Continuidade de Negócios;
10. Compatibilidade
    - Ser capaz de tornar compativel com os modelos de fora do brasil

4. Defina as características de qualidade do software

Funcionalidade: É saber o que o software tem que fazer em aspectos funcionais. É saber o tanto que ele tem que se adequar aos processos

Confiabilidade: É a capacidade que o sistema tem de tolerar falhas. É a observação do seu comportamento com relação a falhas, ou seja, não falha.

Confiabilidade da disponibilidade --> 24 hrs no ar;

Usabilidade: É um foco importante hoje e tem-se um valor maior

Eficiência: É o comportamento que o software tem em relação sao seu desempenho, ou seja, medir o tempo de resposta com relação aso recursos disponíveis.

Manutenibilidade: É o esforço de manter o software em operação ao longo do seu ciclo de vida.

Portabilidade: É a capacidade que o sistema tem de operar em ambientes operacionais especificados.