Escolas Integradas – Educação Continuada

GESTAO DA SEGURANCA DA INFORMACAO

EDUCAÇÃO DIGITAL

Agenda da Aula

- APRESENTAÇÃO DO PROFESSOR;
- OBJETIVOS DA DISCIPLINA;
- ROTEIRO DE ESTUDOS:
  - TEMA 1 Gestão de Riscos
  - TEMA 2 Análise de Vulnerabilidades
  - TEMA 3 Medidas de Proteção
  - TEMA 4 Segurança em Ativos de TI
  - TEMA 5 Sistemas de Gestão da Segurança da Informação

- DISCUSSÃO DO CASO;
- DÚVIDAS.

Boas-vindas e apresentação do Docente

Sou o Prof. Ms. Wagner José Quirici

Engº Eletrônico pelo ITA; Mestre em Administração pela FEA - USP

Atuei durante 25 anos em funções executivas, como Presidente do Serpro, da Eletropaulo Telecom, da Engeredes/Algar, da BrasilTelecom DataCenter.

Nos últimos 10 anos venho atuando na área acadêmica, ministrando cursos e desenvolvendo conteúdos na Laureate/FMU, na FEA/FUNDACE, na Universidade Federal do Paraná; na VG Educacional e na Ânima Educação.

Apresentação do Conteúdo

OBJETIVOS DA DISCIPLINA:

Caro(a) estudante, ao ler este roteiro, você vai:

- aprender como gerenciar os riscos identificados de uma organização;
- identificar vulnerabilidades dentro de processos de trabalho;
- propor medidas de proteção diante de cenários de risco;
- conhecer a gestão da segurança no âmbito de ativos de TI;
- Entender a implantação de um *software* de gestão da segurança da informação;
- compreender os múltiplos processos da gestão da segurança da informação.

ROTEIRO DE ESTUDOS:

Oferece uma visão ampla e sistemática da proteção de um dos bens mais estratégicos das organizações: **a informação**;

As consequências das violações leva a organização a mobilizar recursos para implementar as melhores práticas de garantia de ambientes informacionais seguros;

O caráter estratégico da informação, para qualquer área de negócio,
leva as organizações a priorizar sua segurança;

ROTEIRO DE ESTUDOS:

Conheceremos:

Os **padrões e procedimentos de segurança da informação**, baseados em normas internacionais de segurança;

Como as normas estão estruturadas, de forma a facilitar a adoção de suas práticas, de maneira gradativa e segmentada;

Como implementar práticas e propor soluções eficazes no gerenciamento da segurança da informação.

O conceito de Risco:

Combinação da **probabilidade** e das **consequências** da ocorrência de um evento indesejado, o que direcionam as organizações para a gestão dessas variáveis:

probabilidade e consequências das ocorrências

que caracterizam um evento como risco

(ABNT, 2005, p. 2)

Os componentes do Risco

O risco ocorre quando é concretizada:

uma **vulnerabilidade (causa),** de um incidente **indesejado (evento),**

que implicará em um **efeito (consequência)** no fluxo do trabalho.

O evento de risco é considerado uma **ameaça** quando prejudica o desenvolvimento de atividade/processo, e compromete o alcance dos objetivos organizacionais.

As análises/avaliações de riscos devem:

Identificar, Quantificar e Priorizar os riscos

com base em critérios de **aceitação, ou eliminação**, dos riscos relevantes para a organização;

Análises orientam as ações mais adequada, e as prioridades, para o gerenciamento dos riscos, bem como, a implementação dos controles de proteção contra estes riscos

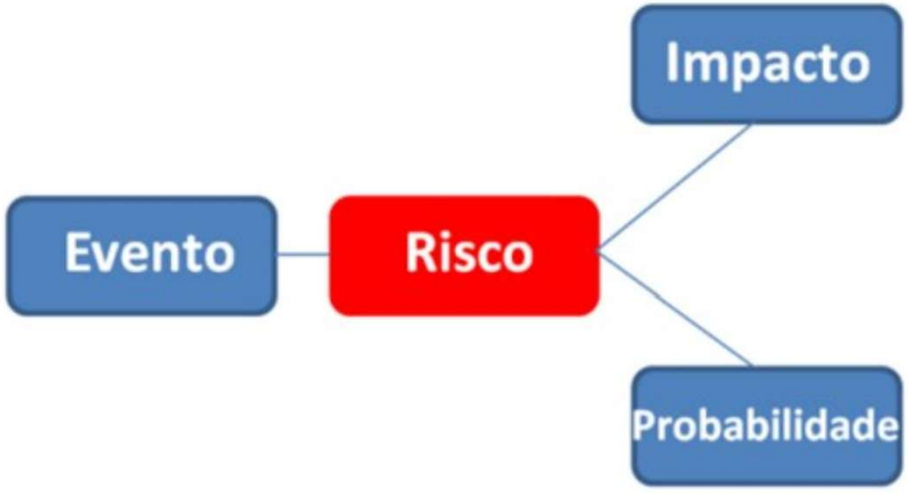
(ABNT, 2005, p.2)

Fatores de Análise do Risco

Os riscos são medidos em termos de **probabilidade de ocorrência** e do **impacto** resultante da concretização do evento de risco.

A mensuração da **probabilidade** de ocorrência está ligada a uma investigação das **causas** do risco.

O dimensionamento do **impacto** está ligado às c**onsequências** do risco.



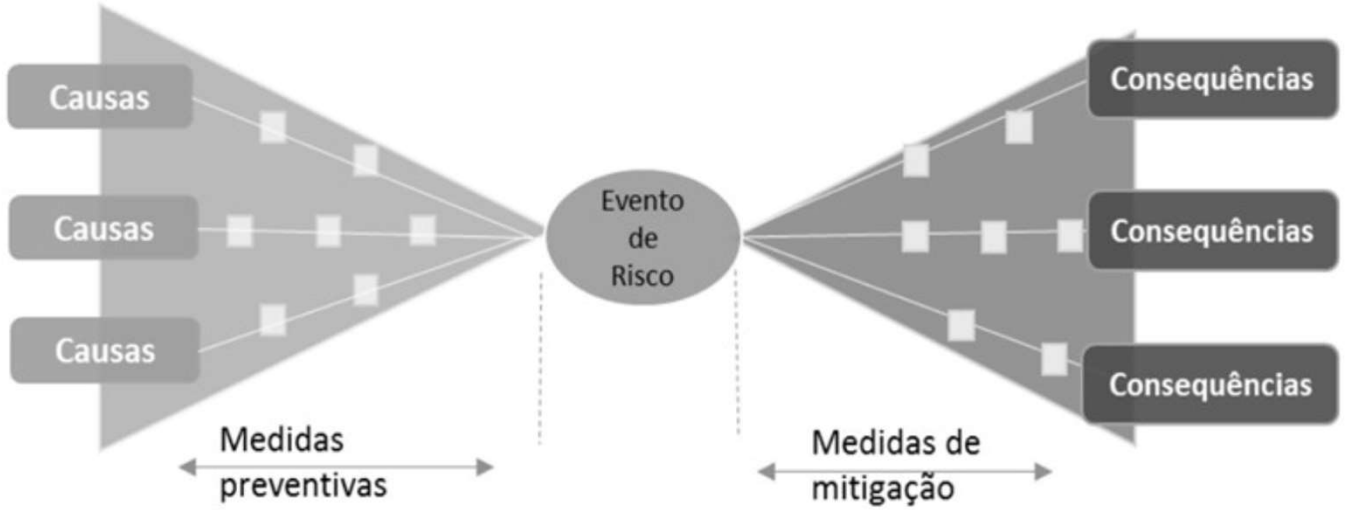
Consequências

Causas

TEMA 1 Gestão de Riscos

Análise de Risco

Conforme o Manual de Riscos do INPI (2018), é necessário conhecer o **processo de trabalho** analisado, **seus objetivos e as fontes de riscos** presentes nas atividades, quanto mais detalhada for o seu mapeamento, melhor será a análise dos eventos que podem ocorrer e afetar os objetivos.



https://www.gov.br/inpi/pt-br/governanca/integridade-publica/arquivos/documentos/manualdegestoderiscosv2-0_gequgrimn0001_aprovado.pdf

Gestão de Riscos

Etapas da Implementação

TEMA 1 Gestão de Riscos

1 - Definição dos objetivos

Objetivos:

minimizar riscos, analisar custo-benefício, reduzir falhas de sistemas...

devem estar alinhados com as **estratégias globais de negócio da organização.**

O risco é inerente a toda atividade humana.

- ✓ *A capacidade de definir o que poderá acontecer e optar entre várias alternativas é preocupação central às sociedades contemporâneas;*
- ✓ *Gestão de risco oferece uma ampla gama de decisões, exigindo atenção às possíveis falhas ou erros, nas informações e na complexa tecnologia dos processo envolvidos.*

2 - Identificação dos riscos

Definidos os objetivos, os riscos precisam ser **identificados.**

Essa etapa exige um **conhecimento apurado dos processos de trabalho da organização, como e que tipo de informação** está armazenada em seu parque tecnológico.

A gestão de riscos é uma das **áreas mais críticas**
da gestão de segurança da informação, e deve ser **precisa e efetiva**.

2 - Identificação dos riscos

Para que riscos sejam efetivamente identificados é necessário que:

- ❑Entender a área de atuação da empresa;
- ❑Mapear todo processo computacional da empresa;
- ❑Identificar e compreender as normas e as políticas internas;
- ❑Inspecionar todas as atividades críticas da empresa;
- ❑Levantar o histórico de falhas de segurança nos últimos anos

2 - Identificação dos riscos

Com os resultados desta etapa será possível:

“determinar as ações gerenciais apropriadas, priorizar os riscos a serem tratados, e implementar os controles para a proteção dos riscos identificados”

A identificação dos riscos de uma organização, por si só, não é suficiente para viabilizar a execução do processo de gestão como um todo:

É necessária a análise e a avaliação de cada risco identificado.

ABNT, 2005, p. 11

3 - Análise dos riscos

Uma ferramenta utilizada para priorização dos riscos é a matriz:

Gravidade, Urgência e Tendência GUT.

Cada risco identificado é avaliado sob a ótica dessas 3 variáveis.
Cada variável tem diferentes níveis de criticidade associados.
Cada nível tem um valor numérico correspondente.

A partir da pontuação de cada risco, segundo cada variável,
Obtem-se um valor de pontuação usado para a priorização dos riscos.

Priorização dos Riscos

Matriz GUT

MATRIZ GUT

G x U x T

A combinação dessas pontuações definirá quais ações serão prioritárias. Essa combinação é feita com um cálculo de multiplicação dos três fatores (G) x (U) x (T).

GRAVIDADE

É o impacto que o problema gerará nos envolvidos, podendo ser os colaboradores, os processos, tarefas, resultados da empresa etc. A análise é feita nos efeitos que o problema, caso não seja resolvido, acarretará em médio e longo prazo.

URGÊNCIA

É o prazo, ou o tempo disponível para a resolução do problema. Quanto menor o tempo, mais urgente será o problema que deverá ser resolvido. O recomendado é fazer a pergunta: Isso pode esperar?

TENDÊNCIA

É a probabilidade (ou o potencial) que o problema tem de crescer com o passar do tempo. A pergunta a ser feita é: Se eu não resolver isso hoje, o problema vai piorar aos poucos ou bruscamente?

Kiko Fernandes
Coaching e Mentoria

https://www.effettivo.com.br/category/blog/

Priorização dos Riscos

Matriz GUT

VALOR	G GRAVIDADE	U URGÊNCIA	T TENDÊNCIA	PONTUAÇÃO GxUxT
5	Prejuízos extrememanente graves	Não tem pressa	Agravamento imediato	
4	Muito grave	Agir com alguma urgência	Vai piorar rapidámente	
3	Grave	Agir o mais cedo possível	Vai piorar no médio prazo	
2	Pouco grave	Pode esperar um pouco	No longo prazo tende a piorar	
1	Sem gravidade	Não tem pressa	Não vai piorar	

Priorização dos Riscos

Matriz GUT

RISCOS VULNERABILIDADES	G GRAVIDADE	U URGÊNCIA	T TENDÊNCIA	PONTUAÇÃO GxUxT
Faltam Políticas, Requisitos de Segurança e um sistema SGSI				
Barreira Física 1: Falta controle de acesso na Portaria				
Barreira Física 2: Falta controle de circulação interna				
Barreira Física 3: Falta controle de dos discos rígidos HDs				
Barreira Virtual: Falta controle das Senhas Pessoais				
Falta Rotina de Auditoria de Segurança da Informação				
Outros				

4 - Planejamento do Tratamento de Risco

Para os riscos identificados e priorizados a organização precisa determinar **quais riscos serão aceitos, e quais não serão.**

"**Riscos podem ser aceitos**: se, por exemplo, for avaliado que o risco é baixo, ou que o custo do tratamento não é economicamente viável para a organização";

É importante que ações sejam devidamente definidas e registradas para cada risco previamente identificado.

ABNT (2005, p. 6),

4 - Planejamento do tratamento de risco

Tipos de Tratamentos que podem ser dados aos riscos:

- **aplicar controles** apropriados para mitigar e reduzir os riscos;
- **evitar riscos**, não permitindo ações que poderiam causar a ocorrência de riscos;
- **transferir os riscos** associados para outras partes, por exemplo, seguradoras ou fornecedores

ABNT, 2005, p. 6

TEMA 1 Gestão de Riscos

Opções para Tratamento De Risco

Manual de Riscos do INPI (2018), :

- **Aceitar (ou tolerar)**: a organização decide, deliberadamente, não tomar nenhuma medida em relação ao risco. A sua **probabilidade e impacto são tão baixos** que não justificam a criação de controles para mitigação (o custo de tomar uma ação pode ser desproporcional ao benefício potencial gerado), ou os controles existentes já resguardam boa parte de suas consequências. Ocorre quando o risco está dentro do limite de exposição a risco da organização. Esta opção pode ser suplementada por um **plano de contingência** – é um plano de ação para conter/minimizar os impactos (consequências) que adviriam caso a ameaça acorra.
- **Mitigar (ou reduzir):** Mitigar um risco é provavelmente a técnica de gerenciamento de riscos mais utilizada. Também é a mais fácil de compreender e de implementar. Mitigar significa atuar para **reduzir a probabilidade e/ou impacto do risco,** de modo que mesmo que ele ocorra, o problema gerado é menor e mais fácil de corrigir. Significa restringi-los a um determinado nível aceitável, tornando-o menor ou mesmo removendo-o da lista dos principais riscos. Exemplo: Redundância de recursos.

https://www.gov.br/inpi/pt-br/governanca/integridade-publica/arquivos/documentos/manualdegestoderiscosv2-0_gequgrimn0001_aprovado.pdf

TEMA 1 Gestão de Riscos

Opções para Tratamento De Risco

Manual de Riscos do INPI (2018), :

- **Transferir (ou compartilhar):** transferência é uma opção de gerenciamento de risco que não é utilizada muito frequentemente, e tende a ser mais comum em projetos onde há várias partes. É o caso especial de se reduzir a consequência e/ou probabilidade de ocorrência do risco por meio da **transferência ou compartilhamento de uma parte do risco.** Isso pode ser feito através de **contratação de seguros** ou de cláusulas específicas e **garantias em contratos**, ou, ainda, através da **terceirização de atividades** das quais a organização não tem suficiente domínio. É importante notar que alguns riscos não são totalmente transferíveis, como, por exemplo, transferir risco de reputação e imagem, mesmo se a entrega dos serviços foi contratada para um terceiro.
- **Evitar (ou eliminar):** significa alterar ou reduzir escopos/requisitos, ou não iniciar ou **descontinuar atividades/processos** para eliminar o objeto sujeito ao risco, eliminando a ameaça na origem. Exemplo: cancelar o projeto.

https://www.gov.br/inpi/pt-br/governanca/integridade-publica/arquivos/documentos/manualdegestoderiscosv2-0_gequgrimn0001_aprovado.pdf

5 - Implementação do controle do risco

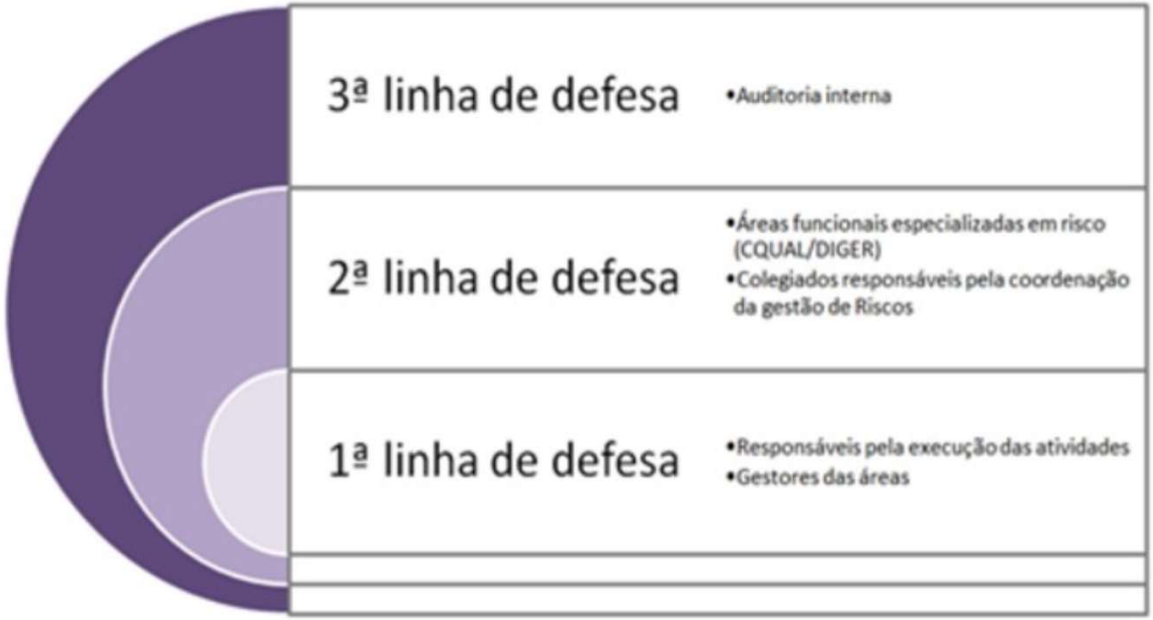
Controle de Riscos constitui:

“uma forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal”.

Em outras palavras, a implementação do controle de riscos significa **“executar o que foi planejado para tratar os riscos identificados”**

5 - Implementação do controle do risco

Monitoramento de Riscos - Três Linhas de Defesa



Modelo das Três Linhas de Defesa separa:
Primeira linha: responsabilidades administrativas de gestão de riscos, formada pelos gestores das unidades;
Segunda Linha: o papel de outras funções no apoio e supervisão do gerenciamento de riscos, formada pelas áreas funcionais especializadas em risco;
Terceira Linha: papel da auditoria interna em prestar avaliação objetiva.

https://www.gov.br/inpi/pt-br/governanca/integridade-publica/arquivos/documentos/manualdegestoderiscosv2-0_gequgrimn0001_aprovado.pdf

6 - Avaliação e Revisão dos Riscos

Essa etapa final agrega um **caráter cíclico ao processo**, uma vez que os riscos podem sofrer mudanças a todo o momento.

Quando isso ocorre, todo o planejamento em torno de sua análise, tratamento e controles precisa ser revisado e, quando necessário, ajustado para que se mantenha em conformidade com a realidade da organização.

Gestão de Riscos

CICLO PDCA

TEMA 1 Gestão de Riscos

O CICLO DA GESTÃO DE RISCOS

O processo de gestão de riscos deve reproduzir o cíclo de melhoria contínua, composto por quatro etapas, que se sucedem:

- ✓**Plan (Planeja)**
- ✓**Do (Executa)**
- ✓**Check (Controla)**
- ✓**Act (Atua)**

Cada etapa tem sua própria forma de gerenciamento e execução, mas todas convergem para um objetivo em comum:

Garantir a segurança
e a disponibilidade dos ativos.

TEMA 2 Análise de Vulnerabilidades

Vulnerabilidade

São definidas como fragilidades de um ativo ou grupo de ativos que podem ser exploradas por uma ou mais ameaças

ABNT, 2005, p. 3

Dessa definição, entende-se que vulnerabilidades podem ser identificadas nos diferentes setores, departamentos e instalações de uma organização;

Duas seções de controles de segurança diretamente suscetíveis a apresentar vulnerabilidades são:

Segurança Física e o Ambiente e o Controle de Acesso.

,

TEMA 2 Análise de Vulnerabilidades

Vulnerabilidade

Instalações e todo ambiente que pode representar algum risco de segurança para a organização devem ser contemplados na análise de vulnerabilidades, de forma a “prevenir o acesso físico não autorizado, danos e interferência com as instalações e informações da organização”

ABNT, 2005, p. 32

TEMA 2 Análise de Vulnerabilidades

Vulnerabilidade

Informação corporativa associada à computação em nuvem, exige que a segurança passe a se concentrar na informação;

É necessário aplicar controles diferenciados para as informações:

a utilização de soluções de criptografias,
controle de acesso e critérios rigorosos de compartilhamento;

A área de segurança da informação deve assegurar:

a confidencialidade, integridade, disponibilidade,
e rastreabilidade das informações estratégicas para o negócio.

Busca de Fragilidades no acesso à informação

Uma análise de vulnerabilidades deve ser feita de forma análoga considerando os controles de acesso.

O objetivo é garantir que:

"o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação"

ABNT, 2005, p. 65

TEMA 2 Análise de Vulnerabilidades

Varredura de Fragilidades - deve considerar:

- **perímetro de segurança física**: avaliar áreas que contenham informações e instalações de processamento da informação;
- **controles de entrada física:** verificar se as áreas seguras oferecem controles para garantir que apenas pessoas autorizadas tenham acesso;
- **segurança em escritórios**, **salas e instalações:** conferir a existência de controles de segurança físicos nesses ambientes;
- **proteção contra ameaças externas e do meio ambiente**: avaliar a existência de proteção contra eventos naturais ou incidentes no perímetro (vazamentos, explosões etc.);
- **acesso ao público e a áreas de carregamento**: garantir o controle de acesso nesses espaços;
- **segurança de equipamentos**: avaliar o estado de utilidades e cabeamentos, além de verificar a segurança da utilização dos mesmos fora da organização.

TEMA 2 Análise de Vulnerabilidades

Busca de Fragilidades no acesso à informação - Procedimentos:

- **política de controle de acesso**: fazer a conferência crítica da documentação existente;
- **gerenciamento de acesso do usuário**: analisar a existência de procedimentos formais para o controle e a distribuição de direitos de acesso a sistemas da informação;
- **responsabilidade dos usuários**: avaliar as políticas preparadas para garantir que os usuários estejam conscientes de suas responsabilidades em relação ao uso de senhas e de segurança dos equipamentos;
- **controle de acesso aos recursos e sistemas computacionais:** verificar os procedimentos relacionados à computação móvel, trabalho remoto, acesso a aplicações e sistemas operacionais e à rede.

TEMA 2 Análise de Vulnerabilidades

O fator humano como uma vulnerabilidade em segurança da informação

Comentário:
Entre as possíveis vulnerabilidades relacionadas à segurança da informação que estão presentes em um ambiente organizacional, técnicas, físicas e humanas, a literatura destaca o fator humano como o elemento mais fraco e mais importante na gestão de segurança da informação. Não é possível a criação de barreiras ou ferramentas que protejam o componente humano, da mesma forma que estas são criadas para os componentes técnicos e físicos.
Este artigo tem por objetivo realizar uma análise descritiva das vulnerabilidades ocasionadas pelas ações humanas em um ambiente organizacional a partir da percepção do usuário e da equipe de suporte a TI, com o foco nas ameaças e incidentes causados pelo fator humano.

Disponível em:
http://www.sustenere.co/index.php/rbadm/article/view/SPC2179-684X.2017.003.0012/1259

TEMA 3 Medidas de Proteção

Medidade de proteção a serem adotadas:

Diferentes medidas de proteção podem ser propostas e adotadas de acordo com as especificidades dos processos de cada organização;

É necessário priorizar as áreas cujas vulnerabilidades têm maior potencial de ocorrer uma invasão;

A segurança física e do ambiente e o controle de acesso merecem receber o foco de atenção quanto à implementação de medidas para a garantia da segurança.

TEMA 3 Medidas de Proteção

Segurança física e do ambiente:

definição clara dos **limites do perímetro de segurança** e a **eliminação de brechas** estruturais que poderiam viabilizar uma invasão;

Sistemas de detecção de intrusos e a construção de barreiras físicas:

para a contenção de acessos não autorizados também são recomendados;

TEMA 3 Medidas de Proteção

Controle de entradas físicas:

registros da data e hora de entrada e saídas possibilitam que os visitantes sejam supervisionados.

Acesso identificado:

exigência de que todos os funcionários, fornecedores e terceiros, todos os visitantes, e mesmo alguma atividade de carga e descarga, tenham alguma forma de identificação visível, com o objetivo de impedir que intrusos se aproveitem de situações que podem camuflar o acesso indevido.

TEMA 3 Medidas de Proteção

Medidas de proteção relativas ao controle de acesso:

podem variar de medidas simples a soluções tecnologicamente elaboradas.

Nesse sentido, a segregação de funções de controle de acesso e a utilização de identificadores de usuários (ID de usuário) podem proporcionar que o gerenciamento de acesso seja efetuado de maneira mais segura e simples.

Conscientizar e auditar a confidencialidade das senhas:

utilizadas pelos usuários. Isso permitirá que o acesso aos ativos computacionais da organização (rede, sistemas operacionais, aplicações e acesso remoto) esteja alinhado com os requisitos de segurança previamente estabelecidos.

TEMA 3 Medidas de Proteção

Mapeamento de processos: conceitos, técnicas e ferramentas

Autores: Egon Walter Wildauer e Laila Del Bem Seleme Wildauer
Editora: InterSaberes
Ano: 2015

Comentário:
no livro indicado, apresenta-se, de forma simples e direta, uma temática fundamental no mundo das organizações: o mapeamento de processos. São fornecidas bases para nortear o entendimento do tema pelo leitor. Além disso, são apresentados casos práticos que fornecem um aprofundamento acerca do mapeamento. Recomenda-se, em particular, a leitura dos **Capítulos 1 e 2.**

Disponível na Biblioteca Virtual.

Inventário dos Ativos de TI:

È o ponto de partida da gestão da segurança dos ativos de TI.

Qualquer que seja o tipo de ativo de uma organização, esse deve constar no inventário.

Esse instrumento possibilita que a organização tenha uma visão ampla do seu parque tecnológico

O mapeamento correto dos ativos e responsáveis exige que haja um inventário preliminarmente, com todos os ativos que forem relevantes para a organização.

TEMA 4 Segurança em Ativos de TI

Ativos de TI incluem:

- **ativos de informação:** base de dados, arquivos, contratos e acordos, documentação de sistemas, manuais de usuários, material de treinamento, planos de continuidade do negócio etc.;
- **ativos de *software***: aplicativos, sistemas, ferramentas de desenvolvimento;
- **ativos físicos:** equipamentos computacionais, equipamentos de construção, mídias removíveis etc.;
- **serviços:** serviços de computação e comunicações, utilidades gerais como iluminação, refrigeração etc.;
- **pessoas** e suas qualificações, habilidades e experiências;
- **intangíveis**, tais como a reputação e a imagem da organização

ABNT, 2005, p. 21

Segurança em Ativos de TI: Os responsáveis por cada ativo

Está intrinsecamente relacionada com a forma de gestão desses ativos.

A segurança nesse contexto se inicia pela definição e formalização de quem são os **responsáveis por cada ativo**.

“Convém que **todas as informações e ativos** associados com os recursos de processamento da informação tenham um **proprietário designado** por parte da organização”

ABNT, 2005, p. 22

Segurança em Ativos de TI: Regras de utilização dos ativos

Adicionalmente à definição dos responsáveis por cada ativo, é recomendável a formalização do que representa o uso aceitável de cada um deles:

Deve ser claro, para cada funcionário, fornecedor e terceiros, quais são as regras de uso de cada ativo.

Convém que sejam incluídas normas documentadas de uso da internet e do correio eletrônico, além de diretrizes regulando o uso de dispositivos móveis dentro e fora das instalações da organização.

Segurança em Ativos de TI: Classificação das informações

A gestão dos ativos de TI, na segurança da informação, tende a ser uma realidade apenas em organizações de grande porte.

Mas micro/pequenas empresas precisam dar atenção a essa atividade.

A definições das normas de uso, e atribuição de responsáveis, requer também a **classificação da informação**, a fim de receber a forma adequada de proteção.

A classificação é determinada pela:

sensibilidade, valor, requisitos legais e pela importância para a organização.

A classificação deve estar de acordo com a forma como o ativo é utilizado no negócio.

TEMA 4
Segurança em Ativos de TI

Classificação das informações: como definir níveis de segurança?

A Lei Geral de Proteção de Dados LGPD

Em seu Artigo 46 determina a adoção de medidas para proteger os dados pessoais de acessos não autorizados, conforme descrito abaixo:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Como se adequar à LGPD e evitar sanções?

No espaço deste artigo, não conseguimos trazer todos os pontos de adequação que sua empresa deve tomar, mas o primeiro passo, sem dúvidas, é proceder a uma classificação das informações e dados sensíveis à LGPD.

https://alleasy.com.br/classificacao-de-informacoes/#:~:text=A%20classifica%C3%A7%C3%A3o%20da%20informa%C3%A7%C3%A3o%20faz,requisitos%20legais%2C%20criticidade%20e%20sensibilidade.

TEMA 4
Segurança em Ativos de TI

Classificação das informações: como definir níveis de segurança?

O que é classificação das informações?

Esse processo trata-se de uma prática relativamente antiga que servia sobretudo para governos e empresas protegerem informações consideradas essenciais.

A Classificação das Informações inicia por um bom **"mapeamento de dados (data mapping)",** em que deve-se encontrar os dados sensíveis à LGPD e descobrir quais usuários têm acessos a esses dados, qual o nível de permissionamento e quem realmente os está acessando.

Em tempos de troca de dados de maneira instantânea e com o armazenamento de volume de informações cada vez maiores, essa prática se torna ainda mais importante e, fazer a classificação das informações, é um dos passos da segurança da informação mais importantes que sua empresa precisa tomar, seja ela grande, seja ela pequena.

Mas, afinal, o que significa fazer a classificação das informações e como isso pode ajudar na segurança dos dados? Quais são as principais recomendações e como começar? Prossiga a leitura para entender!https://alleasy.com.br/classificacao-de-informacoes/#:~:text=A%20classifica%C3%A7%C3%A3o%20da%20informa%C3%A7%C3%A3o%20faz,requisitos%20legais%2C%20criticidade%20e%20sensibilidade.

TEMA 5 Sistemas de Gestão da Segurança da Informação

Sistema de Gestão da Segurança da Informação SGSI

A adoção de um SGSI é uma decisão estratégica para a organização, tendo em vista o seu impacto nos processos de trabalho e no modelo de negócio;

A gestão de riscos é uma atividade com **caráter cíclico.** Isso quer dizer que todas as suas etapas devem ser continuamente executadas de forma a promover um gerenciamento efetivo e eficaz

Em função disso, sua implantação deve ser executada nos moldes do modelo de melhoria contínua **PDCA *Plan-Do-Check-Act*, ou Planejar-Fazer-Verificar-Agir**.

https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html#:~:text=O%20que%20%C3%A9%20um%20Sistema,de%20Confidencialidade%2C%20Integridade%20e%20Disponibilidade.

TEMA 5 Sistemas de Gestão da Segurança da Informação

Ciclo PDCA de implantação de um SGSI

TEMA 5 Sistemas de Gestão da Segurança da Informação

1ª Etapa: Estabelecer (Plan) o SGSI

Definição do escopo e os limites do sistema, considerando:

as características do negócio, a organização,
suas expectativas, sua localização, ativos e tecnologia.

O planejamento da gestão de riscos no SGSI, deve identificar quais riscos pertencem ao escopo do sistema, e proceder com a:

análise, avaliação, proposição de tratamento,
seleção de controles e objetivos a serem alcançados

ABNT, 2006

TEMA 5 Sistemas de Gestão da Segurança da Informação

1ª Etapa: Estabelecer (Plan) o SGSI

- Definir o escopo (abrangência) do SGSI;
- Definir uma Política de SGSI;
- Definir uma metodologia para identificação, análise e avaliação de riscos, bem como a definição de opções de tratamento desses riscos;
- Selecionar objetivos de controle e quais controles serão utilizados para tratar os riscos;
- Obter aprovação da direção dos riscos residuais propostos, bem como da autorização para implementar e operar o SGSI;
- Preparar a Declaração de Aplicabilidade.

TEMA 5 Sistemas de Gestão da Segurança da Informação

2ª Etapa: Implementar e Operar (Do) o SGSI

É recomendável que a organização implemente:

uma política de gerenciamento de operações e de recursos do sistema;
programas de conscientização;
treinamento;
e ponha em prática:

"procedimentos e controles capazes de permitir a pronta detecção de eventos de segurança da informação e resposta a incidentes de segurança da informação"

ABNT, 2006

TEMA 5 Sistemas de Gestão da Segurança da Informação

2ª Etapa: Implementar e Operar (Do) o SGSI

- Elaborar e implementar um plano de tratamento de riscos;
- Implementar controles selecionados para atender aos objetivos de controle;
- Definir a medição da eficácia dos controles;
- Implementar programas de conscientização e treinamento;
- Gerenciar operações e recursos para o SGSI;
- Implementar procedimentos e outros controles para detectar e responder prontamente a incidentes de segurança da informação.

TEMA 5 Sistemas de Gestão da Segurança da Informação

3ª Etapa : Monitoramento e Verificação (Check) do SGSI

A organização deve executar verificações regulares:

avaliando a eficácia do sistema; o atendimento da política e dos objetivos do SGSI; e a análise crítica de controles de segurança;

Deve, ainda, considerar os resultados de auditorias de segurança da informação, os incidentes de segurança e as sugestões.

TEMA 5 Sistemas de Gestão da Segurança da Informação

3ª Etapa : Monitoramento e Verificação (Check) do SGSI

- Realizar regularmente análises críticas da eficácia do SGSI;
- Medir a eficácia dos controles;
- Realizar análise crítica periódica das avaliações de riscos para verificar e considerar mudanças ocorridas;
- Realizar auditorias internas periódicas do SGSI;
- Realizar periodicamente a análise crítica do SGSI pela direção;
- Atualizar planos de segurança;
- Registrar eventos e ações que possam impactar na eficácia ou no desempenho do SGSI.

4ª Etapa: Manter e Melhor (*Act*) oo SGSI

Finaliza um ciclo e gera os subsídios para um novo ciclo:

Nesse último passo deve ser realizada uma **revisão de todo o ciclo de gestão de riscos,** buscando identificar a efetividade do SGSI e a necessidades de melhorias;

As **melhorias identificadas devem ser implementadas**, erros e falhas, corrigidos, e lições aprendidas registradas.

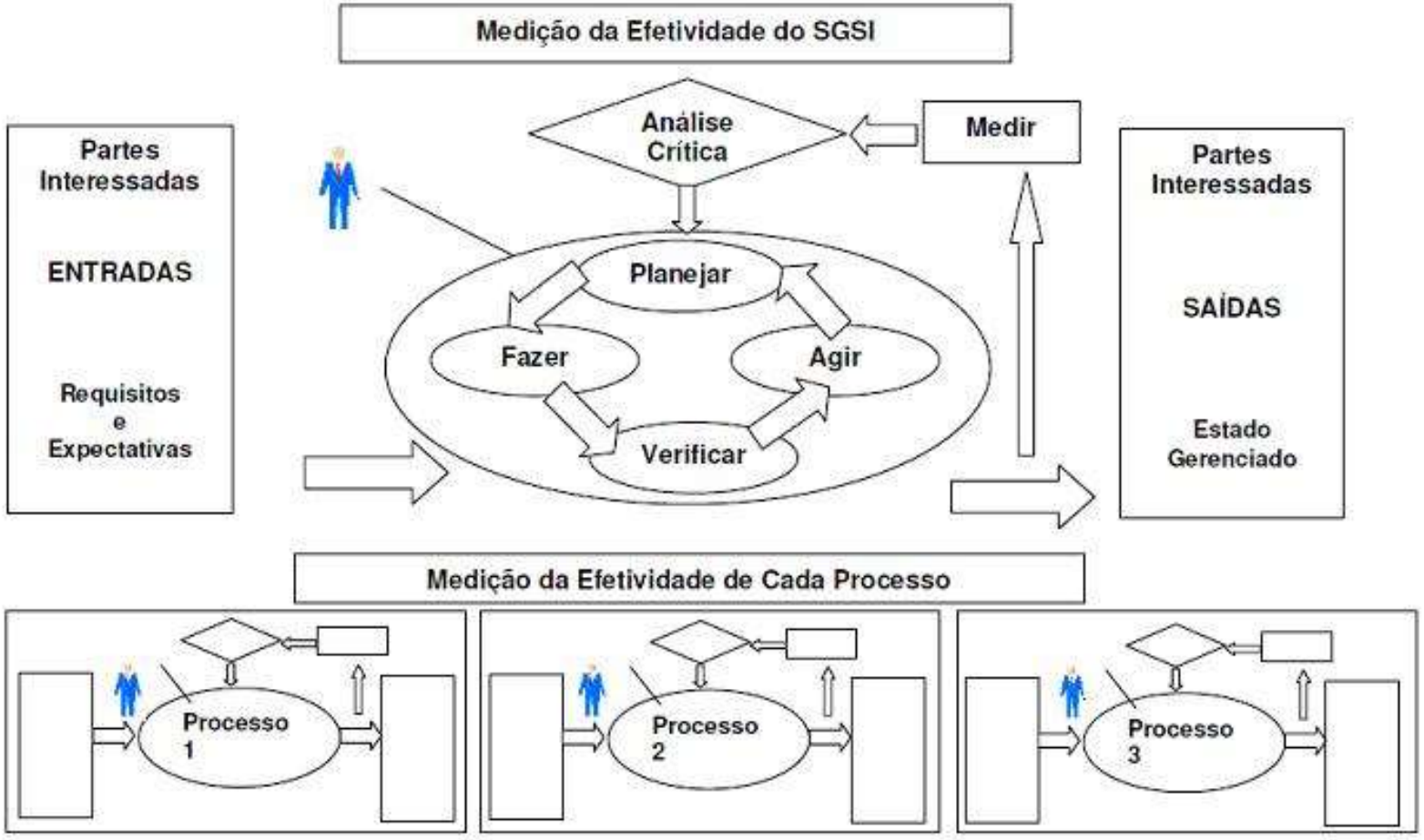
TEMA 5 Sistemas de Gestão da Segurança da Informação

4ª Etapa: Manter e Melhor (*Act*) o SGSI

- Implementar melhorias identificadas no SGSI;
- Executar ações preventivas e corretivas aplicando-se as lições aprendidas;
- Comunicar ações e melhorias para as partes interessadas;
- Garantir que as melhorias realmente estejam atingindo os objetivos pretendidos.

Sistema de Gestão da Segurança da Informação SGSI

4ª Etapa: Manter e Melhor (*Act*) o SGSI



Sistema de Gestão da Segurança da Informação SGSI

Plano de Ação

Sistema de Gestão da Segurança da Informação SGSI

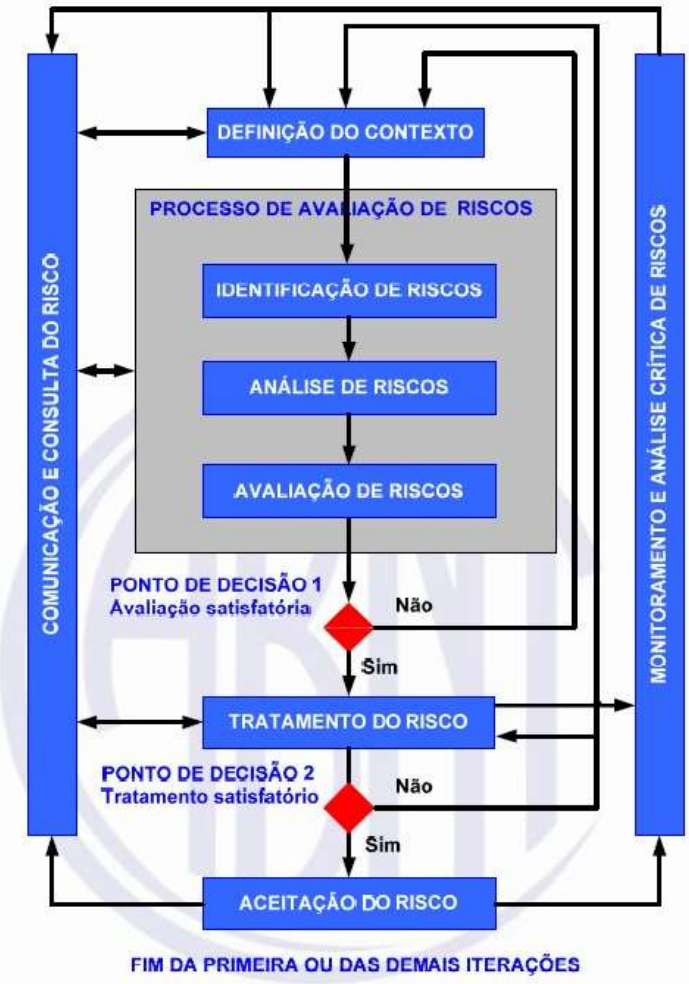
4ª Etapa: Manter e Melhor (*Act*) o SGSI

http://www.arrudaconsult.com.br/2020/03/analise-de-risco-tecnica-bow-tie.html

Sistema de Gestão da Segurança da Informação SGSI

Processo de Gestão de Riscos Segurança da Informação NBR ISO 31000

A ISO 31000 recomenda que o Processo de Gestão de Riscos (PGR) seja integrado na estrutura, operações e processos da organização, e que seja parte integrante da gestão do negócio e da tomada de decisão, podendo ser aplicado nos níveis estratégico, operacional, de programas e de projetos. Recomenda também que a natureza dinâmica e variável do comportamento humano seja considerada ao longo de todo o Processo de Gestão de Riscos.



Processo de gestão de riscos de segurança da informação

https://administradores.com.br/artigos/processo-de-gestao-de-riscos-iso-31000

Sistema de Gestão da Segurança da Informação SGSI

ABNT NBR ISO 31000
Gestão de riscos — Princípios e diretrizes

Embora todas as organizações gerenciem os riscos em algum grau, esta Norma estabelece um número de princípios que precisam ser atendidos para tornar a gestão de riscos eficaz.

Esta Norma recomenda que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura1) cuja finalidade é integrar o processo para gerenciar riscos na governança, estratégia e planejamento, gestão, processos de reportar dados e resultados, políticas, valores e cultura em toda a organização.

A gestão de riscos pode ser aplicada a toda uma organização, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos.

https://edisciplinas.usp.br/pluginfile.php/4656830/mod_resource/content/1/ISO31000.pdf

TEMA 5 Sistemas de Gestão da Segurança da Informação

Sistema de Gestão da Segurança da Informação SGSI

Em todas as etapas do processo PDCA de implantação de um SGSI, o **comprometimento da direção** é crucial.

A institucionalização de todos os procedimentos e políticas é de responsabilidade da direção, que precisa, além disso, garantir que recursos suficientes sejam alocados para a subsidiação de todo o processo.

A aderência, ou não, do corpo funcional da organização ao correto uso e manutenção do SGSI tem relação direta com o pleno envolvimento da direção.

TEMA 5 Sistemas de Gestão da Segurança da Informação

Sistema de Gestão da Segurança da Informação SGSI

A implantação e a operacionalização de um ***software* de Gestão da Segurança da Informação** exige o **alinhamento das funcionalidades do *software*** com os requisitos de segurança da organização:

- **Elaborar um planejamento** para o tratamento de cada risco no qual as ações correspondentes devem ser definidas e priorizadas;
- **Implementar o plano de tratamento de riscos** para alcançar os objetivos identificados, incluindo questões sobre financiamento e atribuição de papéis e responsabilidades;
- **Selecionar os objetivos de controle** para o tratamento dos riscos, a fim de atender aos requisitos identificados pela análise e avaliação de riscos;
- **Aplicar critérios de aceitação** previamente definidos, a fim de selecionar quais riscos serão aceitáveis e quais deverão receber algum tratamento.

TEMA 5 Sistemas de Gestão da Segurança da Informação

ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação (SGSI)

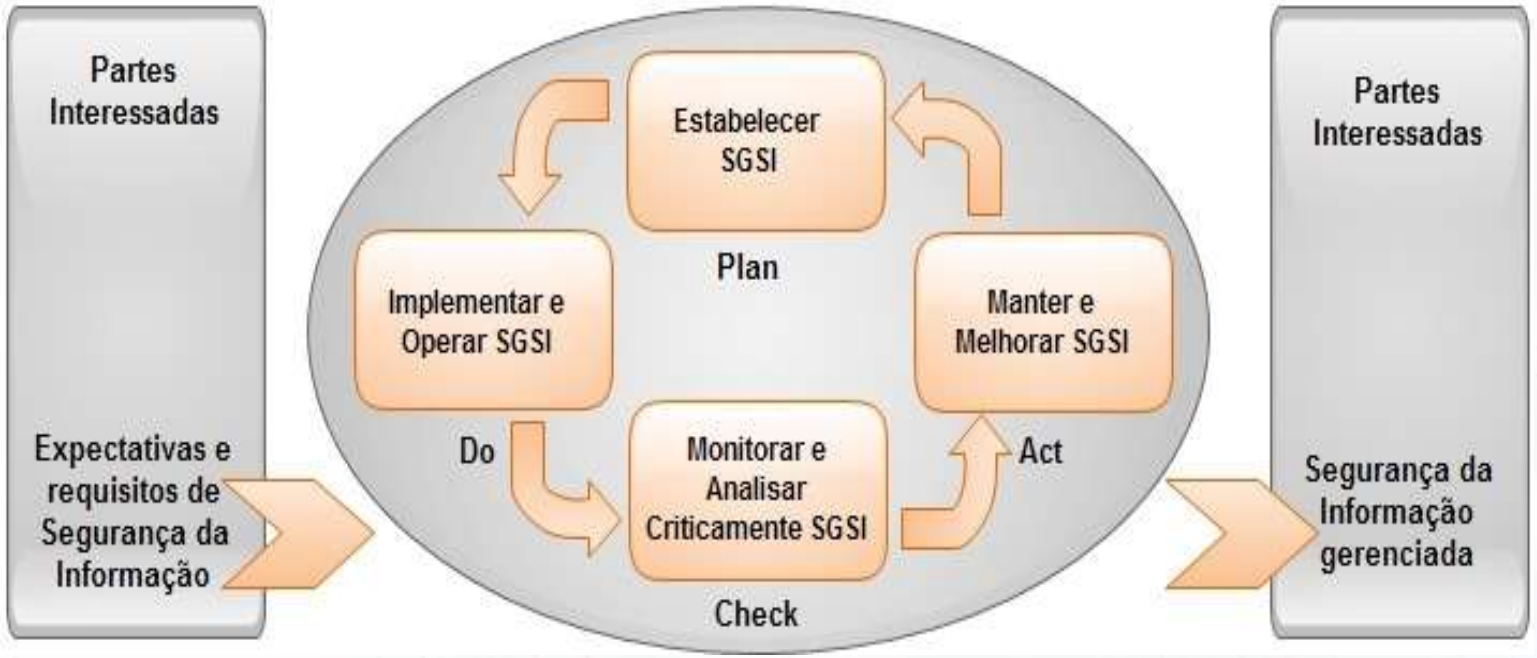
Comentário:
Esta Norma prove um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).
A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização.
É esperado que este e os sistemas de apoio mudem com o passar do tempo. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples.
Esta Norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas
Disponível em:
https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001-20060331Ed1.pdf

SGSI

Norma ISO/IEC 27001

ABNT NBR ISO/IEC 27001 Sistema de Gestão de Segurança da Informação (SGSI)

A **Norma adota o ciclo PDCA (*Plan, Do, Check, Act*)** de melhoria contínua para estruturar todos os processos envolvidos em um Sistema de Gestão de Segurança da Informação SGSI.



TEMA 5 Sistemas de Gestão da Segurança da Informação

Sistemas de segurança da informação na era do conhecimento

Autor: Armando Kolbe Júnior
Editora: InterSaberes
Ano: 2017

Comentário: por se tratar de uma área estratégica para a organização, a segurança da informação não raro é relevante para a tomada de decisões gerenciais. Aplicar a segurança da informação nesse contexto, porém requer que os sistemas de gestão sejam preparados para manipular as informações de modo apropriado.
No **capítulo 5** desse livro, conheça algumas diretrizes de preparação de um SGSI para que possa apoiar a tomada de decisões.

Disponível na Biblioteca Virtual.

TEMA 5 Sistemas de Gestão da Segurança da Informação

INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O objetivo deste texto é apresentar uma introdução conceitual à gestão da segurança, com base na gestão de riscos de segurança da informação.
O texto apresenta algumas orientações para a introdução da gestão de riscos nas organizações, baseadas na Norma AS-NZS 4360 (Standards Australia and Standards New Zealand, 2004), da qual deriva a ISO/IEC 31000 (ISO/IEC, 2009).
O texto foi produzido para suporte às atividades do CEGSIC 2009-2011, a partir de aprimoramento de material previamente desenvolvido em versões anteriores do CEGSIC (TRF JUS).

Desenvolvido em atendimento ao plano de trabalho do Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC 2009-2011.

https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf

TEMA 5 Sistemas de Gestão da Segurança da Informação

ISO 27001 & ISO 27002

ISO 27001

É a norma internacional que define os Requisitos para Sistemas de Gestão de Segurança da Informação. Ela ajuda a empresa a adotar um sistema de gestão da segurança da Informação que permita mitigar os riscos de segurança atribuídos a seus ativos e adequar as necessidades a área de negócio.

ISO 27002

Fornece um conjunto de Controles baseados em melhores práticas para a Segurança da Informação.

É recomendável que a ISO 27001 seja utilizada em conjunto com a 27002 , que é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação , facilitando atingir os requisitos especificados pela Norma ISO 27001.

https://www.portalgsti.com.br/2011/05/iso-27001-e-iso-27002.html

TEMA 5 Sistemas de Gestão da Segurança da Informação

Webinar - Lançamento Norma ISO 27002: 2022
- O que tem de novo na Segurança da Informação?

https://www.youtube.com/watch?v=5AMG8TRgDvE

SÍNTESE

Exploramos as orientações de segurança aplicadas a diferentes áreas de uma organização;

Dois setores são críticos para a garantia da segurança da informação:

a segurança física e do ambiente e o controle de acesso.

São duas áreas que demandam muito esforço e investimento para impedir que suas vulnerabilidades se convertam em ameaças para a organização.

Analisamos as formas como as normas viabilizam uma adoção gradativa de suas práticas, que orienta a implantação de um *software* de gestão de segurança da informação.

TRANSIÇÃO DE TEMA

DÚVIDAS...

DISCUSSÃO DO CASO

Introdução

Olá Estudante!
A proposta de estudo de caso apresenta uma organização fictícia cuja estrutura pode ser encontrada, atualmente, em diversas empresas:

A realidade dessa organização, em termos de segurança da informação, apresenta **várias vulnerabilidades de diferentes criticidades**.

Embora algumas medidas de segurança já tenham sido implementadas pela organização, elas se mostram inadequadas ou insuficientes.

Dentro desse cenário, um
incidente de violação de segurança grave é reportado.

Ciente da pouca maturidade e comprometimento da organização com a segurança da informação, a gerência propõe a **aquisição imediata de um sistema d**e gestão da segurança da informação, para sanar as deficiências.

Nesse contexto, a equipe gestora da segurança da informação precisa se posicionar, a favor ou contra a iniciativa da gerência, com argumentos pautados nas normas de segurança ISO.

DISCUSSÃO DO CASO

Problematização

Empresa Gênesis Tecnologia
Responsável pela manutenção e instalação
do hardware e software das urnas eletrônicas

A Empresa:

A estrutura física da Genêsis é muito parecida com qualquer empresa da área;

Todas as dependências da empresa são monitorasa por câmeras de segurança e na portaria, vigias exigem a identificação de todos que acessam as dependências da empresa;

Apesar dessa orientação á medida que vão conhecendo os funcionários a identificação por meio de crachá costuma ser desconsiderada;

O saguão principal da empresa contem diversas bancadas onde as urnas eletrônicas são montadas e desmontadas para manutenção e atualização;

Vários componentes das urnas também ficam expostos nessas bancadas;

DISCUSSÃO DO CASO

Problematização

Empresa Gênesis Tecnologia
Responsável pela manutenção e instalação
do hardware e software das urnas eletrônicas

A Empresa:

A partir do sagão principal é possível ter acesso aos outros departamentos da empresa: setores de desenvolvimento de sistemas, de banco de dados, redes de computadores, e o departamento específico para os componentes eletrônicos das urnas;

Todas as urnas contem uma cópia das informações sigilosas dos eleitores e dados relativos à segurança da eleição;

Todas essas informações são mantidas no disco rígido HD da urna e a única maneira de ter acesso á essas informações é via senha pessoal, que é gerada para cada funcionário da empresa;

Porém, como o acesso às informações contidas na urna é feita diariamente, uma prática adotada por eles é de manter a senha pessoal adotada em um pequeno papel que é fixado ao lado do monitor;

É comum também que um funcionário empreste sua senha pessoal para outro funcionário;

DISCUSSÃO DO CASO

Problematização

Empresa Gênesis Tecnologia
Responsável pela manutenção e instalação
do hardware e software das urnas eletrônicas

O Incidente:

Em um dia normal de trabalho um dos funcionários que atua diretamente com os componentes eletrônicos das urns detetou o desaparecimento de um dos discos rígidos contendo informações críticas e sigilosas;

Esse incidente foi reportado à equipe gestora da segurança da informação;

Durante o processo de apuração do ocorrido as câmeras mostraram que uma pessoa não identificada passou pela portaria no meio de 4 funcionários, que já eram muito conhecidos;

A pessoa teve acesso ao saguão principal de onde ela conseguiu levar um disco rígido das urnas que estava exposto em uma bancada e como um departamento estava vazio naquele instante ela acabou levando uma das senhas que ficava fixada nos monitores dos funcionários;

Colocando tudo dentro da mochila ele saiu naturalmente pela portaria.

DISCUSSÃO DO CASO

Problematização

Empresa Gênesis Tecnologia
Responsável pela manutenção e instalação
do hardware e software das urnas eletrônicas

A Equipe Gestora da Segurança de Informação:

Passou imediatamente a trabalhar em um plano de mitigação do incidente;

Todas as ações foram baseadas em diretrizes da Norma ISO 27.001;

A Direção da Empresa:

Ao tomar conhecimento do incidente a direção da empresa entendeu que eles estavam com graves deficiências quanto à segurança da informação, por isso, sugeriu a aquisição imediata de um software para gestão da segurança da informação;

DISCUSSÃO DO CASO

Problematização

Empresa Gênesis Tecnologia
Responsável pela manutenção e instalação
do hardware e software das urnas eletrônicas

Você, como membro
da Equipe de Gestão da Segurança da Informação:

Numa situação assim, que argumentos, baseado nas normas de segurança da informação, apresentaria para se posicionar a favor, ou contra, a iniciativa da direção?

PROBLEMATIZAÇÃO

DISCUSSÃO DO CASO

Dica 01:
Autenticação e Autorização

Nenhuma ferramenta de gestão da segurança da informação consegue promover benefícios concretos para uma organização quando não há um efetivo controle de acessos à informação.

Que medidas podem ser adotadas, para garantir que as informações estejam disponíveis apenas para quem está autorizado a acessá-las?

PROBLEMATIZAÇÃO

DISCUSSÃO DO CASO

Dica 02:
Requisitos e Políticas de Segurança

A introdução de um *software* de gestão em uma empresa precisa ser considerada a implementação de uma estratégia que visa ao atendimento de uma demanda real.

Logo, a definição daquilo que realmente precisa ser gerido e de como se dará essa gestão são cruciais para o bom funcionamento do *software*.

Que definições precisam ser feitas, para que o estabelecimento de um *software* de gestão de segurança possa estar alinhado com as necessidades de uma empresa?

PROBLEMATIZAÇÃO

DISCUSSÃO DO CASO

Dica 03:
O Comprometimento de Todos com a Segurança

A gestão da segurança da informação é uma atividade que exige o envolvimento de todos os setores da organização, o que inclui a alta gerência.

O processo de adoção de um *software* para apoiar essa gestão não é diferente.

Explique de quais formas a direção pode manifestar comprometimento com um ciclo de gestão da segurança da informação suportado por software?

DISCUSSÃO DO CASO

DICAS

Dica 04: Pesquisa Bibliográfica

O fator humano como uma vulnerabilidade em segurança da informação
https://www.researchgate.net/publication/334406978_O_fator_humano_como_uma_vulnerabilidade_em_seguranca_da_informacao

Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa
https://periodicos.unifacef.com.br/index.php/resiget/article/view/1065

IMPORTÂNCIA DA POLITÍCA DE SEGURANÇA E AS TÉCNICAS DE PROTEÇÃO AOS SISTEMAS DE INFORMAÇÃO
https://www.unifimes.edu.br/filemanager_uploads/files/documentos/semana_universitaria/xii_semana/artigos/engenharias_tecnologias/IMPORTANCIA%20DA%20POLITICA%20DE%20SEGURANCA%20E%20AS%20TECNICAS%20DE%20PROTECAO%20AOS%20SISTEMAS%20DE%20INFORMACAO.pdf

Integrando a Segurança da Informação a um Sistema de Gestão Organizacional
https://repositorio.altecasociacion.org/handle/20.500.13048/266

Relatório de Ameaças BlackBerry 2021
https://www.blackberry.com/br/pt/forms/enterprise/report-bb-2021-threat-report-pt

TEMA 5 Sistemas de Gestão da Segurança da Informação

INTRODUÇÃO À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O objetivo deste texto é apresentar uma introdução conceitual à gestão da segurança, com base na gestão de riscos de segurança da informação.
O texto apresenta algumas orientações para a introdução da gestão de riscos nas organizações, baseadas na Norma AS-NZS 4360 (Standards Australia and Standards New Zealand, 2004), da qual deriva a ISO/IEC 31000 (ISO/IEC, 2009).
O texto foi produzido para suporte às atividades do CEGSIC 2009-2011, a partir de aprimoramento de material previamente desenvolvido em versões anteriores do CEGSIC (TRF JUS).

Desenvolvido em atendimento ao plano de trabalho do Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC 2009-2011.

https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf

TRANSIÇÃO DE TEMA

DÚVIDAS...

Escolas Integradas – Educação Continuada

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

PROF. WAGNER JOSÉ QUIRICI

Contatos:

Email: wquirici@gmail.com
Lattes: http://lattes.cnpq.br/1964137755924285
Linkedin: https://www.linkedin.com/in/wagner-quirici-5ba20743/

OBRIGADO!