Curso Fundamentos e Gestão da Segurança da Informação

Elias Sousa

v11032024

Conteúdo do curso

1 Fundamentos de Segurança da Informação
Entendimento dos principais aspectos e definições gerais relacionados à segurança da informação.

2 Organização e Segurança da Informação
Como a segurança da informação se relaciona com as partes internas e externas, seus requisitos e direcionamentos.

3 Gestão dos Ativos
Gerenciamento dos ativos da organização.

4 Operações de Segurança da Informação
Análise das operações de segurança da informação na Organização.

Módulo 01

Fundamentos de Segurança da Informação

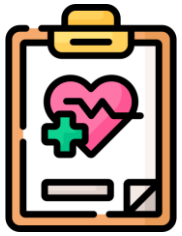
Entendimento dos aspectos e definições gerais relacionados à segurança da informação.

O que é a Segurança da Informação

A Segurança da Informação pode ser definida como a preservação da confidencialidade, integridade e disponibilidade das informações da organização. É muito comum o uso das siglas ***CIA (inglês)*** ou ***CID (português)*** quanto aos principais pilares da segurança da informação.

Confidencialidade
(confidentiality)

Propriedade de que as informações **não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados.**
Em outras palavras, as informações são acessíveis apenas pelas partes devidamente autorizadas e que necessitam do acesso à informação.



Integridade
(integrity)

Diz respeito a propriedade de **precisão e integridade da informação, ou seja, a informação é completa e confiável.** Pode-se dizer que a informação tem sua integridade assegurada quando ela não é alterada por uma parte sem autorização.

Disponibilidade
(availability)

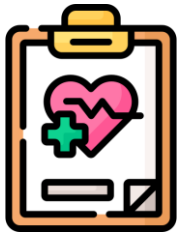
Propriedade de que **as informações devem ser acessíveis sempre que forem solicitadas**, ou seja, independente do período, quando solicitada a informação deve estar disponível para a parte requisitante.

Exemplo prático

Cenário: envio de um contrato para um advogado

Confidencialidade

Antes de disponibilizar o documento para o advogado, e necessário **criptografar o documento para que apenas as partes que possuem a senha consigam ler/modificar o documento**.



Integridade

Por estar criptografado, **apenas as pessoas que possuem a senha podem editar o documento,** logo, o documento está protegido contra alterações não autorizadas.

Deve ser levado em consideração a existência de métodos que exploram vulnerabilidades criptográficas e/ou o vazamento da senha.

Disponibilidade

O documento foi disponibilizado no drive pessoal da parte, teoricamente, estando **disponível constantemente para que seja consultado sempre que necessário**. Mesmo que esteja disponível para pessoas não autorizadas, apenas as pessoas que possuem a senha são capazes de ler/modificar o documento.

Conceitos chave

Outros itens que devem ser considerados

Autenticidade

Propriedade de que uma parte é quem diz que é, ou seja, uma informação pode ser considerada autêntica quando foi criada/enviada por **uma parte verídica onde sua origem é confiável**.

Não repúdio

A característica de que não é possível negar a autenticidade da informação, ou seja, **não é possível contestar a autoria da informação**.

Identificação

A utilização de **meios para identificação da parte**, como por exemplo, nome de usuário, e-mail ou ID's

Autenticação

Os mecanismos e garantias de que **a parte é capaz se assegurar que ela é quem ela diz que é**. Por exemplo, a utilização das credenciais para se autenticar em um portal onde a parte possui seu usuário.

Autorização

O conjunto de direitos relacionados ao usuário, após sua autenticação, o usuário possui suas devidas permissões e autorizações atribuídas, estando a parte permitida a **executar as ações as quais fora autorizado**.

Auditoria /Accounting

Diz respeito ao **rastreio e registros das ações e atividades do usuário**, auxiliando também nas auditorias, além de poder identificar pontos de inconformidade e/ou ações não autorizadas – todas as ações podem ser rastreadas e ligadas a algo/alguém.

Triple AAA

- Authentication
- Authorization
- Accounting

Métodos de autenticação

Uma parte é capaz de se autenticar por diversos meios, os mais comuns são:

O que ele SABE

Trata de meios como **senhas/palavras chave, códigos** e afins.

São recursos onde apenas a pessoa "sabe/conhece" o meio para a autenticação.

O que ele É

Contempla o uso de métodos relacionados a pessoa física, como **biometria, leitura facial, leitura de retina/íris.**

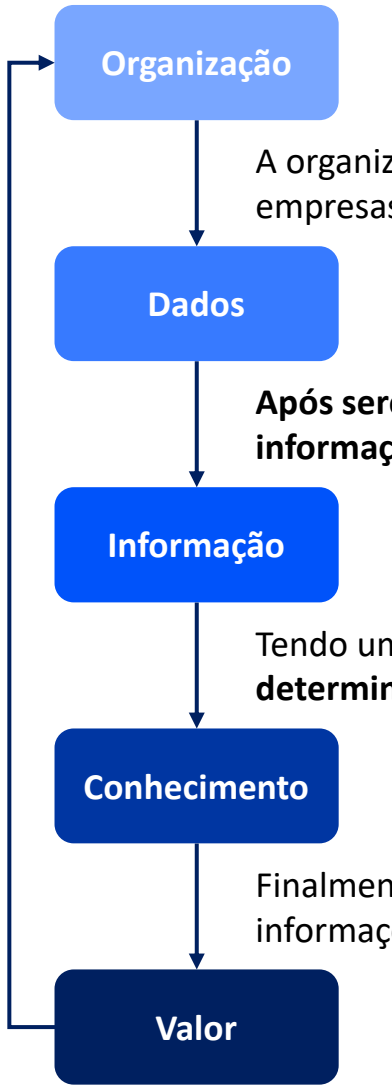
O que ele TEM

Abrange os recursos que a pessoa possua/tenha, como **tokens, cartões físicos, crachás, chaves e passes de acessos.**

MFA / 2FA

A autenticação multifator *(Multi-factor authentication)* diz respeito ao uso de dois ou mais métodos de autenticação. Por exemplo, um sistema que necessita de uma senha (o que ele sabe) e o uso da leitura biométrica (o que ele é).

Informação, dados e Organização



A organização (pode ser também quaisquer outras partes como empresas, clientes, terceiros e etc) **gera e processa os dados.**

Após serem processados, os dados são transformados em informação, tendo assim um significado.

Tendo um objetivo agora, **a informação é utilizada para uma determinada finalidade, transformando-a em conhecimento**.

Finalmente, o conhecimento adquirido através das informações processadas **geram valor para a organização.**

Dados

Ana 24 Paula
30 Rafael 12 França
Bahia São Paulo

Informação e conhecimento

- Ana, possui 24 anos e mora em São Paulo
- Paula, possui 12 anos e mora na França
- Rafael, possui 30 anos e mora na Bahia

Geração de valor

A organização utiliza as informações adquiridas para a análise e execução de suas estratégias de negócio.

Ciclo de vida da informação

1

Planejamento e aquisição

Trata de todo planejamento envolvido para a **execução da criação ou coleta das informações**, como a identificação das partes, objetivos, arquiteturas, padrões e modelos. Posteriormente, a criação dos registros de dados, compra de dados, carregamento de arquivos externos e etc.

2

Armazenamento

A fase em que **a informação é armazenada, seja digitalmente nos dispositivos eletrônicos ou documentos físicos** como papel e registros da organização.

3

Compartilhamento

A informação é disponibilizada para uso através de um método de distribuição. As atividades nesta fase se referem aos processos de **alocação da informação em locais onde ela possa ser acessada e utilizada** pelas partes como um arquivo ou banco de dados.

4

Manuseio

A informação é usada para atingir os objetivos das partes. As atividades nesta fase podem se referir a **todos os tipos de uso/manuseio de informação.**

5

Monitoramento

É assegurado que a informação continue funcionando adequadamente, ou seja, continue tendo valor para as partes. As atividades desta fase podem se referir a **manutenção (revisão e atualização) da informação.**

6

Descarte

A informação é descartada quando já não têm mais utilidade. As atividades desta fase podem se referir ao **arquivamento e/ou destruição da informação.**

Controles de Segurança

Os *controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modifiquem o risco, ou seja, **se trata de uma medida que visa modificar o risco**.

*Além do termo controle, é comum a utilização de termos como medidas, contramedidas e salvaguardas em documentações.

Categorias de controles

Controles Detectivos

São **mecanismos que visam identificar quaisquer *eventos** que possam representar uma ameaça aos ativos da organização.

Controles Dissuasivos

São controles que tem como intenção **dissuadir a parte mal intencionada, ou seja, fazendo com que ela desista de prosseguir** e realizar uma ação não autorizada.

Controles Preventivos

São controles que **visam prevenir/evitar a materialização da ameaça explorar uma vulnerabilidade**.

Controles Repressivos

São mecanismos que objetivam reprimir os impactos da ameaça, ou seja, **após a materialização do riscos as medidas são acionadas para mitigar os impactos**.

Controles Compensatórios

Trata da implementação de outros controles para **compensar a ausência de um determinado controle**.

Controles Corretivos

Medidas que atuam de maneira corretiva ou de recuperação por exemplo, onde **após a materialização dos impactos tais controles são acionados para restaurar os ativos da organização**.

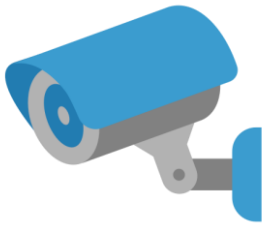
*Um evento pode ser definido como qualquer ocorrência detectável que tem importância para a gestão dos serviços de TI, podendo indicar que algo não está de acordo com a operação normal do serviço ou descumprindo um nível de serviço acordado.

Exemplo prático

Organizacional

A implementação de uma **Política de Segurança da Informação** fornece os direcionamentos para os colaboradores quanto aos requisitos da organização, onde **as partes que violarem as diretrizes da política ficam sujeitas a punições como encerramento de contratos, multas e demissões.**

Físico



Uma **câmera de vigilância pode detectar** ações mal intencionadas, além de **dissuadir e/ou prevenir possíveis ações** que um invasor possa tentar executar por exemplo.

Lógico

Um firewall devidamente configurado no ambiente da organização **pode evitar conexões não autorizadas**, e a depender pode auxiliar na **detecção de eventos e geração de alertas de segurança.**

Introdução à gestão de riscos

A gestão de riscos trata das atividades e controles que uma organização executa - identificando, analisando, avaliando e tratando os riscos aos quais a organização possa estar exposta.

A ISO fornece algumas das metodologia mais utilizadas tratando de gestão de riscos, como por exemplo:

- **ISO 31000 - Gestão de riscos**
- **ISO 27005 - Gestão de riscos de segurança da informação**

O risco é o efeito da incerteza sobre os objetivos da organização. É a **combinação da probabilidade de um evento e as suas consequências**, gerando assim um efeito positivo/negativo. Um risco de segurança da informação pode ser expresso como a combinação de um evento de segurança da informação e as suas consequências.

Ameaça = Algo/Alguém que represente uma ameaça à organização podendo causar algum dano a mesma – a ameaça pode ser acidental, intencional ou natural

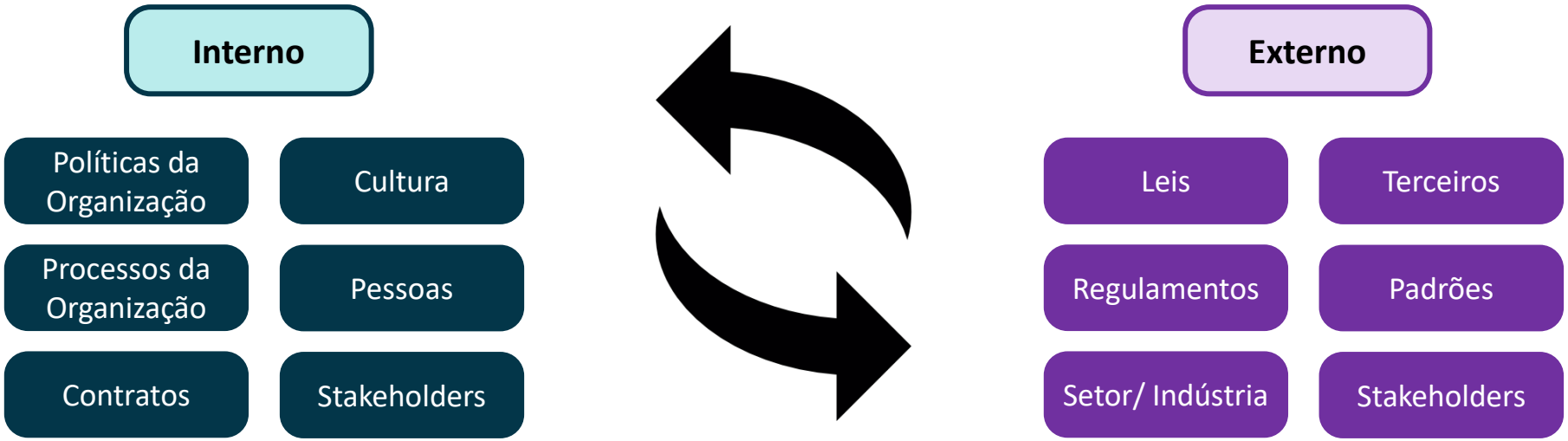
Vulnerabilidade = Ponto de fraqueza/falha em um ativo – pessoas, processos ou tecnologia

Impacto = Os efeitos causados pela exploração de uma vulnerabilidade por uma ameaça, os efeitos podem ser tangíveis, intangíveis, diretos ou indiretos – financeiros, imagem/reputação, operacional ou legal por exemplo

Risco = A relação entre a probabilidade da materialização do evento e os efeitos do impacto

Escopo e contexto

Antes de efetivamente iniciarmos uma análise de risco, **é crucial a compreensão do contexto da organização.**



Entender quais itens a organização está sujeita é importante, pois isto irá nos **fornece os direcionamentos e escopo para a realização das atividades da organização** - se uma organização possui uma empresa em um outro país, as leis e normas deste país devem ser consideradas, como a norma de privacidade de dados por exemplo, **descrevendo os requisitos que a empresa deve atender para estar em conformidade e poder operar.**

Os itens ilustrados acima são apenas alguns exemplos, cada organização possui seu próprio contexto que por sua vez deve ser compreendido pela equipe responsável pela análise de riscos.

Ameaças

Eventos Naturais

- Chuvas
- Raios
- Tornados
- Furacões
- Terremotos
- Tsunamis
- Fenômenos Meteorológicos
- Condições climáticas adversas

São ameaças naturais que fogem do controle humano. Devem ser considerados os aspectos climáticos e sazonalidades da região nas análises

Danos físicos

- Água
- Fogo
- Poluição
- Poeira
- Corrosão
- Congelamento
- Umidade
- Defeitos nos equipamentos

São ameaças relacionadas aos aspectos físicos dos ativos da organização

Pessoas

- Hackers/Crackers
- Hacktivismo
- Espionagem industrial
- Organizações criminosas
- Estado/nação
- Script kiddies
- Insiders

São ameaças relacionadas as pessoas, seja direta ou indiretamente

Sistema

- Malwares
- Falhas ou “bugs”
- Comprometimento dos dados
- Abuso de privilégios
- Acesso ou alteração não autorizada
- Indisponibilidade
- Outros

São ameaças relacionadas aos sistemas de informação da organização

São ameaças relacionadas aos serviços e fornecedores da organização

Interrupção de serviços críticos

- Fornecimento de água
- Fornecimento de eletricidade
- Fornecimento de insumos em geral para a organização

Invasores

Hackers (legal)

Crackers (ilegal)

Pessoa ou grupo de pessoas que **intencionalmente buscam realizar invasões à sistemas, para fins de ganho/mérito próprio**. Eles podem possuir variados níveis de recursos, conhecimentos e motivações.

Hacktivismo

O nível de recursos e conhecimentos podem variar, normalmente não são agressivos e **focam em aspectos políticos ou ideológicos.**

Espionagem industrial

Nível sofisticado de recursos, são **motivados por ganhos próprios** podendo afetar diretamente ou indiretamente a Organização.

Organizações criminosas

Nível variável de recursos, porém, é uma ameaça que sempre deve ser considerada. **São motivados por ganhos próprios**.

Estado/nação

Possuem um nível extremo de recursos, são motivados por **questões políticas, ideológicas, econômicas, guerras e outros.**

Script kiddies

São pessoas que possuem **poucos recursos e** conhecimentos **e/ou que visam buscar algum tipo de reconhecimento.**

Insiders

São os **funcionários da organização, que acidental ou intencionalmente podem fazer algo contra a organização**, podem ser motivados por ganhos próprios ou vingança.

White hat: Também conhecido como hacker ético, ele atua legalmente, “explorando” as vulnerabilidades afim de ajudar a organização a melhorar e corrigir seus sistemas

Grey hat: Alguém que atua tanto para o White quando o Black hat, pode ajudar a organização mas também pode buscar ganhos próprios quando conveniente

Black hat: Uma pessoa mal intencionada que explora e expõe as falhas da organização sem nenhum tipo de autorização

Vulnerabilidade – Exemplo prático

Uma vulnerabilidade, de forma macro, pode contemplar fatores como pessoas, processos ou tecnologias da organização.

1. **Os funcionários da Organização:**
    - Não praticam as diretrizes da Política de Segurança da Informação, mesa limpa por exemplo, onde a intenção é fazer com que não tenha informações desnecessárias e/ou confidenciais na mesa do funcionário, como uma folha com a relação de nomes e salários dos funcionários da organização exposta e sem a presença do funcionário responsável, ou mesmo um post-it com senhas
    - Conversam de maneira desatenta na hora do almoço em um ambiente público, expondo acidentalmente dados e informações sobre os projetos internos da organização
2. **Os processos da Organização:**
    - São totalmente manuais e dependente dos funcionários, qualquer problema com o funcionário pode causar a interrupção do processo
    - Estão desatualizados, perdendo eficiência e podendo estar em inconformidade com os órgãos regulamentadores
3. **A tecnologia da Organização:**
    - É obsoleta, estando sujeita a ineficiência e possíveis vulnerabilidades, visto que não recebem mais atualizações de segurança de seus fornecedores
    - Não há gestão sobre os acessos lógicos dos sistemas

Quem estiver analisando as vulnerabilidades deve ter um olhar crítico, dado uma situação/cenário ele(a) deve pensar em todos os possíveis impactos que podem ocorrer caso essa “falha” seja explorada e qual a relevância desse impacto à organização.

Impacto – Exemplo prático

O impacto se dá através dos **efeitos que uma ameaça causa ao explorar uma vulnerabilidade**. Diversos impactos podem ser causados de acordo com o contexto da organização, isso deve ser analisando pela equipe responsável. Os tipos de impactos mais comuns são:

Financeiro

- A empresa ficaria paralisada por 5 horas, causando um impacto de R$ 1 milhão/hora.
- Suas ações iriam perder valor na bolsa de valores.
- Por ter processos críticos, a paralização acarretará uma multa advinda de partes terceiras.

Legal/regulatório

- Por ter processos críticos que não podem estar indisponíveis, a organização ficará em inconformidade ante os órgãos regulamentares ou quaisquer requisitos que ela tenha que cumprir.
- A paralização acarretará sanções à organização por parte dos órgãos regulamentares ou quaisquer requisitos que ela tenha que cumprir.

Reputação/imagem

- A paralisação pode passar a imagem para os funcionários, terceiros, parceiros ou clientes de que a organização carece de medidas, afetando a organização por meio da diminuição de vendas, queda na confiança e até mesmo abalando a relação interna entre as equipes da organização.

Operacional

- Por estar paralisada, a operação da Organização seria inexistente, estando consideravelmente impactada.
- A depender da área afetada, outras vertentes da organização podem estar operantes, por exemplo, a fábrica está inoperante, porém, a administração continua a operar.

É comum um tipo de impacto ter uma influência indireta em outro tipo de impacto, por exemplo, uma inconformidade legal pode afetar drasticamente a imagem de uma empresa, fazendo com que ela perca mercado, dado que outras empresas não vão querer ter relações com essa empresa.

Exemplo dano direto: se a organização parar sua produção, ela não terá mais produtos, logo, não poderá vende-los

Exemplo dano indireto: problemas na reputação da organização podem causar diminuição nas vendas

Impacto

Já identificados os pontos chave, iremos analisar o risco, classificando os níveis de impacto e probabilidade que o risco pode representar à organização.

Os impactos podem ser **quantitativos e/ou qualitativos**.

Definição dos critérios

Quantitativo: Descrição mais "palpável", especificando valores na definição dos critérios, exemplo, R$ 1 milhão e 24 horas

Qualitativo: Atua mais nos cenários e possibilidades do risco, por exemplo, impacto causado em mais de 2 empresas da organização ou ocorrência nos últimos 12 meses

	Financeiro	Legal	Imagem	Operacional
Muito alto (4)	• Impactos superiores a R$ 1 milhão • Impactos superiores a 50% da receita liquida da Empresa	• Inconformidades diretas ante os Órgãos regulamentares • Processos judiciais graves	• Impacto direto às estratégias da Empresa • Perda de confiança de stakeholders críticos • Repercussão em mídias sociais, na mídia nacional e internacional	• Interrupção nas operações da Empresa por um período superior a 24 horas • Interrupção total da Empresa
Alto (3)	• Impactos superiores a R$ 500 mil • Impactos superiores a 35% da receita liquida da Empresa	• Sanções administrativas e multas • Processos judiciais	• Repercussão na mídia regional • Dano ante os stakeholders	• Interrupção nas operações da Empresa por um período superior a 12 horas • Interrupção das atividades de administrativas da Empresa
Médio (2)	• Impactos superiores a R$ 100 mil • Impactos superiores a 10% da receita da Empresa	• Notificações legais	• Repercussão na mídia local	• Interrupção nas operações da Empresa por um período superior a 2 • Interrupção das atividades de produção da Empresa
Baixo (1)	• Impactos inferiores a R$ 100 mil • Impactos inferiores a 10% da receita da Empresa	• Nenhum impacto	• Repercussão interna entre os colaboradores	• Interrupção nas operações da Empresa por um período inferior a 2 horas

Cabe à Organização definir os métodos e classificações de acordo com seu próprio contexto, podem ser simples (baixo, médio, alto) ou mais complexas (muito baixo, baixo, médio, alto, muito alto, crítico) – O mesmo para a classificação da probabilidade.

Probabilidade

Igualmente aos impactos, a probabilidade deve ser definida, podendo também ser quantitativo **e/ou** qualitativo.

Quais as chances de uma ameaça explorar uma vulnerabilidade?

- Qual a probabilidade de um servidor exposto à internet que está rodando um Windows Server 2012 ser invadido?
- Qual a probabilidade de uma pessoa entrar acidentalmente na sala do servidor da empresa que está localizada ao lado do banheiro e sem controles de acesso?
- Qual a probabilidade de um carro bater no poste de energia que fornece as fibras de internet para a Empresa e causar a indisponibilidade de rede?
- Qual a probabilidade de um avião cair no local onde ficam os servidores primários e de contingência da Empresa?

	Descrição
Provável (4)	• 75% ou mais de chances de ocorrer • Histórico de ocorrência nos últimos 6 meses • É extremamente capaz de ocorrer
Possível (3)	• 50% ou mais de chances de ocorrer • Histórico de ocorrência nos últimos 12 meses • Pode ocorrer
Médio (2)	• 25% ou mais de chances de ocorrer • Histórico de ocorrência nos últimos 2 anos • Há uma chance de que ocorra
Baixo (1)	• Até 25% de chances de ocorrer • Histórico de ocorrência superior a 2 anos • Improvável de ocorrer

Avaliação de riscos

Avaliar o risco consiste em definir uma classificação ao risco, para que assim a organização consiga **priorizar os riscos de maneira adequada**.

Critérios de avaliação

Probabilidade				
Provável (4)	4	8	12	16
Possível (3)	3	6	9	12
Médio (2)	2	4	6	8
Baixo (1)	1	2	3	4
	Baixo (1)	**Médio (2)**	**Alto (3)**	**Muito alto (4)**

Impacto

Classificação do Risco

Crítico	12 - 16
Risco Alto	8 - 9
Risco Médio	3 - 6
Risco baixo	1 - 2

Conceitos complementares

Rinoceronte Cinza

"riscos que têm uma **chance grande de ocorrer e um impacto enorme se acontecerem, mas que deixamos de reconhecer** como ameaças porque negligenciamos sua obviedade. Não é que não tenhamos visto o problema chegando; nós apenas o desprezamos"

Cisne Negro

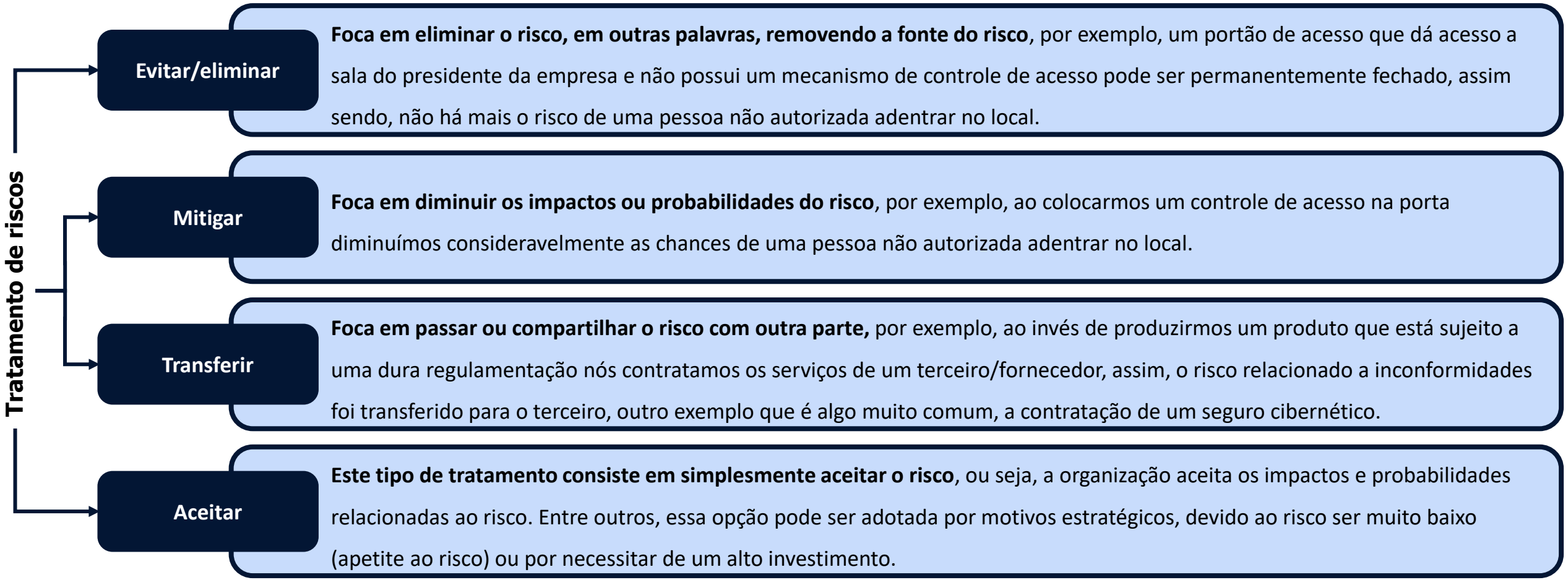
"têm **uma probabilidade muito baixa de ocorrer, mas podem ter consequências catastróficas** se ocorrerem."

Referência para leitura

Há variadas metodologias para avaliação do risco que podem incluir mais itens além do impacto e probabilidade, a organização deve definir qual irá seguir, por exemplo, ela irá desenvolver sua própria metodologia para avaliar o risco ou irá seguir algum padrão já existente no mercado.

Tratamento de riscos

Após sua avaliação, os riscos devem ser tratados de acordo com a sua criticidade e prioridade ante a organização. As partes envolvidas (direção, equipes responsáveis, comitês e áreas de negócios que forem os donos dos processos relacionados ao risco) deverão selecionar a **estratégia que irão adotar quanto ao risco, posteriormente aplicando os respectivos controles**.



Aceitação e apetite ao risco

O apetite ao risco da organização basicamente reflete o nível de risco que ela está disposta a aceitar, por exemplo, ao olharmos para a tabela da avaliação de riscos, a organização decidiu que quaisquer riscos que forem classificados como “Baixo” serão aceitos.

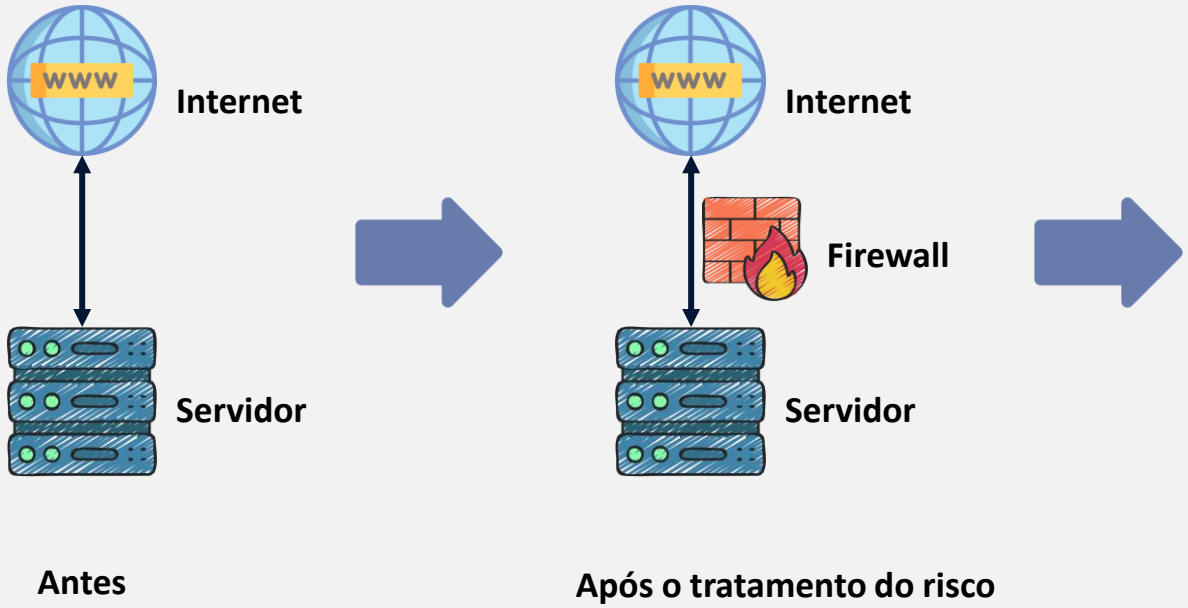
- **Exceções devem ser consideradas**, não é porque um risco se encaixa no apetite a risco da organização que ele deve ser automaticamente aceito sem uma análise prévia;
- **O risco deve ser devidamente registrado**, assim como as partes envolvidas, além do mais, ele deve ser monitorado caso ocorram alterações em seus impactos por exemplo;
- O risco quando aceito, **deve ser aceito de forma explícita e formal entre as partes envolvidas**, por exemplo, por meio de relatórios ou cartas de aceitação de risco, onde é formalizado entre as partes que mesmo com os impactos envolvidos a estratégia selecionada foi de aceitar o risco;

Risco residual

O risco residual são todos os riscos que restarem após o tratamento do risco, ou seja, após a aplicação dos controles, restaram alguns riscos ou mesmo riscos novos foram criados com a aplicação dos controles.

Exemplo prático

Cenário: um servidor da organização que é utilizado pelos clientes e pelos colaboradores está exposto na internet sem nenhuma proteção.



Riscos Residuais

- Os clientes podem ter dificuldades para acessar o servidor
- As integrações que o servidor possuía podem ter ficado indisponíveis devido alguma regra do firewall
- Pode haver problemas relacionados a eficiência e capacidade dos recursos devido ao firewall estar filtrando as requisições

Complementar

Risco inerente: Se trata do nível do risco sem a aplicação de nenhum controle. O risco inerente vai entender o nível do risco antes da aplicação de um controle (cenário normal/original), enquanto o residual, vai entender o nível do risco após a aplicação dos controles

Gestão de riscos – Visão geral

Identificação do escopo e contexto da Organização

- Requisitos internos
- Requisitos externos
- Requisitos Regulatórios/ Legais

Identificar os fatores relacionados ao risco

- Identificação das vulnerabilidades e ativos vulneráveis
- Identificação das ameaças
- Identificar e listar as chances e os possíveis impactos que podem ser causados

Analisar as informações coletadas e entender os impactos envolvidos

- Avaliar e classificar os impactos
- Avaliar e classificar a probabilidade

Avaliar e classificar o risco

- Avaliar o risco para identificar sua criticidade ante a Organização (apetite ao risco)

Formalizar a aceitação do risco junto as partes envolvidas e prosseguir gerenciando o risco

Avaliar se após o tratamento do risco os riscos residuais estão dentro do apetite a risco da organização

Definir uma estratégia de tratamento

- Evitar
- Mitigar
- Transferir
- Aceitar

Entender se o risco foi avaliado de maneira adequada, se a classificação dele reflete de fato o seu risco e faz sentido para a organização.

Complementar – SLE, ALE, EF e ARO

SLE *(Single loss Expectancy):* Expectativa de perda única

ALE *(Annualized loss Expectancy):* Expectativa de perda anual

EF *(Exposure Factor):* Fator de exposição

ARO *(Annualized Rate of Occurence):* Taxa de ocorrência anual

EF

Pode ser compreendido como a porcentagem dos danos à um ativo.

SLE

Diz respeito ao dano à organização que será causado pela ocorrência de um determinado evento.

Valor do ativo X EF

ARO

Trata da frequência da ocorrência durante o ano.

ALE

Diz respeito ao dano à organização que será causado pelas ocorrências do evento no ano.

SLE x ARO

Exemplo prático

- Mensalmente, há 2 ocorrências de roubo de notebooks dos colaboradores (notebook corporativo);
- Cada notebook custa R$ 5.000;
- O seguro cobre 75% do valor do notebook, ou seja, 25% do valor está exposto;

EF =	25%	
SLE =	5.000 x 0,25	= R$ 1.250
ARO =	2 x 12	= 24
ALE =	1.250 x 24	= R$ 30.000

Exemplo prático

Cenário: Empresa Xpto

Informações coletadas:

1. Uma vez ao ano, há ocorrência de fortes chuvas e inundações na região (cidade pequena do interior) onde está localizado o centro fabril da Empresa Xpto, é normal a região ter indisponibilidades que durem de 1 a 3 dias em determinados pontos da cidade;
2. A Empresa possui um estoque de segurança localizado no centro de distribuição (em outra cidade) com uma capacidade equivalente a 24 horas de produção;
3. A Empresa fatura em média R$ 500 mil/hora e seus clientes são outras empresas, as quais possuem contratos de curto prazo, renovados a cada 2 anos.

Análise dos dados

- Há histórico e é quase certo de que ao menos 1 vez ao ano haja chuvas e inundações na região da fábrica, podendo causar indisponibilidade na fábrica por até 3 dias;
- Por ser uma cidade pequena, do interior e que as chuvas e inundações são recorrentes, há poucos aspectos ligados a exposição pública local da empresa;
- A empresa possui um estoque máximo de 1 dia de produção (centro de distribuição);
    - O tempo máximo que a fábrica pode ficar indisponível não é coberto - apenas 1/3 está “protegido”;
- A Empresa poderia deixar de faturar cerca de R$ 24 milhões - se considerarmos a utilização dos itens no estoque de 1 dia, a Empresa sofreria os impactos equivalentes a 2 dias de produção;
- Grande parte das vendas são para outras empresas com contrato firmado e um curto prazo de renovação, pode haver um impacto na reputação da Empresa ante as outras empresas no cenário em que haja atrasos nas entregas, causando a perda dos prazos dessas empresas e podendo gerar variados impactos pela falta do fornecimento dos produtos. Mas deve ser considerado que elas provavelmente possuem um estoque de segurança;
- Indenizações podem ser requisitadas pelas empresas que sofreram algum impacto devido a indisponibilidade do produto pela Empresa Xpto.

Há variadas metodologias para avaliação do risco que podem incluir mais itens além do impacto e probabilidade, a organização deve definir qual irá seguir, por exemplo, ela irá desenvolver sua própria metodologia para avaliar o risco ou irá seguir algum padrão já existente no mercado.

Exemplo prático

Avalição do risco

- **Financeiro –** Impacto de R$ 24 milhões na receita da empresa
- **Legal –** Pode haver ações contra a empresa advindas dos clientes/Sem aspectos regulatórios
- **Imagem –** Baixa exposição pública, porém, há um impacto direto ante seus clientes, podendo causar a perda de confiança na Empresa Xpto
- **Operacional –** Ficaria no máximo 3 dias inoperante

	Financeiro	Legal	Imagem	Operacional
Muito alto (4)	• **Impactos superiores a R$ 1 milhão** • **Impactos superiores a 50% da receita liquida da Empresa**	• Inconformidades diretas ante os Órgãos regulamentares • Processos judiciais graves	• **Impacto direto às estratégias da Empresa** • **Perda de confiança de stakeholders críticos** • **Repercussão em mídias sociais, na mídia nacional e internacional**	• **Interrupção nas operações da Empresa por um período superior a 24 horas** • **Interrupção total da Empresa**
Alto (3)	• Impactos superiores a R$ 500 mil • Impactos superiores a 35% da receita liquida da Empresa	• **Sanções administrativas e multas** • **Processos judiciais**	• **Repercussão na mídia regional** • **Dano ante os stakeholders**	• Interrupção nas operações da Empresa por um período superior a 12 horas • Interrupção das atividades de administrativas da Empresa
Médio (2)	• Impactos superiores a R$ 100 mil • Impactos superiores a 10% da receita da Empresa	• Notificações legais	• Repercussão na mídia local	• Interrupção nas operações da Empresa por um período superior a 2 • Interrupção das atividades de produção da Empresa
Baixo (1)	• Impactos inferiores a R$ 100 mil • Impactos inferiores a 10% da receita da Empresa	• Nenhum impacto	• Repercussão interna entre os colaboradores	• Interrupção nas operações da Empresa por um período inferior a 2 horas

$$\textbf{Impacto} = \frac{4 + 3 + 4 + 4}{4} = \textbf{4 (Muito Alto)}$$

$$\textit{Impacto} = \frac{\textit{Impacto Financeiro + Impacto Legal + Impacto Imagem + Impacto Operacional}}{4}$$

	Descrição
Provável (4)	• 75% ou mais de chances de ocorrer • Histórico de ocorrência nos últimos 6 meses • É extremamente capaz de ocorrer
Possível (3)	• 50% ou mais de chances de ocorrer • Histórico de ocorrência nos últimos 12 meses • Pode ocorrer

Probabilidade = 3

Exemplo prático

Critérios de avaliação

Probabilidade				
Provável (4)	4	8	12	16
Possível (3)	3	6	9	12
Médio (2)	2	4	6	8
Baixo (1)	1	2	3	4
	Baixo (1)	Médio (2)	Alto (3)	Muito alto (4)

Impacto

Classificação do Risco

Crítico	12 - 16
Risco Alto	8 - 9
Risco Médio	3 - 6
Risco baixo	1 - 2

Tratamento do risco	Possíveis controles	Risco residual
Eliminar	Transferir a unidade fabril para outra localidade – uma nova unidade	Riscos relacionados ao novo local
Mitigar	Aumentar os estoques de segurança para 1 semana	Diminuição da eficiência da gestão dos recursos no estoque em um primeiro momento
Transferir	Contratar um seguro contra os impactos causados	• O dano causado pode ser superior a cobertura do seguro • O valor do seguro pode ser extremamente alto • O seguro pode não cobrir todos os itens
Aceitar	Não aplicar nenhum controle	N/A

Sistema de Gestão da Segurança da Informação (SGSI)

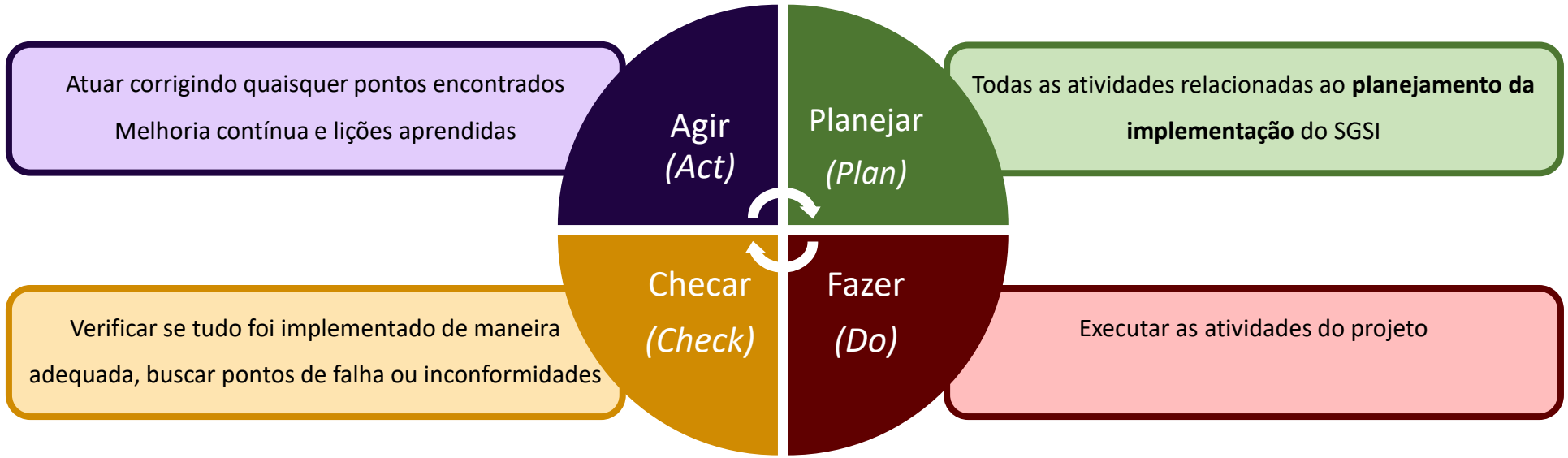
O SGSI tem o objetivo de garantir a segurança das informações da Organização, por exemplo, **assegurando os pilares da segurança da informação através da utilização de uma abordagem de gestão de riscos,** além do mais, **fornece a confiança às partes interessadas de que os riscos da Organização são gerenciados de forma adequada**.

A ISO fornece normas que auxiliam e especificam os requisitos para estabelecer, implementar, manter e melhorar um SGSI dentro do contexto da organização.

As principais são:

- **ISO 27001 - Técnicas de Segurança - Sistemas de gestão da segurança da informação - Requisitos**
- **ISO 27002 - Controles de segurança da informação**

Ciclo PDCA – implementação do Sistema



O SGCI é constituído de vários recursos, não é necessariamente um sistema típico, e sim um conjunto de recursos como pessoas, processos e tecnologias que colaboram com os mecanismos de segurança da informação.

Implementação de um SGSI - Exemplos

Políticas de SI	Papeis e responsabilidades	Contato com autoridades	SI na gestão de projetos	Gestão de ativos	Threat Intelligence	Uso aceitável
Classificação das informações	Controle de acessos	SI em fornecedores	SI em cloud	Resposta a incidentes	Propriedade intelectual	Conformidade
Medidas disciplinares	Segregação de tarefas	Treinamento e conscientização	Background check	NDAs	Trabalho remoto	Segurança do perímetro
Monitoramento físico	Mesa limpa	Segurança de mídias	Gestão de privilégios	Gestão da capacidade	Gestão de mudanças	Proteção contra malwares
Backup	Logs	Proteção contra vazamentos	Criptografia	Segregação de redes	Desenvolvimento seguro	Menor privilégio

Leis e padrões

Payment Card Inustry Data Security Standard (PCI DSS): É um padrão de segurança de informações usado para lidar com cartões de crédito, seu uso é obrigatório pelas empresas que lidam com atividades relacionadas a utilização e processamento de cartões de crédito. O PCI fornece um conjunto de requisitos que tem como premissa assegurar a proteção de informações confidenciais e garantir a segurança de dados sensíveis em transações financeiras.

International Organization for Standardization (ISO): A ISO é conhecida mundialmente, ela desenvolve e publica padrões que são utilizados por diversas indústrias e setores no mundo. A família ISO 27000 nos traz as normas relacionadas ao tema de segurança da informação, das quais, as principais são as ISO's 27001 e 27002.

Health Insurance Portability and Accountability Act (HIPAA): É um conjunto de normas que organizações de saúde norte-americanas devem cumprir para proteger as informações.

Sarbanes Oxley Act (SOX): Assegurar a transparência na gestão das empresas quando aos aspectos financeiros, o objetivo é exigir das companhias maior governança nas informações divulgadas e, consequentemente, dar maior segurança aos stakeholders sobre seus investimentos.

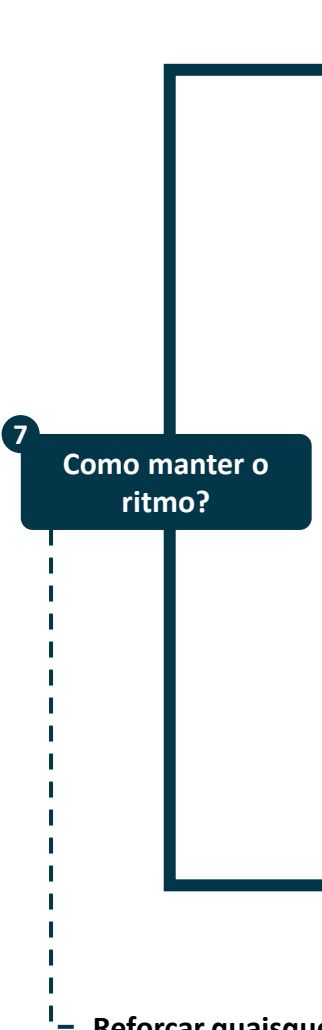
General Data Protection Regulation (GDPR): O Regulamento Geral sobre a Proteção de Dados, trata sobre a privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu.

Lei Geral de Proteção de Dados (LGPD): Regula as atividades de tratamento de dados pessoais

Existem dezenas de leis e padrões que podem ser considerados, porém, a organização deve identificar aquelas as quais ela **quer** e **deve** atender, a fim de estar em conformidade ou mesmo para objetivos estratégicos.

Modelo de melhoria continua ITIL

A melhoria continua é uma **atividade organizacional recorrente realizada em todos os níveis para garantir que o desempenho de uma organização atenda continuamente às expectativas das partes interessadas**. O modelo de Melhoria Contínua do ITIL pode ser usado como um guia de alto nível para apoiar iniciativas de melhoria.



1. **Qual a visão?** — **Traduzir/compreender a visão e os objetivos da organização, para que o contexto, os objetivos e os limites de qualquer iniciativa de melhoria sejam compreendidos/definidos.**
2. **Onde estamos agora?** — **Avaliação do estado atual**, dos serviços existentes, percepção dos usuários sobre o valor recebido, pessoas, processos, tecnologias, e outros, que serão utilizado como indicadores e linha de base.
3. **Onde queremos estar?** — As **melhorias são identificadas e priorizadas, objetivos são definidos, juntamente com fatores críticos de sucesso e indicadores-chave de desempenho (KPI's). Os objetivos acordados precisam ser SMART** (específicos, mensuráveis, alcançáveis, relevantes e com prazo determinado).
4. **Como chegamos lá?** — Agora que os pontos inicial e final de melhoria foram definidos, **uma rota específica pode ser seguida**. Com base na compreensão da visão da melhoria e dos estados atuais e alvo, **um plano para executar as demandas da iniciativa pode ser criado**.
5. **Tome uma ação/Agir** — **Executar o plano de ação elaborado na etapa anterior.**
6. **Chegamos?** — Esta etapa **envolve verificar as metas e objetivos para ter certeza de que o ponto desejado foi alcançado**. Vamos verificar se o estado alvo definido na etapa 3 foi alcançado após a ação na etapa 5. Se o resultado desejado não for alcançado, ações adicionais podem ser necessárias para concluir o plano e alcançar o objetivo acordado.

7. **Como manter o ritmo?** — **Reforçar quaisquer novos itens introduzidos**. Isso garante que o progresso feito não seja perdido e cria suporte e impulso para as próximas melhorias.