Apostila Adicional

EXIN Information Security Management Professional baseada na ISO/IEC 27001 (ISMP)

Propósito deste material

- Antes de fazer o seu exame, examine bem este material, pois todas as perguntas da prova partem destes princípios.
- Aqui você encontrará a base do exame. Imagine que ele foi desenvolvido sob a perspectiva dos termos e conteúdos encontrados aqui
- Todo este conteúdo é complementar ao curso. Ele incluem as ultimas atualizações do Syllabus e do exame.
- Como as perguntas deste exame ISMP não são iguais aos do nível fundamentos, com perguntas e respostas diretas, conceituais, você então terá que entender o assunto para apresentar soluções adequadas.

Literatura adicional (opcional)

A. Cazemier, J.A., Overbeek, P., and Peters, L.
Information Security Management with ITIL V3
Van Haren Publishing, 2010
ISBN 978 90 8753 552 0

B. Whitman, M.E., Mattord, H.J.
Management of Information Security
Cengage learning, 2010 Sixth Edition
ISBN: 978 1 337 40571 3

C. ISO/IEC 27001:2013 (EN)
Information technology -- Security techniques -- Information security management systems – Requirements
Switzerland, ISO/IEC, 2013
www.iso.org

1. Introdução

Definições

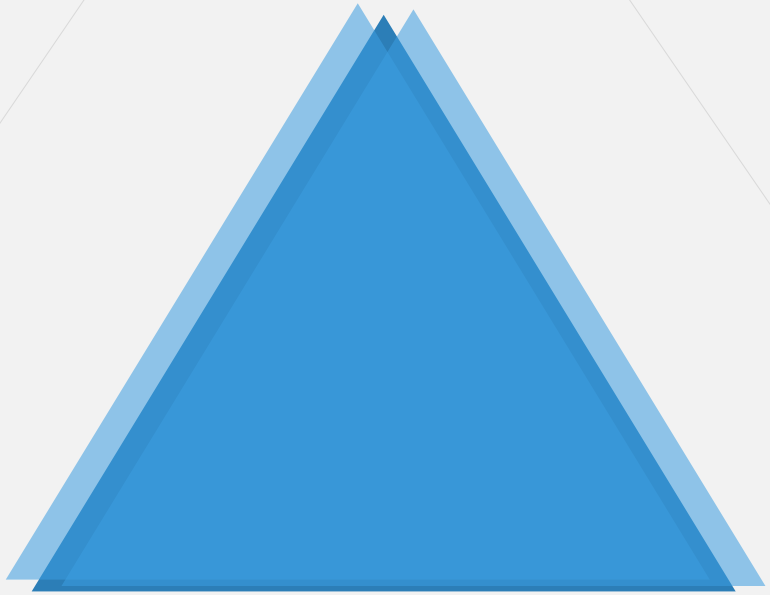
A segurança da informação lida com…

1. a definição, implementação, manutenção, conformidade e avaliação
2. um conjunto coerente de controles

3. salvaguardar, disponibilidade, integridade e confidencialidade
4. o fornecimento de informações (manual e automatizado)

Isso implica...

Um sistema de gerenciamento como ISO/IEC 27001

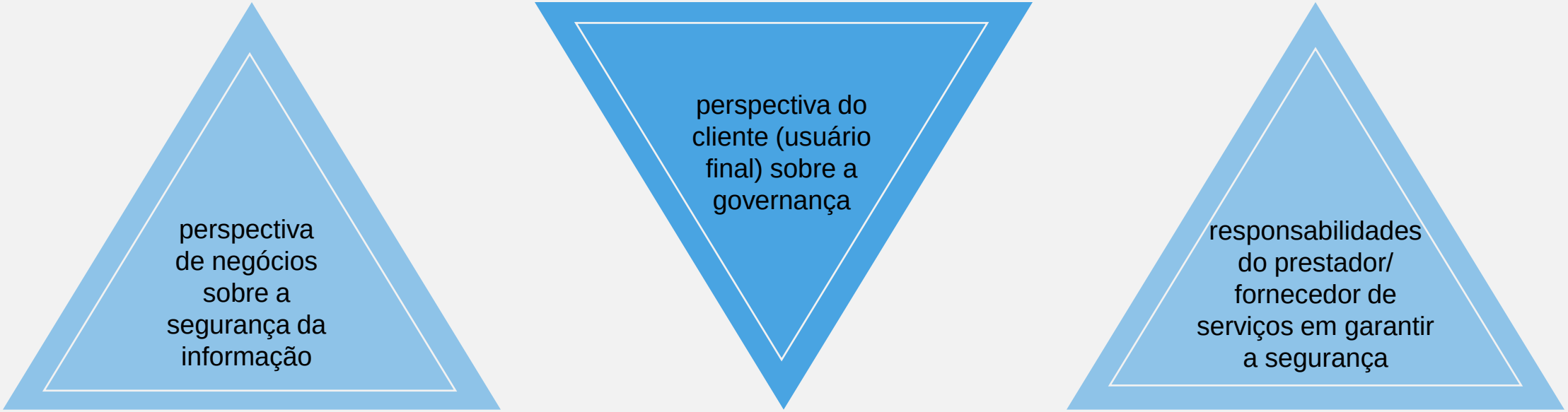


Um conjunto de controles como ISO/IEC 27002

Foco na disponibilidade, confidencialidade e integridade

2. Perspectiva da Segurança da Informação

Perspectivas de Segurança da Informação



2.1 Interesse do Negócio na Segurança da Informação

A perspectiva do negócio

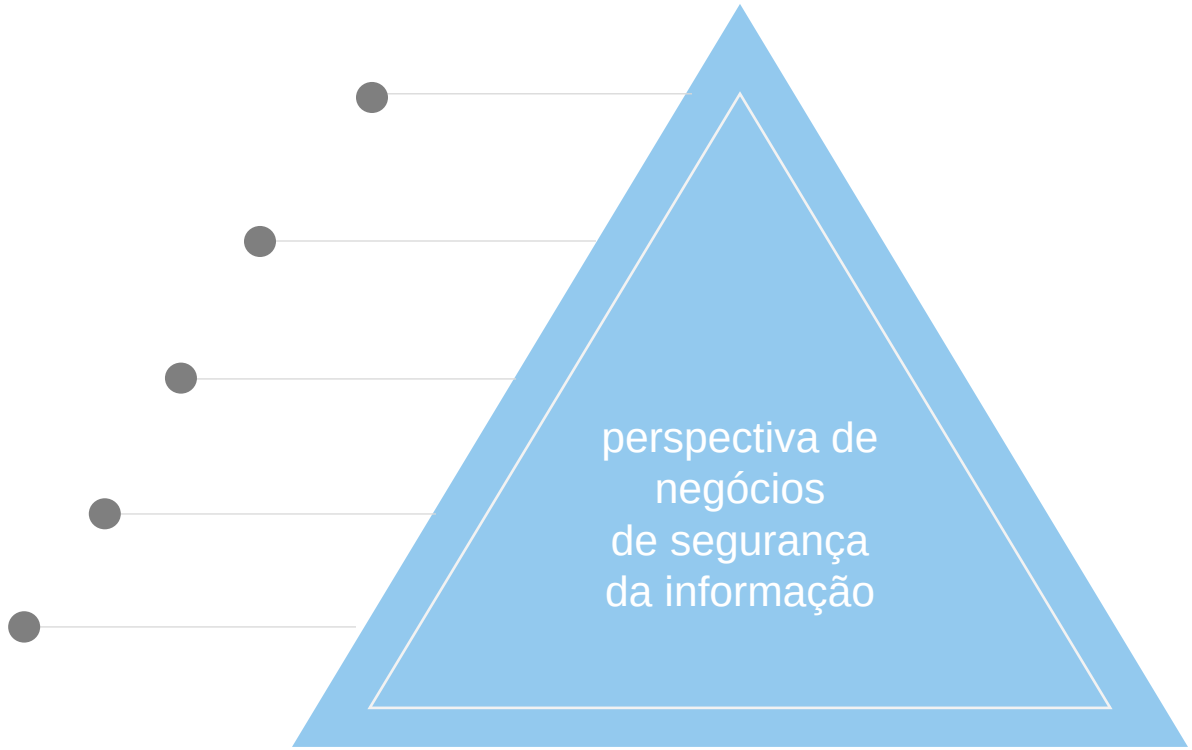
As informações se tornaram o ativo mais importante para a maioria dos negócios

A proteção desse ativo valioso contra perda, adulteração e divulgação é vital e os controles devem ser implementados em um nível apropriado de acordo com o valor da informação ou do ativo

Informação está em toda parte; mesmo fora do perímetro da organização, dificultando a proteção, mas ainda mais necessária; A segurança da informação não se limita apenas ao campo da TI

Os custodiantes da informação precisam mostrar que são confiáveis; governança e conformidade são fundamentais!

Padrões internacionais respeitados e melhores práticas de segurança, como a série ISO 2700x, ajudam a entender como lidar com o acima exposto (também ao usar fornecedores)



A perspectiva do negócio

As leis e os regulamentos obrigam as organizações a cumprirem com as melhores práticas de privacidade de dados e propriedade intelectual.

Histórias de incidentes viajam rápido; danos à reputação podem estar fora de seu controle, é necessário um foco na prevenção.

Como as informações estão em toda parte, a segurança das informações e a conscientização dos riscos precisam da atenção de todos.

Monitoramento, registro e organização proativa são elementos-chave; a detecção imediata de incidentes e o gerenciamento de incidentes são processos cruciais.

A segurança da informação precisa ser incorporada na organização.

Clientes e até fornecedores exigem transparência e conformidade.

2.2 Perspectiva do Cliente (Usuário Final) Sobre a Governança

Perspectiva do Cliente (Usuário Final) Sobre a Governança

Os clientes exigem a continuidade das operações de TI nos negócios, 24/7

Devido a um mercado aberto, os clientes podem levar seus negócios para outro lugar

As preocupações com a privacidade ainda são muito fortes, embora o uso das mídias sociais mostre que essa é uma faca de dois gumes

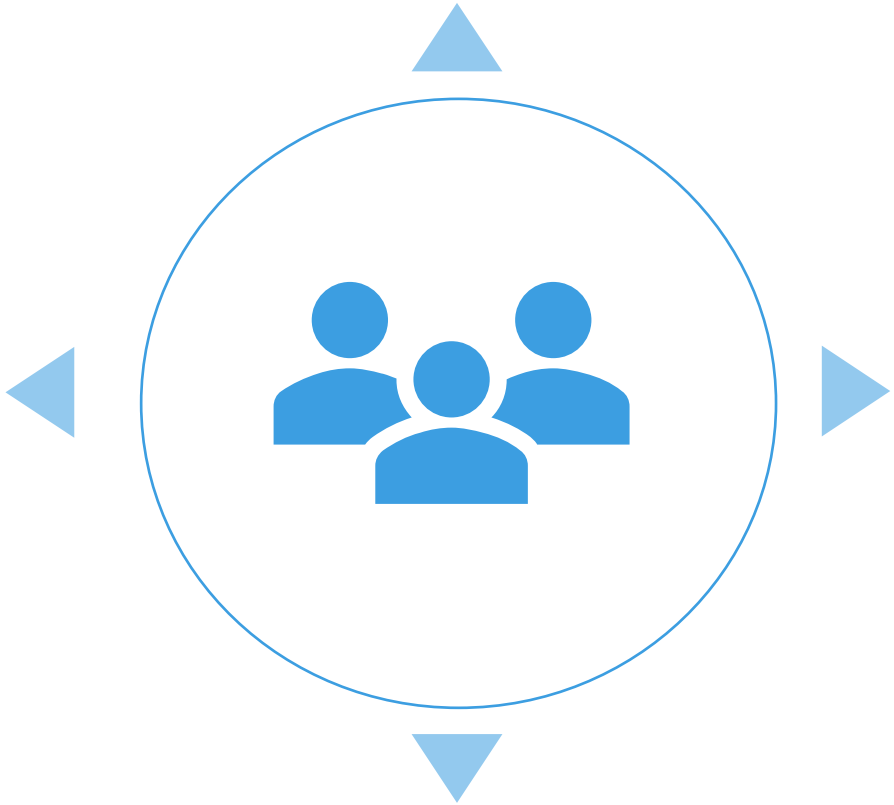
Os clientes se tornaram muito fortes… incidentes de segurança, portanto, recebem forte atenção da mídia

Os clientes confiam nas organizações que são transparentes na maneira como lidam com os riscos

Perspectiva do Cliente (Usuário Final) Sobre a Governança

Em ambientes B2B, a cadeia de confiança requer conformidade e governança.

Os usuários finais quase não recebem treinamento, também o treinamento em segurança de TI está ausente. Os usuários finais não percebem os riscos à segurança da mesma maneira que os profissionais.



A segurança é geralmente considerada como um complemento opcional em vez de um requisito de design incorporado.

As partes interessadas não têm ideia de que prova precisam para decidir que os riscos de segurança da informação são gerenciados.

2.3 Responsabilidades na Garantia de Segurança pelos Prestador / Fornecedor de Serviços

Responsabilidades na Garantia de Segurança pelos Prestador / Fornecedor de Serviços

Os fornecedores precisam mostrar o devido cuidado com relação à segurança da informação

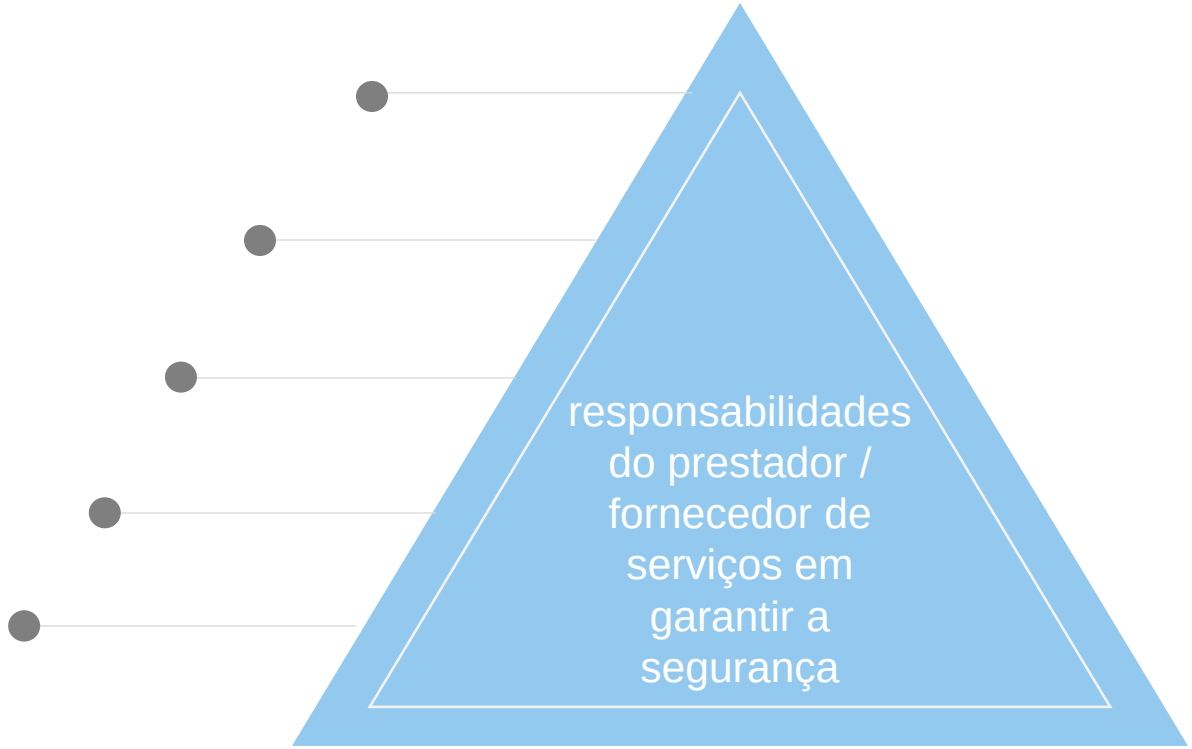
O uso de padrões de boas práticas prevalece

Gerenciamento de incidentes, mudanças e continuidade são processos-chave

O desempenho da segurança da informação precisa se tornar parte dos processos de gerenciamento do SLA

O monitoramento ativo e o gerenciamento de vulnerabilidades precisam de mais atenção

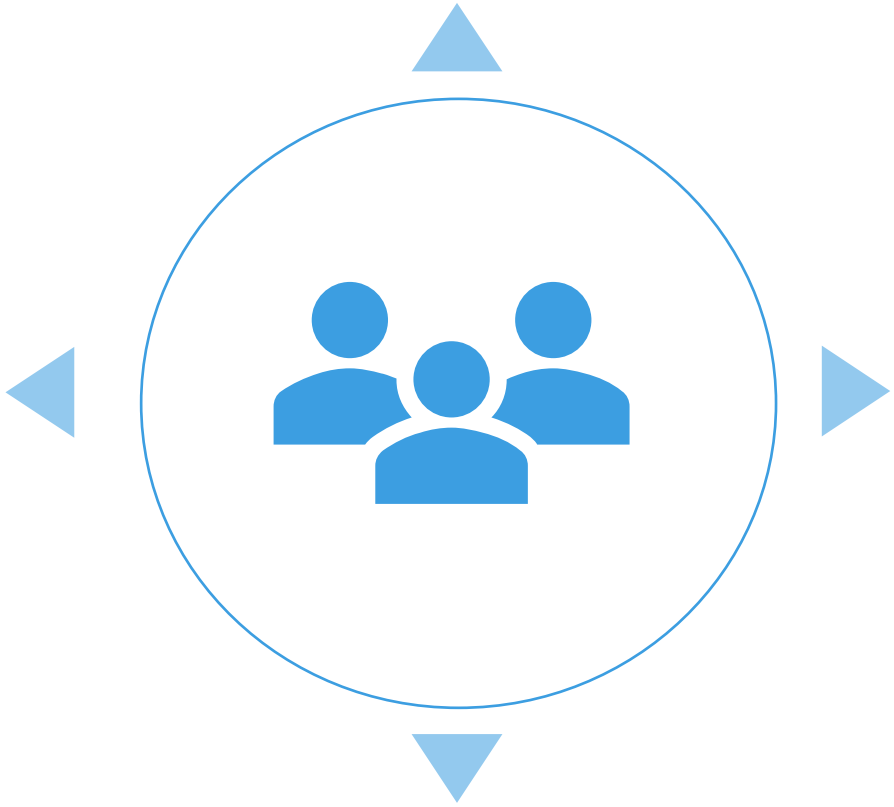
A transparência é fundamental, mas difícil de manter em um ambiente de serviço compartilhado



Responsabilidades na Garantia de Segurança pelos Prestador / Fornecedor de Serviços

Os provedores de serviços precisam entender os negócios e os requisitos de seus clientes.

O gerenciamento e a segurança de TI precisam ser implementados usando os padrões de melhores práticas, como os padrões ITIL, CobiT e ISO. Os indicadores de desempenho SMART são essenciais.

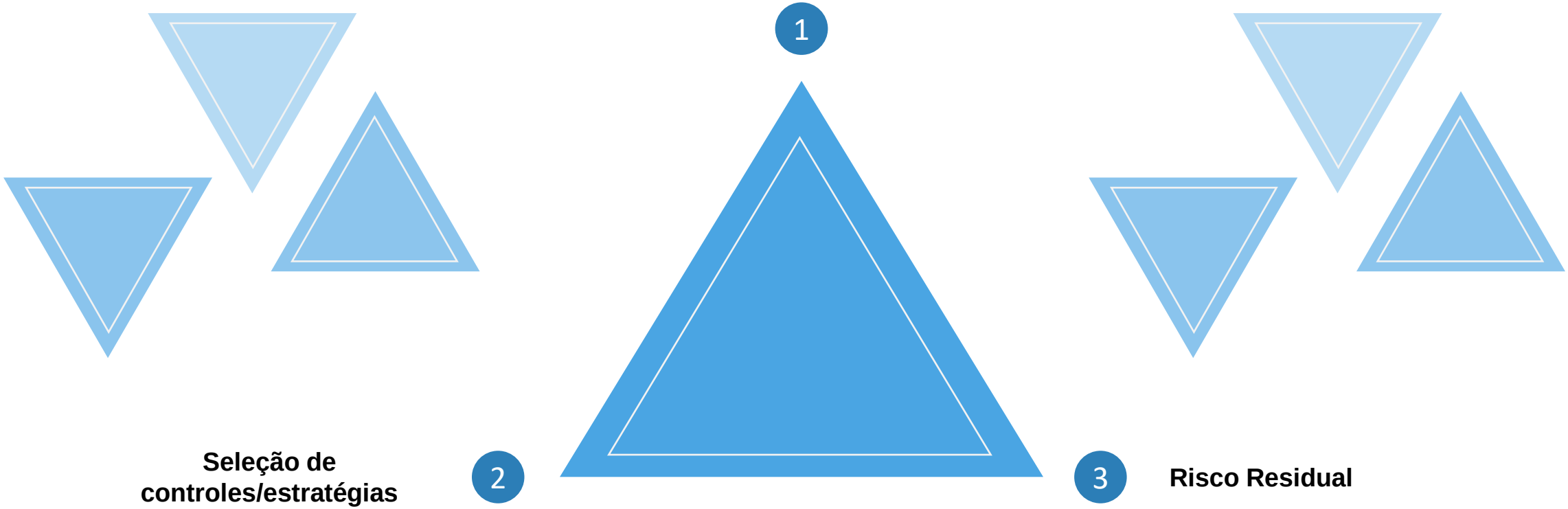


Os fornecedores nem sempre são transparentes sobre os riscos de segurança inerentes às soluções que eles fornecem; avaliação de terceiros desses riscos é vital.

A segurança do perímetro ainda é importante, mas a segurança dos dados ainda mais, isso requer uma mentalidade e produtos / soluções diferentes.

3. Gerenciamento de Riscos

Assuntos de Gerenciamento de Riscos



3.1. Princípios do Gerenciamento de Riscos

Gerenciamento de Riscos

A avaliação de riscos responde a uma série de perguntas

- Quais (ativos de informação) precisamos proteger?
- Por que precisamos proteger esses ativos?
- Quais são os riscos?
- Quais são as prioridades ao lidar com esses riscos?
- Quais são as opções para lidar com esses riscos?

Etapas nos processos de avaliação de risco

1 Ativos

- Determinar os ativos no escopo da avaliação
- Determinar quem são os proprietários desses ativos
- Discutir com esses proprietários as ameaças a esses ativos

2 Ameaças

- Decidir quem são os agentes de ameaça
- Obter opiniões de especialistas sobre vulnerabilidades desses ativos
- Obter opiniões de especialistas sobre as probabilidades de que as ameaças ocorram
- Obter opiniões de especialistas sobre impactos quando as ameaças ocorrerem
- Fazer um brainstorm com representantes de todas as partes interessadas

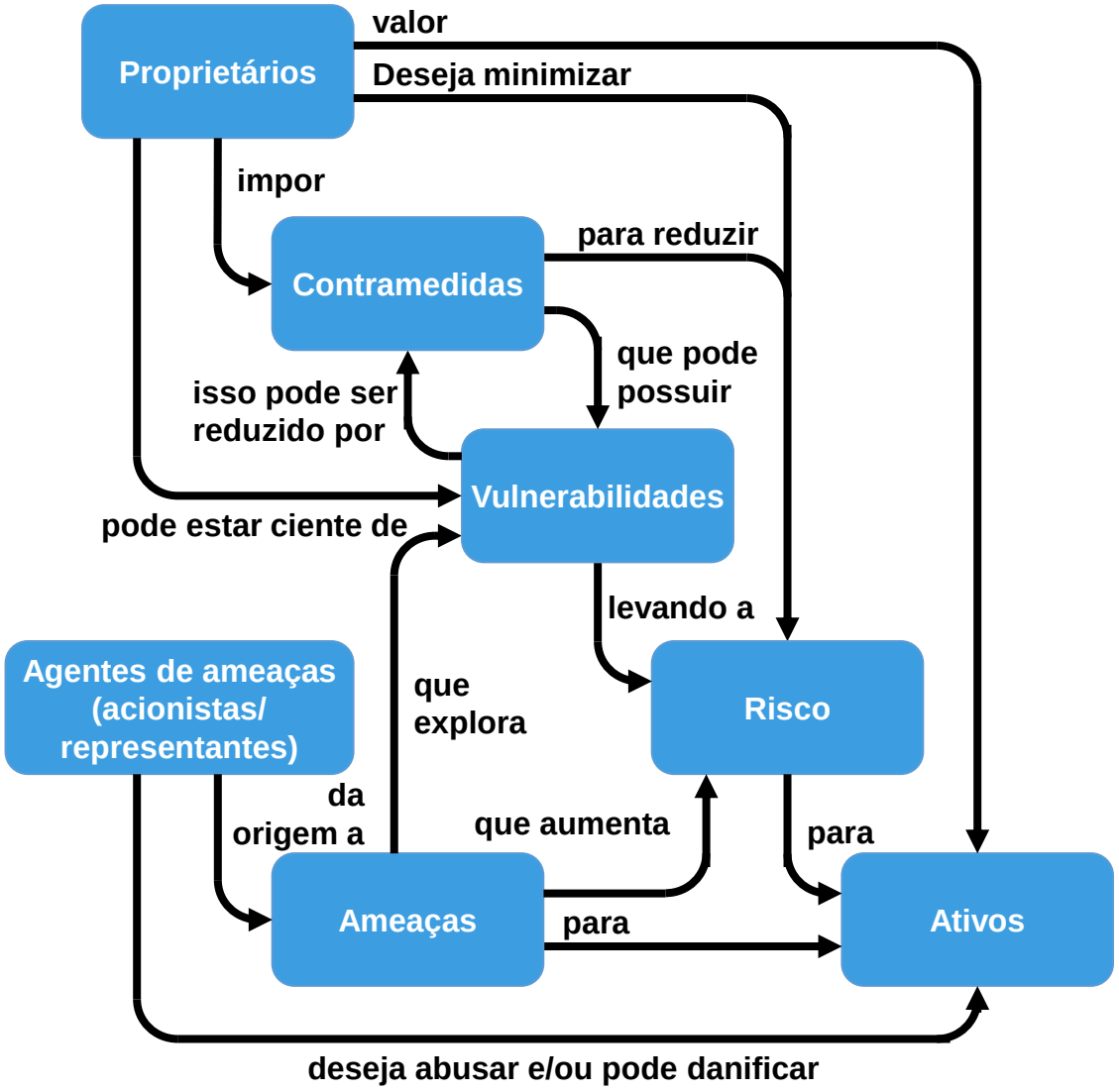
Riscos 3

- Definir algum tipo de fórmula para calcular a magnitude dos riscos
- Definir o apetite ao risco do(s) proprietário(s)
- Encontrar opções para mitigar riscos inaceitáveis

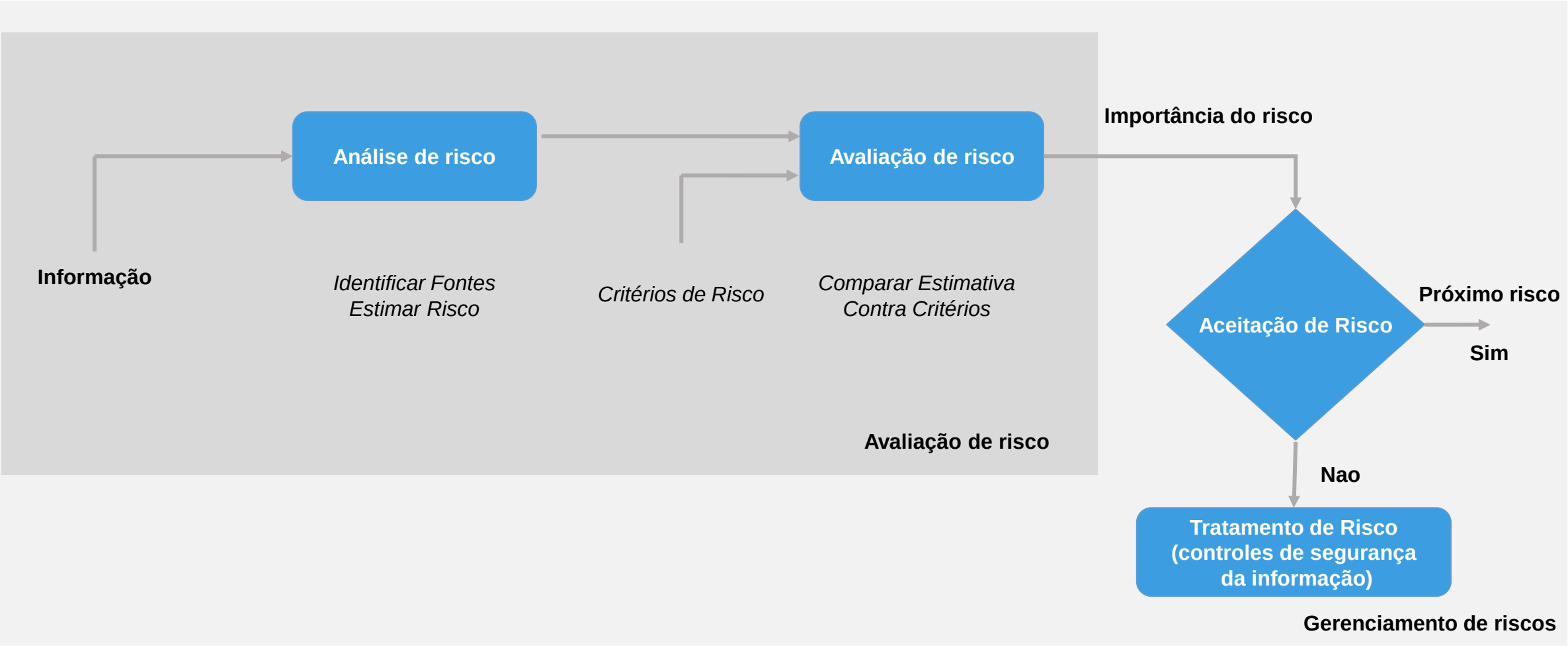
Controles 4

- Implementar controles
- Compreender e mitigar os novos riscos dos próprios controles
- Aceitar quaisquer riscos residuais e repitir todas as opções acima

Fluxo de trabalho genérico de avaliação de risco



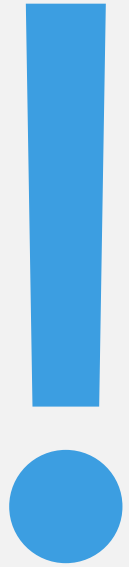
Gerenciamento de riscos de acordo com a ISO/IEC 27001/2



A ISO / IEC 27001 refere-se explicitamente e alinha-se com
ISO / IEC 31000 - Gerenciamento de riscos - Princípios e diretrizes

Avaliação de riscos - Pontos de atenção

- Produza uma Análise de Impacto nos Negócios primeiro para determinar onde é necessária uma avaliação de riscos
- Implemente uma linha de base (baseline) sobre os riscos. No entanto, os controles de mitigação de risco devem ser implementados somente quando necessário.
- Discuta os riscos que ainda não ocorreram. Precisa ter uma mente aberta
- A análise de riscos pode ser facilitada por um especialista, mas requer uma abordagem multidisciplinar com membros de todas as funções de negócios
- Existem amplas ferramentas disponíveis, mas as ferramentas podem apenas ajudar o processo; não realizá-lo!
- A avaliação de riscos fornecerá a direção na qual os controles devem ser implementados para lidar com os riscos enfrentados pela organização. Isso é essencial ao projetar um programa de segurança da informação em toda a empresa.
- A melhor maneira de alcançar um bom nível de eficácia na governança de segurança é executando uma avaliação periódica dos riscos como parte de um programa de gerenciamento de riscos.
- A organização não elevará os riscos a um nível 0. No entanto, as partes devem ser informadas sobre os riscos residuais e aceitá-lo de acordo com o apetite de risco da organização (a quantidade de risco que as organizações estão dispostas a aceitar ao avaliar as compensações entre segurança e acessibilidade ilimitada).



Análise de Impacto nos Negócios

Lida apenas com o impacto de um evento, como perda, dano ou divulgação de informações

Em termos comerciais, ou seja, perda financeira, danos à reputação, consequências legais etc.

Permite que um negócio identifique os processos em que a segurança é importante

Deve ser realizado junto com o(s) proprietário(s) do(s) negócio(s)

Não analisa ativos, ameaças, vulnerabilidades, probabilidades etc.; apenas o impacto dos eventos

Atua como um filtro de atividades onde uma avaliação de risco é necessária e onde não é

Princípio da Linha de Base (Baseline)

- **Implemente um conjunto limitado de controles para os ativos que fazem parte do escopo.**
- **Ser capaz de explicar e justificar por que é suficiente implementar apenas esses controles sobre esses ativos (ferramenta: análise de impacto nos negócios).**
- **Faça uma avaliação de risco em todos os outros ativos e implemente controles extras apenas quando necessário.**
- **Objetivos organizacionais, restrições operacionais e legislação e regulamentação aplicáveis sempre precisam ser levados em consideração ao implementar controles de risco.**
- **Representa a maneira de começar a definir os controles de segurança das informações da organização.**

3.2. Controlando os Riscos

Determinar quais ativos estão no escopo da avaliação

- **Objetivo:**

Determinar quais ativos serão avaliados nas próximas etapas.

- **Como:**

A análise de impacto nos negócios deixou claro quais processos levam ao maior impacto se ocorrer perda, dano ou divulgação. Os ativos dentro desses processos são pessoas, sistemas, aplicativos, sistemas operacionais, edifícios / salas, serviços públicos etc.

- **Diretrizes:**

Elabore a lista de ativos, mas mantenha um alto nível de abstração e agrupe os ativos sempre que possível.

Determinar quem são os proprietários desses ativos

- **Objetivo:**

Somente os proprietários podem discutir claramente o valor dos ativos.

- **Como:**

Principalmente a análise de impacto nos negócios já esclareceu quem são os proprietários.

- **Diretrizes:**

Determinar os proprietários de ativos compartilhados (como rede, infraestrutura de e-mail, acesso à Internet) pode ser complicado ... então o proprietário será o gerente responsável pela manutenção (delegada) desses ativos.

Discutir com esses proprietários as ameaças aos ativos

- **Objetivo:**

Para determinar quais ameaças são aplicáveis aos ativos dentro do escopo, apenas essas ameaças precisam ser analisadas nas próximas etapas.

- **Como:**

Existem listas padrão de ameaças, mas discuta com o proprietário se a lista está completa.

- **Diretrizes:**

Seja o mais completo possível, não filtre ameaças neste momento. Tente compilar uma lista de ameaças inerentes, não as ameaças para as quais existem riscos residuais no momento. Por exemplo, não cancele a ameaça de perda de dados porque os backups já foram feitos.

Decidir quem são os agentes de ameaça

- **Objetivo:**

Conhecer seu inimigo permite determinar melhor as probabilidades e vulnerabilidades das ameaças que ocorrem.

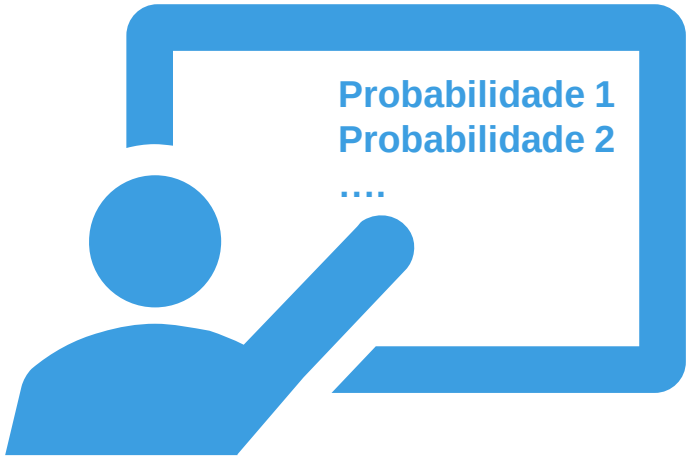
- **Como:**

Discuta quem pode estar interessado em atacar sua organização e os meios que esses adversários têm à sua disposição.

- **Diretrizes:**

Os adversários podem ser funcionários, criminosos, todos os tipos de hackers, concorrentes, estados, terroristas etc.

Obter opiniões de especialistas sobre as probabilidades de que as ameaças ocorram



- **Objetivo:**

Permitir que os presentes durante o workshop de avaliação de riscos tenham informações detalhadas suficientes para tomar decisões.

- **Como:**

Entrevistas com especialistas sobre aspectos de segurança da informação relevantes para os ativos no escopo, como especialistas técnicos e gerentes de instalações, mas também governo local, polícia, corpo de bombeiros, etc. Obter também informações públicas, quando disponíveis, de incidentes no passado, dentro e fora da empresa.

- **Diretrizes:**

Os dados obtidos precisam ser qualificados em termos de alta/média/baixa vulnerabilidade. Tente ser exaustivo. Converse com o maior número possível de especialistas dentro do escopo e do orçamento.

Obter opiniões de especialistas sobre vulnerabilidades dos ativos

- **Objetivo:**

Permitir que os presentes durante o workshop de avaliação de riscos tenham informações detalhadas suficientes para tomar decisões.

- **Como:**

Entrevistas com especialistas sobre aspectos de segurança da informação relevantes para os ativos no escopo, como especialistas técnicos e gerentes de instalações, mas também governo local, polícia, brigada de incêndio etc.

- **Diretrizes:**

Os dados obtidos precisam ser qualificados em termos de alta/média/baixa vulnerabilidade. Tente ser exaustivo. Converse com o maior número possível de especialistas dentro do escopo e do orçamento.

Definir o impacto para todas as ameaças quando elas ocorrerem

- **Objetivo:**

Permitir que os presentes durante o workshop de avaliação de riscos tenham informações detalhadas suficientes para tomar decisões.

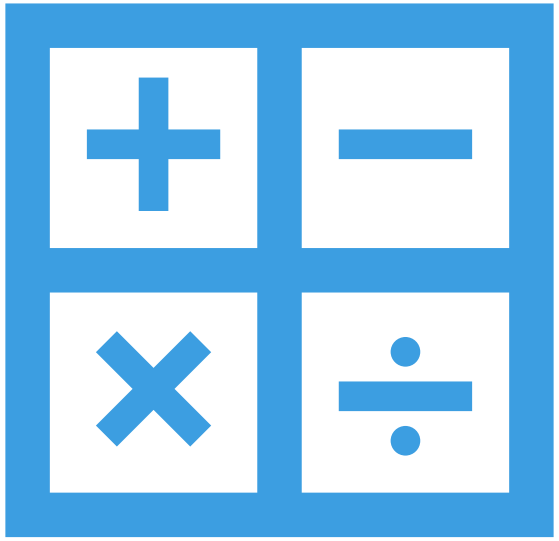
- **Como:**

Para cada ameaça, discuta com especialistas qual seria o impacto máximo quando a ameaça ocorrer.

- **Diretrizes:**

É difícil considerar impactos quando uma ameaça nunca ocorreu antes. Considere perdas monetárias, problemas legais, perda de negócios, vantagens para um concorrente, perda de imagem etc. Se possível, classifique todas as perdas possíveis em termos financeiros.

Definir uma fórmula para calcular o risco



- **Objetivo:**

Reunir todas as informações sobre uma ameaça em um parâmetro quantitativo ou qualitativo que permita decidir se o risco está acima ou abaixo do nível de risco aceitável.

- **Como:**
  - **Quantitativo**: quando apenas números são usados para calcular o risco
  - **Qualitativo:** Ao usar classes de risco, por exemplo, BBM (Baixa probabilidade, Baixa vulnerabilidade, Médio impacto) ou quantificar (B = 1, M = 2, A = 3) e depois multiplicar (BBM = 1 * 1 * 3 = 3) ou use alguma outra fórmula. (metodologia de risco mais aceita).

- **Diretrizes:**

Tome cuidado, quando relevante, ao quantificar para não perder a distinção entre, por exemplo, BBM e MBB (ambos são 3).

Definir o apetite ao risco do(s) proprietário(s)

- **Objetivo:**

Determinar o nível acima do qual um risco é inaceitável (ou seja, deve ser mitigado sempre que possível).

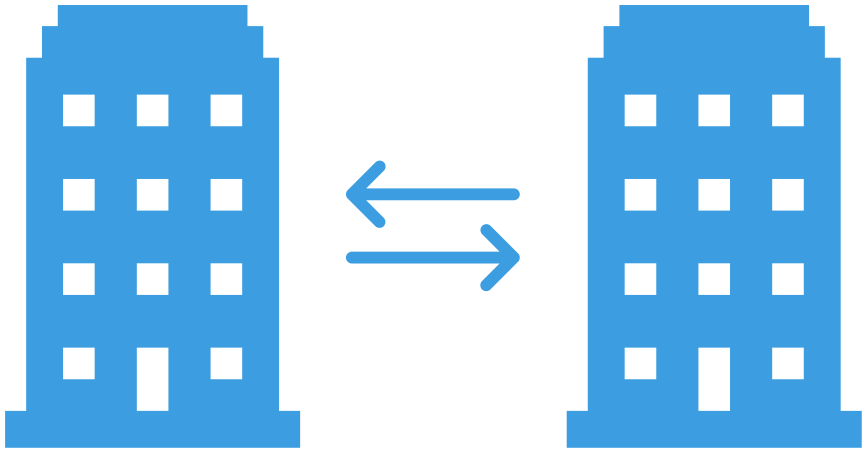
- **Como:**

Para cada ameaça ou para todas as ameaças de uma só vez, peça ao proprietário do processo que decida qual nível de risco é inaceitável.

- **Diretrizes:**

Tenha também uma visão externa; o que os clientes/fornecedores considerariam aceitável? O que as entidades legais considerariam aceitáveis?

Encontre opções para mitigar riscos inaceitáveis



- **Objetivo:**

Selecionar os riscos para os quais os controles mitigadores são necessários.

- **Como:**

Decida se um risco pode ser evitado, transferido para outra parte, aceito ou se precisa ser mitigado.

- **Diretrizes:**

Evitar, por exemplo, significa cancelar o processo de negócios em questão ou mover a organização para uma área menos arriscada. A transferência de um risco pode ser feita com um seguro contra ele. Ambas as ações tendem a ser exceções, levando a discussões apenas para decidir se um risco pode ser aceito ou se precisa ser mitigado.

Implementando controles

- **Objetivo:**

Para os riscos que não podem ser aceitos, é necessário selecionar e implementar controles que reduzam a probabilidade, a vulnerabilidade e/ou o impacto.

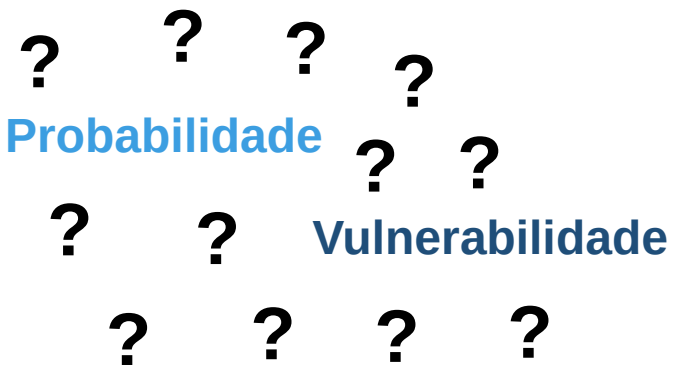
- **Como:**

Use um conjunto de controles padrão de boas práticas de linha de base, como ISO/IEC 27002, e selecione os controles que atenuam o risco.

- **Diretrizes:**

Se e quais controles atenuam um risco, são necessários conhecimentos sobre, por exemplo, aspectos técnicos, legais, processuais, físicos/de instalações. Verifique se a visão especializada sobre todos esses aspectos está disponível.

Observações



Nem sempre a distinção entre probabilidade e vulnerabilidade é clara.

Exemplo:

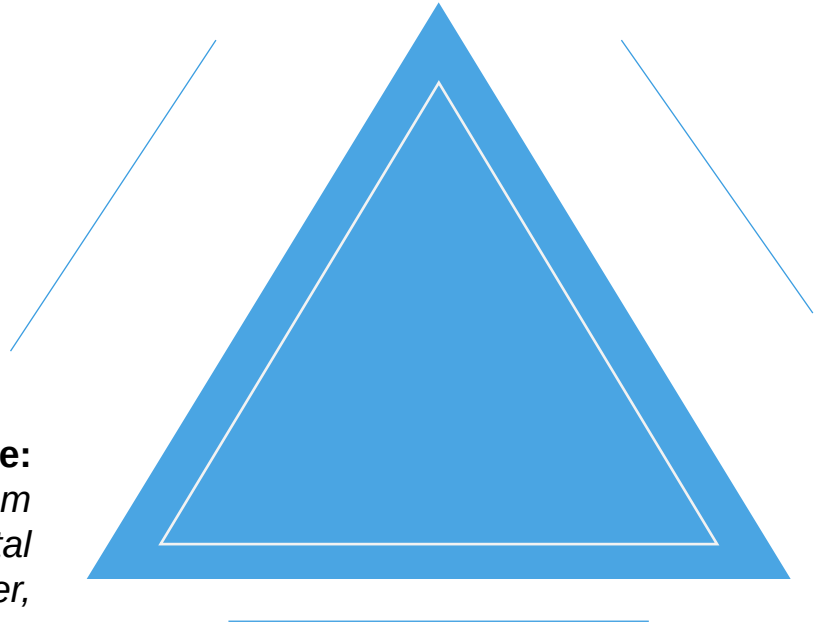
- Imagine duas casas próximas a uma fábrica de produtos químicos. Uma explosão na fábrica causa incêndios em seu entorno. Ambas as casas têm a mesma probabilidade de incêndio causada pelo problema naquela fábrica. Ambas as casas têm a mesma probabilidade de incêndio causada pelo problema naquela fábrica.

- Mas se uma dessas casas é feita de madeira e a outra de tijolo, a casa de madeira tem uma vulnerabilidade muito maior ao fogo. Como a vulnerabilidade é difícil de determinar, limite o número de classes a (por exemplo) apenas alta ou baixa vulnerabilidade.

Observações

Antes de fazer uma avaliação de risco, chegue a um consenso sobre as classes quanto à probabilidade, vulnerabilidade e impactos. Por exemplo:

Impacto:
alta: pode levar à falência
média: afeta os resultados
baixa: sem impacto

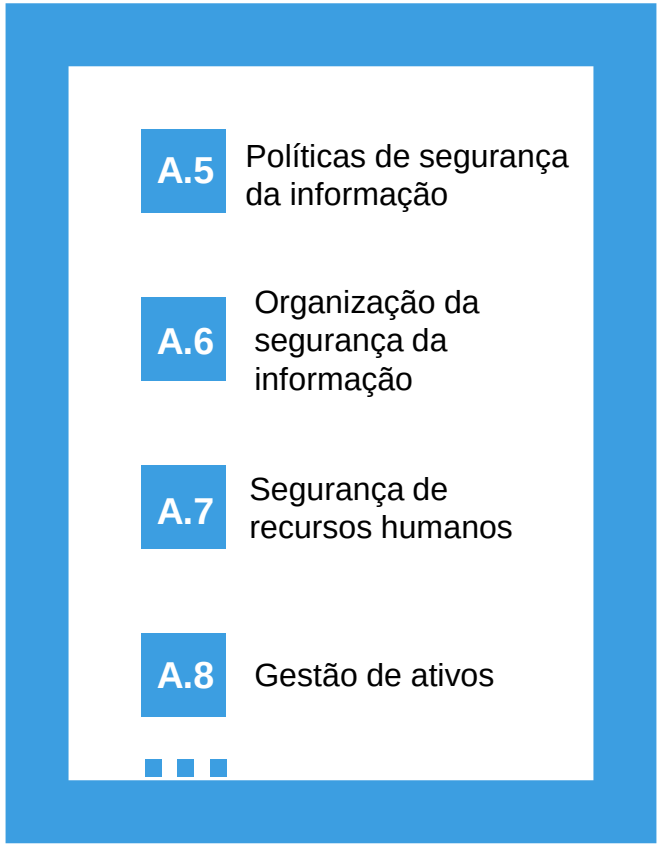


Vulnerabilidade:
alta: quando isso acontece, há um impacto total
baixa: quando isso acontecer, haverá um impacto menor

Probabilidade:
alta: isso pode acontecer a qualquer dia
média: poderia acontecer anualmente
baixa: nunca vai acontecer

Observações

Você pode usar os controles disponíveis na ISO 27001 e na ISO 27002 para outras decisões nas atividades de mitigação de riscos



Declaração de Aplicabilidade (SoA)

- A Declaração de aplicabilidade é um documento que deve ser produzido como resultado do processo de avaliação de risco.
- O documento pode assumir uma forma matricial, listando os controles de segurança da informação usados (para mitigar e/ou minimizar os riscos), as opções de tratamento e, geralmente, também os responsáveis por eles.
- Este documento será necessário durante as atividades de auditoria para fornecer uma boa visão de quais controles foram implementados no escopo do SGSI.
  - Auditoria interna: a auditoria interna será realizada pelos auditores internos da organização, que também têm a responsabilidade de verificar a conformidade da organização (de acordo com o escopo do SGSI) com a Política de Segurança da Informação.
  - Auditoria externa: A auditoria externa será realizada por uma terceira parte e independente, que também avaliará as documentações, processos e políticas, que incluem a Declaração de Aplicabilidade (SoA).

3.3. Riscos Residuais

Compreender e mitigar os novos riscos dos próprios controles

- **Objetivo:**

Determinar se os controles selecionados para mitigar os riscos inaceitáveis introduzem novos riscos**.**

- **Como:**

Discuta com especialistas as implicações dos controles selecionados. Encontre estratégias de mitigação quando novos riscos forem encontrados.

- **Diretrizes:**

Um exemplo pode ser o gerenciamento de chaves; bloqueios físicos ou chaves eletrônicas (senhas/certificados) apresentam todos os tipos de novos problemas (gerenciamento de chaves, perda de chaves, revogação de chaves etc.) que precisam ser entendidos e mitigados.

Aceite quaisquer riscos residuais e repetidos

- **Objetivo:**

Aceitar formalmente os riscos residuais e incorporar esse processo.

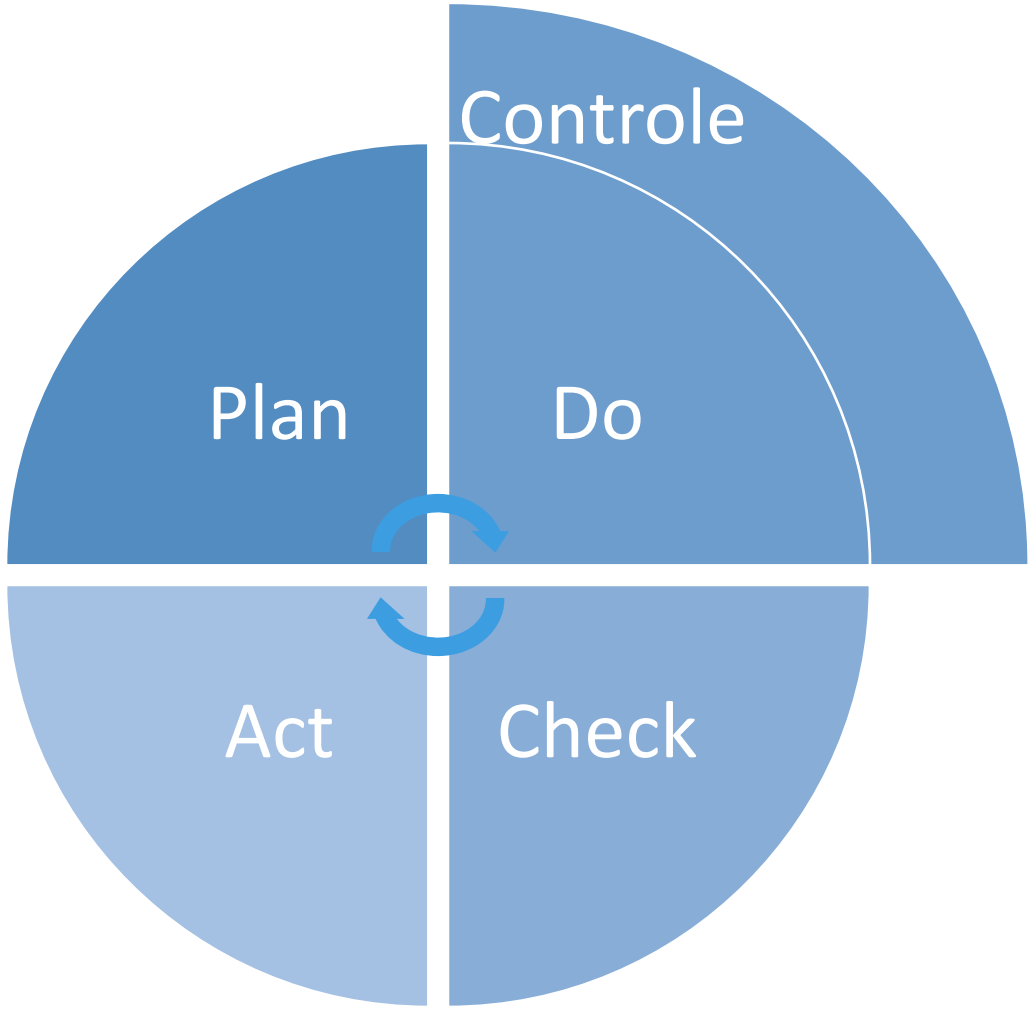
- **Como:**

Faça com que a gerência documente o fato de que existem riscos residuais, mas que podem ou devem ser aceitos. Incorpore esse processo de gerenciamento de riscos ao sistema de gerenciamento, talvez com base na ISO/IEC 27001 ou mesmo na ISO 9001 (qualidade) ou na ISO/IEC 20000 (gerenciamento de TI).

- **Diretrizes**:

Esse processo de gerenciamento de riscos deve estar vinculado ao processo de gerenciamento de incidentes e ao processo de gerenciamento de mudanças. Isso garante que novas ameaças serão consideradas e atenuadas quando necessário**.**

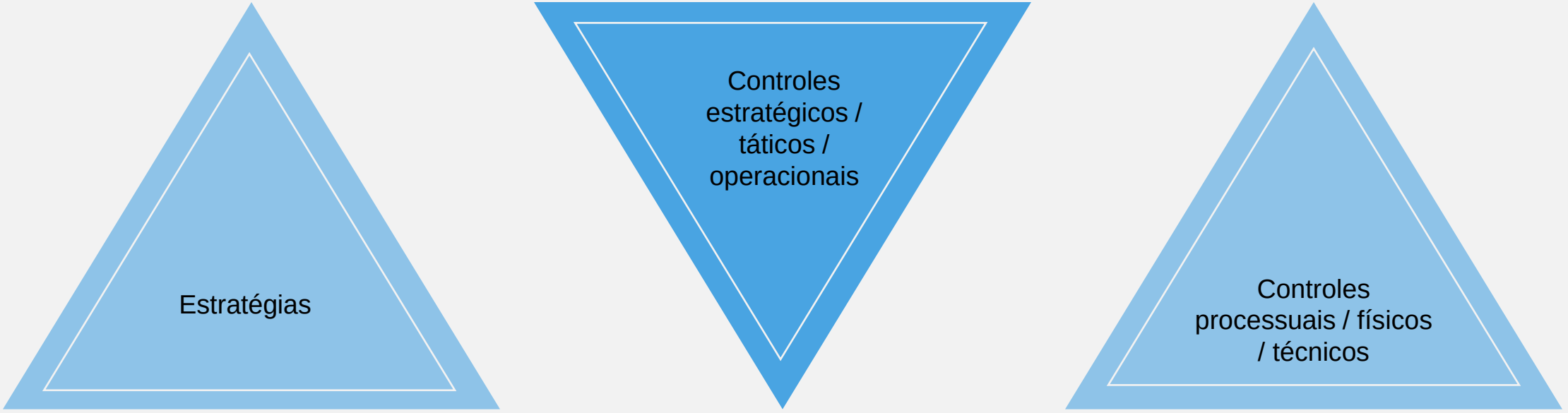
PDCA



- A ISO/IEC 27001 e outras normas para sistemas de gerenciamento (ISO 9001 e CobiT, por exemplo) descrevem o gerenciamento de riscos à segurança da informação em termos do ciclo de PDCA: planejamento/execução/verificação/ação (Deming).
- Pense bem no que é necessário, levando em consideração políticas, avaliação de riscos e gerenciamento (por exemplo, Plan). Em seguida, implemente o que é necessário (procedimentos, controles etc.) e meça o desempenho (por exemplo, Do) e periodicamente - quantas vezes for necessário para garantir que os riscos sejam atenuados - audite/revise tudo (por exemplo, verifique - Check). Por fim, todas as melhorias possíveis devem ser consideradas novamente (por exemplo, Act) e levar a novos planos.
- A segurança da informação geralmente adiciona a função Controle no modelo PDCA.

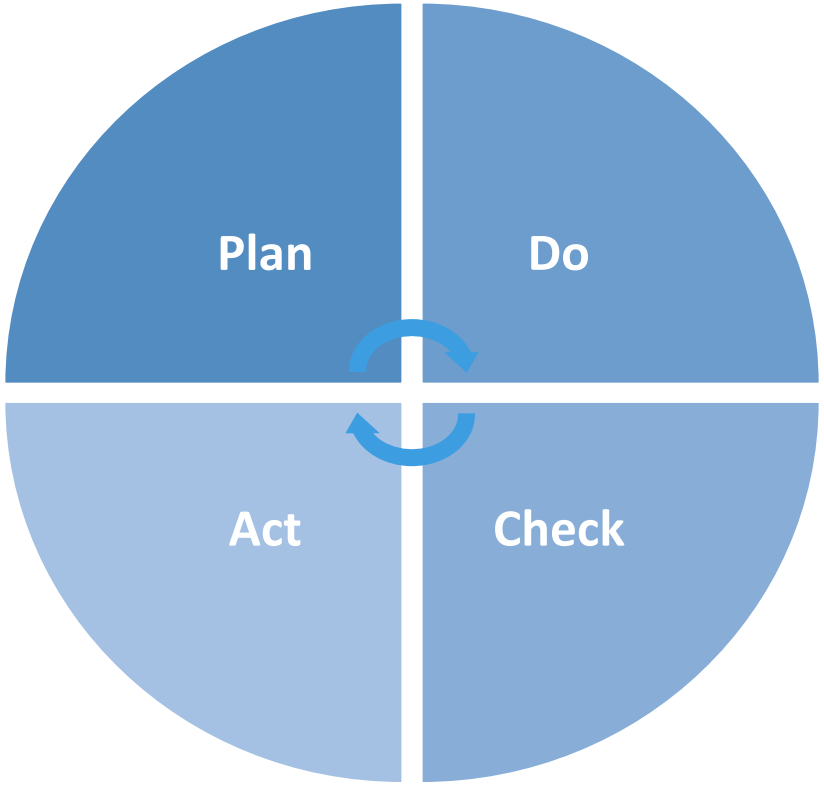
4. Controles de Segurança da Informação

Controles de Segurança da Informação



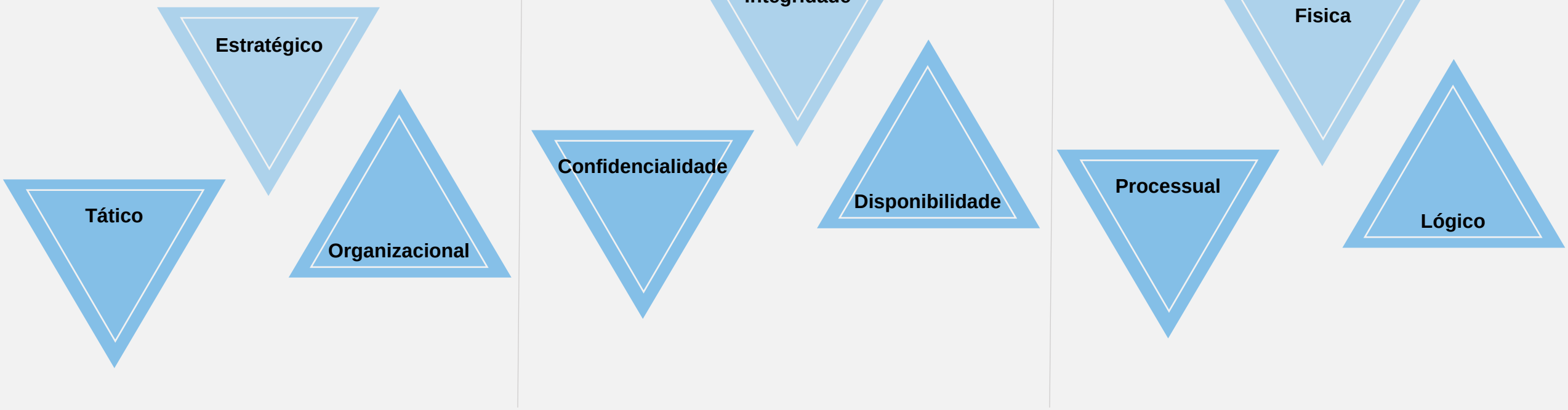
Estratégias

A Segurança da Informação só pode ser aprimorada com a implementação de controles, ou seja, as atividades PLAN do ciclo PDCA são as mais importantes. Não obstante, **implementar os controles certos é crucial** e testar se eles realmente funcionam (ou seja, mitigar riscos) é ainda mais importante.



- **Portanto, parece haver várias opções (estratégias) para melhorar a segurança da informação:**
  - Foco no **'planejar'** (descrevendo os controles planejados);
  - Foco no **'fazer';**
  - Foco no **'checar/agir'** (melhoria continua).

Tríades nos controles



Uma boa mistura de controles

- Atenua os aspectos relevantes da CID
- Nos três níveis hierárquicos
- Leva em consideração a proteção lógica (TIC) e a proteção física
- Está incorporado e documentado

- **Observações importantes:**
  - O comprometimento da gerência e o controle tático é mais importante.
  - Os controles operacionais realmente melhoram a segurança.
  - Se um risco puder ser mitigado por um controle físico, isso é preferido acima da lógica (os controles físicos podem ser auditados com muito mais facilidade).
  - Se um risco pode ser mitigado por um controle lógico, isso é preferível a procedimentos (as pessoas cometem erros, um controle lógico atua como uma rede de segurança).

Visão geral da ISO 27001

Norma ISO 27001

O padrão ISO 27001 representa o padrão global para o estabelecimento de um Sistema de Gerenciamento de Segurança da Informação. A última versão publicada aconteceu em 2013 pela Organização Internacional de Normalização. O padrão é usado em todo o mundo por organizações que desejam implementar a Segurança da Informação com base em um padrão Global.

Estrutura da ISO 27001

- **0 Introdução -** descrição do processo de gerenciamento de riscos à informação.
- **1 Escopo -** descrição dos requisitos genéricos de um SGSI adequados para qualquer tamanho ou tipo de organização.
- **2 Referências normativas -** descrição de outros padrões ISO que podem ser adequados ao assunto.
- **3 Termos e definições -** descrição dos principais termos e definições usados pela ISO 27001.
- **4 Contexto da organização -** descrição de como as organizações devem olhar para o seu próprio contexto, a fim de definir um bom escopo para o SGSI, gerenciar as expectativas das partes interessadas e os principais itens que devem ser estabelecidos, implementados, mantidos e aprimorados continuamente ”no SGSI.
- **5 Liderança -** descrição da função e responsabilidades da Alta Administração em relação ao SGSI, além de definir as principais funções de segurança da informação.
- **6 Planejamento -** descrição das ações que devem ser tomadas para identificar, analisar e planejar o tratamento de riscos às informações. Uma descrição e definição dos objetivos de Segurança da Informação também devem ocorrer.
- **7 Suporte -** descrição das ações que devem ser tomadas para: atribuir recursos adequados e competentes, criar e desenvolver conscientização sobre segurança da informação, preparar, publicar e controlar os processos, políticas e procedimentos necessários.
- **8 Operação -** descrição de ações detalhadas para avaliar e tratar riscos à segurança da informação, gerenciamento de alterações e documentos (registros para facilitar as atividades de auditoria).
- **9 Avaliação de desempenho -** descrição das ações que devem ser tomadas para: monitorar, medir, analisar e avaliar/auditar/revisar os controles, processos e sistema de gerenciamento de segurança da informação, aprimorando sistematicamente quando necessário.
- **10 Melhoria -** descrição das ações que devem ser tomadas para melhorar continuamente o SGSI, com base em constatações de auditoria, análises críticas da gerência, contribuições dos clientes, entre outras.
- **Anexo A Objetivos e controles de controle de referência** - descrição dos principais controles de segurança da informação que devem ser adotados pelas organizações. Os controles selecionados e utilizados, bem como os não utilizados, devem ser descritos no documento Declaração de Aplicabilidade (SoA).

Caminho de Certificação ISO 27001 (visão geral)

A implementação e certificação do SGSI **podem diferir de organização para organização.** No entanto, essas são as etapas mais comuns.

1. Obter compromisso da gestão
2. Definir escopo e contexto do SGSI
3. Planejar o projeto
4. Objetivos do SGSI e sistema geral de gerenciamento
5. Política de segurança da informação
6. Avaliação de risco
7. Declaração de aplicabilidade (SoA)
8. Implementar controles
9. Auditoria interna
10. Revisão de gerenciamento
11. Auditoria externa, estágio um
12. Auditoria externa, estágio dois (certificação)

ISO/IEC 27002:2013

- Esta prática recomendada contém 114 controles
- Agrupados em 35 objetivos de controle
- Agrupados em 14 capítulos
- Cada controle possui aspectos procedimentais, técnicos e, às vezes, físicos
- Apenas um conjunto limitado de controles lida com aspectos humanos e continuidade

Capítulos da ISO/IEC 27002

5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança de recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e ambiental
12. Operações de Segurança
13. Segurança das comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relações com fornecedores
16. Gerenciamento de incidentes de segurança da informação
17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios
18. Conformidade

Capítulos ISO/IEC 27002 - Estratégico

Estratégico

5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança de recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e ambiental
12. Operações de Segurança
13. Segurança das comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relações com fornecedores
16. Gerenciamento de incidentes de segurança da informação
17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios
18. Conformidade

Tático

5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança de recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e ambiental
12. Operações de Segurança
13. Segurança das comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relações com fornecedores
16. Gerenciamento de incidentes de segurança da informação
17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios
18. Conformidade

Operacional

5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança de recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e ambiental
12. Operações de Segurança
13. Segurança das comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relações com fornecedores
16. Gerenciamento de incidentes de segurança da informação
17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios
18. Conformidade

Controles estratégicos

Estratégico

5. **Políticas de segurança da informação**
6. Organização da segurança da informação
7. Segurança de recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e ambiental
12. Operações de Segurança
13. Segurança das comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relações com fornecedores
16. Gerenciamento de incidentes de segurança da informação
17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios
18. **Conformidade**

- Sistema de Gerenciamento de Segurança da Informação
- Alocação de recursos (competentes)
- Governança
  - Liderança
  - Delegando responsabilidades para baixo
  - Gerenciar com base em relatórios para cima
- Gerenciamento de riscos
- Definindo uma política de alto nível
- Iniciar auditorias, ou seja, monitoramento de conformidade

Controles táticos

Tático

5. Políticas de segurança da informação
6. **Organização da segurança da informação**
7. **Segurança de recursos humanos**
8. **Gestão de ativos**
9. **Controle de acesso**
10. Criptografia
11. Segurança física e ambiental
12. Operações de Segurança
13. Segurança das comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. **Relações com fornecedores**
16. **Gerenciamento de incidentes de segurança da informação**
17. **Aspectos de segurança da informação do gerenciamento de continuidade de negócios**
18. Conformidade

- Atribuindo responsabilidades
- Treinamento, conscientização
- Gerenciamento de ativos, classificação
- Gerenciamento de direitos de acesso
- Gerenciamento de relacionamento com fornecedores
- Gerenciamento de incidentes, melhoria
- Aspectos de segurança da continuidade de negócios

Controles operacionais

Operacional

5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança de recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. **Criptografia**
11. **Segurança física e ambiental**
12. **Operações de Segurança**
13. **Segurança das comunicações**
14. **Aquisição, desenvolvimento e manutenção de sistemas**
15. Relações com fornecedores
16. Gerenciamento de incidentes de segurança da informação
17. Aspectos de segurança da informação do gerenciamento de continuidade de negócios
18. Conformidade

- Proteção física
- Aspectos de segurança dos processos de gerenciamento de TI:
  - Gerenciamento de capacidade
  - Gerenciamento de mudança
  - Gerenciamento de incidentes/problemas
  - Gerenciamento de segurança (ou seja, firewall, acesso ...)
- Segurança no ambiente de desenvolvimento/teste/produção

4.1. Controles Organizacionais

Procedimento e Processo (definição da ISO 9001)

Procedimento

Maneira especificada de realizar uma atividade ou um processo. **Os procedimentos podem ser documentados ou não.** Quando um procedimento é documentado, o termo “procedimento escrito” ou “procedimento documentado” é frequentemente usado. O documento que contém um procedimento pode ser chamado de documento de procedimento.

Processo

Um conjunto de **atividades inter-relacionadas ou de interação que transforma entradas em saídas**.

Orientação para procedimentos

Desenvolva procedimentos documentados apenas onde houver um benefício real, por exemplo:

- Quando as atividades são realizadas sob estresse (durante incidentes, por exemplo)
- Quando os funcionários que normalmente executam as atividades podem não estar disponíveis
- Quando as atividades são complexas e os erros levam a resultados desastrosos

Os procedimentos devem ser breves e relevantes e conter representações visuais das atividades sempre que possível.

Se as atividades são realizadas por funcionários com conhecimento, elas não devem ser descritas em detalhes.

Um meta-procedimento deve descrever como os procedimentos são elaborados e como funcionam os processos de aprovação, auditoria, manutenção de documentos etc.

Exemplos de controles processuais

5.1

Política de segurança da informação
Um documento que ajuda todos os funcionários a entender por que a segurança das informações é importante e qual é sua função.

6.1

Organização interna
Descreve a organização de segurança, os acordos de confidencialidade e como lidar com as partes relevantes.

8.1

Responsabilidade pelos ativos
Procedimentos para o inventário, propriedade e uso de ativos.

8.2

Classificação da informação
Procedimentos para a classificação de tipos de informações e o manuseio correto desses vários tipos.

12.1

Procedimentos e responsabilidades operacionais
Todos os procedimentos do dia-a-dia para gerenciamento de informações (principalmente sobre gerenciamento ds TIC), procedimentos para separação de tarefas e desenvolvimento, teste e operação.

15.1

Relações com fornecedores
Identificação de riscos ao lidar com partes externas (fornecedores, clientes etc.) e incluí-los em contratos.

Nota: nem todos os controles ISO/IEC 27002 estão incluídos; Esta lista não é exaustiva, os números se referem à ISO 27002

Lista de políticas e procedimentos - ISO / IEC 27002

Políticas

Política de segurança da informação
Política de controle de acesso
Política de classificação da informação
Política de dispositivo móvel
Política de teletrabalho
Uso de redes e serviços de rede
Política de uso de controles criptográficos
Política para chaves criptográficas
Política de mesa limpa e tela limpa
Política que proíbe o uso de software não autorizado
Política de backup
Política de retenção de registros
Política sobre quais tipos de usuários de software podem instalar
Política para uso aceitável das instalações de comunicação
Política de desenvolvimento seguro
Política de segurança da informação para relacionamentos com fornecedores
Política de conformidade de DPI
Política para manter as condições de licença
Política de descarte ou transferência de software
Política de proteção de dados de privacidade

Procedimentos

Procedimentos para contatos com autoridades
Procedimento para casos de roubo ou perda de dispositivos móveis
Procedimentos para evitar disputas. Direitos de DPI
Procedimentos para backup e continuidade de negócios
Procedimentos para triagem
Procedimentos sobre planejamento, relatórios, registro em log de incidentes de segurança da informação, tratamento de evidências forenses, avaliação e resposta
Procedimentos para rotular / manusear informações
Procedimentos para lidar com ativos, mídia
Procedimentos para descarte de mídia
Procedimentos para transferência física de mídia
Procedimentos de autorização (verificação de identidade)
Procedimentos para proteger o acesso a conexões / serviços de rede
Procedimentos para impedir o uso não autorizado de IDs de administração
Procedimentos de login seguro
Procedimentos de autorização para programas utilitários
Procedimentos para acessar o código-fonte / bibliotecas do programa
Procedimentos de controle de alterações
Procedimentos de gerenciamento de chaves
Procedimentos para trabalhar em áreas seguras
Procedimentos para proteger equipamentos não assistidos
Procedimentos operacionais
Procedimentos de reinicialização e recuperação
Procedimentos de monitoramento
Procedimentos para lidar com a proteção contra malware
Procedimentos de backup e restauração
Procedimentos para instalação de software em sistemas operacionais
Procedimentos de resposta a incidentes de informação
Procedimentos para o gerenciamento de equipamentos de rede
Procedimentos de transferência de informações
Procedimentos para garantir rastreabilidade e não repúdio
Procedimentos de controle de alterações do sistema
Procedimentos para controle e integridade de aplicativos
Procedimentos de engenharia de sistema seguros
Procedimentos de desenvolvimento seguro
Procedimentos para a proteção de dados de teste
Procedimentos para monitorar a aderência às políticas por fornecedores
Procedimentos para garantir o nível de continuidade necessário para a segurança
Procedimentos para garantir a conformidade
Procedimentos de armazenamento e manuseio (para proteção de registros)
Procedimentos para proteção da privacidade

Baseline de Controles Processuais

Política de Segurança da Informação e seu processo de revisão

Compromisso da gestão

Gerenciamento de ativos, incluindo classificação de ativos/informações

Procedimentos de gestão de mudança

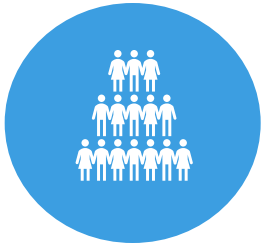
Segregação de deveres (funções)

Programa e política de controle de acesso e seu processo de revisão

Procedimentos de gerenciamento de incidentes

Identificação da legislação aplicável

Proteção dos direitos de propriedade intelectual



Proteção de dados e privacidade de informações pessoais

Classificação

Escopo

- Proteja apenas o necessário (de acordo com o escopo do SGSI).
- Para pensar: Como adicionar consistentemente uma etiqueta aos documentos impressos ... por exemplo, a uma mensagem de e-mail impressa?

Proprietários de ativos

- Permita que os proprietários do ativo classifiquem as informações com base no impacto de perda, dano e/ou divulgação.

Marcação (rótulo)

- Adicione um rótulo correspondente às informações, por exemplo: secreto, confidencial ou público.
- Os documentos classificados só podem ser acessados por pessoas habilitadas para esse nível ou superior.

Controles/Políticas

- Ter regras para lidar com esses rótulos; por exemplo, informações secretas devem ser criptografadas e transportadas pelo serviço de correio.

Orientação para Procedimentos

Procedimentos de gerenciamento de incidentes
Eles descrevem como os incidentes são gerenciados, ou seja, caminhos de escalação, quem é responsável, como os incidentes são resolvidos, quem deve ser informado e como a organização aprende com os incidentes.

Procedimentos de gerenciamento de mudanças
Eles descrevem como as mudanças (da TI) são definidas, como os riscos são mitigados, quem aprova e como as mudanças são controladas.

Procedimentos de gerenciamento de continuidade
Eles descrevem as ações, responsabilidades e caminhos de escalada de grandes incidentes (que podem levar a uma situação de crise) necessários para impedir que a organização falhe em circunstâncias incomuns nos negócios.

4.2. Controles Físicos

Exemplos de controles físicos (1/2)

11.1.1 Perímetro de segurança física
Dividir a(s) área(s) física(s) em zonas e marcar claramente essas zonas.

11.1.2 Controles físicos de entrada
Fechaduras, chaves, sistemas de entrada eletrônica controlados por chaves, crachás, biometria etc.

Nota: nem todos os controles ISO/IEC 27002 estão incluídos; Esta lista não é exaustiva, os números se referem à ISO 27002

Exemplos de controles físicos (2/2)

11.1.5 Trabalhando em áreas seguras

Procedimentos que descrevem as condições para trabalhar na área protegida. Por exemplo, especificando que nessa área ninguém pode trabalhar sozinho.

11.2.2 Utilidades

Proteção contra perda de utilidades (refrigeração, energia, gás, água). Descreve a necessidade de fontes de alimentação ininterruptas e sistemas nobreak.

11.2.7 Eliminação segura ou reutilização de equipamentos

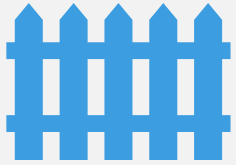
Procedimentos e ferramentas técnicas para descarte seguro de mídia (papel, discos) contendo informações classificadas.

Nota: nem todos os controles ISO/IEC 27002 estão incluídos; Esta lista não é exaustiva, os números se referem à ISO 27002

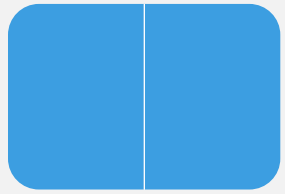
Proteção de perímetro

Alguns exemplos de proteção de perímetro

Paisagismo



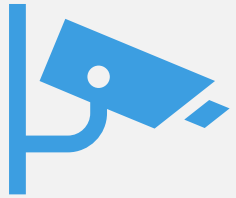
Cercas



Portões

Postes ou Pilares

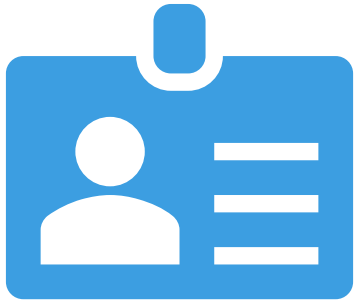
Perímetro de IDS (Intrusion Detection System)



CCTV

Controle de acesso e biometria

Controle de acesso



Identificação (quem é você)

- Algo que você tem (crachá, chave ...)
- Algo que você sabe (pin, senha ...)
- Algo que você é (impressão digital, digitalização de íris ...)

Autorização (que direitos você possui)

- Com base nas listas de identidade e controle de acesso (ACL), seu acesso será controlado

Biometria

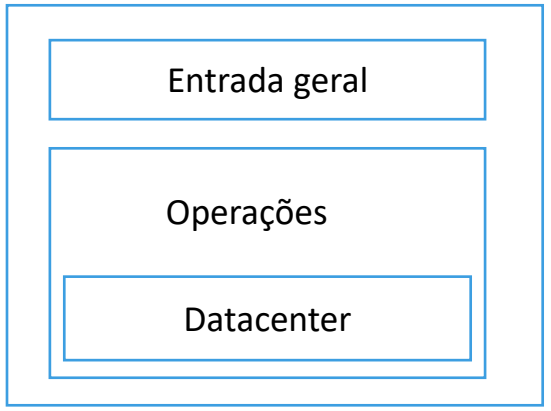
Biometrias

- Falso positivo (tipo I)
- Falso negativo (tipo II)

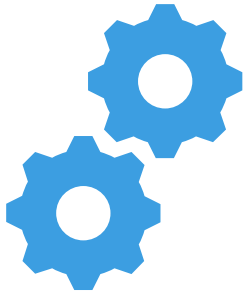
Orientação para controles físicos 1/2

Verifique a legislação quando instalar câmeras de vigilância e outros equipamentos sensíveis à privacidade.

O gerenciamento de direitos de acesso precisa de uma interface estreita com o departamento de recursos humanos quando o pessoal é contratado, demitido ou quando a posição de alguém dentro da organização muda.

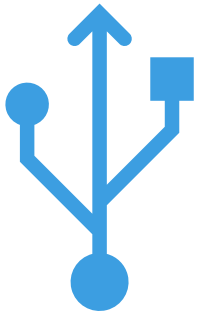


O zoneamento ajuda a decidir quais partes da organização precisam de controles rígidos de entrada física.

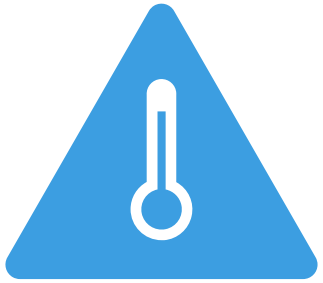


Os controles físicos são geralmente gerenciados pelo departamento de gerenciamento de instalações da organização. Para otimizar esses controles para a proteção das informações, o gerente de segurança, o gerente de TIC e o gerente da instalação devem trabalhar em conjunto nesse assunto.

Orientação para controles físicos 2/2

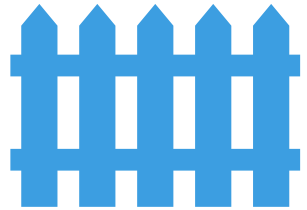


Os sistemas de TI são muito vulneráveis a problemas de energia elétrica. Uma fonte de alimentação de reserva (fonte de alimentação ininterrupta - UPS - para interrupções curtas e sistemas nobreak - geradores - para interrupções mais longas) sempre é necessária.



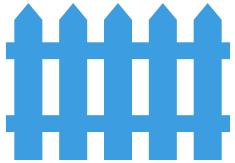
Os sistemas de gerenciamento predial - controle de energia, iluminação, acesso, temperatura etc. - são os próprios sistemas de computador. Eles precisam da mesma proteção que outros sistemas de computadores da organização.

Uma avaliação completa dos riscos ambientais deve determinar que tipo de controle físico de entrada é necessário.

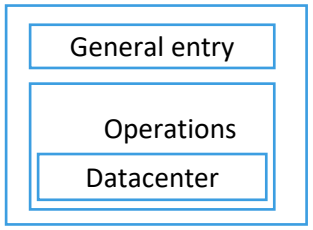


Barreiras físicas não devem obstruir o pessoal que sai das instalações em caso de emergência.

Baseline de Controles Físicos



Perímetro físico
Proteção
(sua força deve depender da classificação dos dados que estão sendo protegidos)



Assegurando escritórios, salas, instalações

Resiliência dos utilitários de suporte, inclusive processos de manutenção

Teste periódico de UPS e sistemas de nobreak

Mystery Guest (Convidado Misterioso)* teste de controles físicos de entrada

* Um profissional treinado que tenta burlar os controles físicos de entrada e encontra possíveis melhorias

4.3. Controle dos Funcionários

Exemplos de controles dos funcionários

- **E6.1.1 Alocação de responsabilidades de segurança da informação**
  Definir as responsabilidades de lidar com informações nos termos e condições do emprego e na política de segurança da informação.
- **13.2.4 Acordos de confidencialidade**
  Esclarece as responsabilidades legais do pessoal pela proteção da confidencialidade das informações.
- **8.1.3 Uso aceitável de ativos**
  Descreve e esclarece o uso permitido e não permitido dos ativos de informação da organização, como PCs móveis, telefones, copiadoras etc.
- **7.1.1 Triagem**
  Procedimentos para a triagem de pessoal nos cargos em que possam ocorrer riscos especiais, por exemplo, em cargos financeiros ou em cargos com altos requisitos de confidencialidade. Em caso de fraude para investigar a estação de trabalho do funcionário, pode ser a única possibilidade legal
- **7.2.2 Conscientização, educação e treinamento em segurança da informação**
  Procedimentos e todas as atividades que a organização realiza para treinar funcionários em segurança da informação em geral e nas políticas da organização em particular.
- **9.2.6 Remoção ou ajuste de direitos de acesso**
  Quando um funcionário deixa a organização, seus direitos de acesso, físicos e lógicos, devem ser imediatamente revogados.

Nota: nem todos os controles ISO/IEC 27002 estão incluídos; Esta lista não é exaustiva, os números se referem à ISO 27002.

Conscientização e Treinamento

- **Aspectos:**
  - Conhecimento (compreensão das regras)
  - Atitude (vontade de cooperar)
  - Comportamento (obedecendo as regras)

- O programa de conscientização deve ser estabelecido em alinhamento com o grupo-alvo e liderado pelo Gerenciamento de Segurança da Informação.
- O nível de conscientização do grupo alvo deve ser medido.
- A mudança de comportamento só acontecerá quando o grupo-alvo tiver obtido todo o conhecimento necessário e entender por que os controles de segurança são necessários.
- Ferramentas: treinamento em sala de aula, e-learning, conversas individuais, discussão, jogos.

Engenharia Social

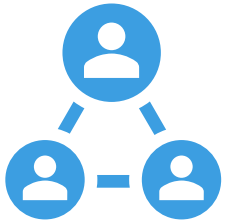
A maioria dos humanos está disposta a ajudar. Os adversários usam isso a seu favor, **construindo confiança com um funcionário** e obtendo informações que ajudam o adversário a ter acesso aos ativos da organização.

Com o sucesso das mídias sociais, uma enorme quantidade de informações pessoais está disponível ao público**. Os funcionários devem entender e seguir as políticas da empresa** o que podem ou não divulgar nas mídias sociais sobre a organização em que trabalham.

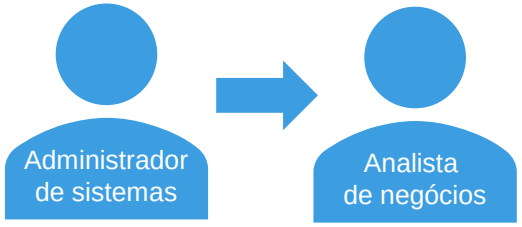
Os funcionários devem ser treinados para identificar a engenharia social e saber como identificar quem pode ter acesso a quais ativos.

Orientação para controles de funcionários

Deve-se ter um cuidado especial com as funções em que ocorrem altos riscos, principalmente nos casos em que são concedidos privilégios de acesso. Onde necessário, é essencial a separação de tarefas. Por exemplo, os administradores devem ter permissão para usar direitos de administrador apenas quando outro administrador estiver presente ("princípio dos quatro olhos").



Definir funções e responsabilidades é mais importante, mas certifique-se de que os funcionários também entendam essas responsabilidades e todas as etapas disciplinares se abusarem delas.



Especialmente quando os funcionários alteram as funções dentro da organização, todos os direitos de acesso devem ser revisados, isso requer ação do departamento de RH e dos gerentes relevantes.

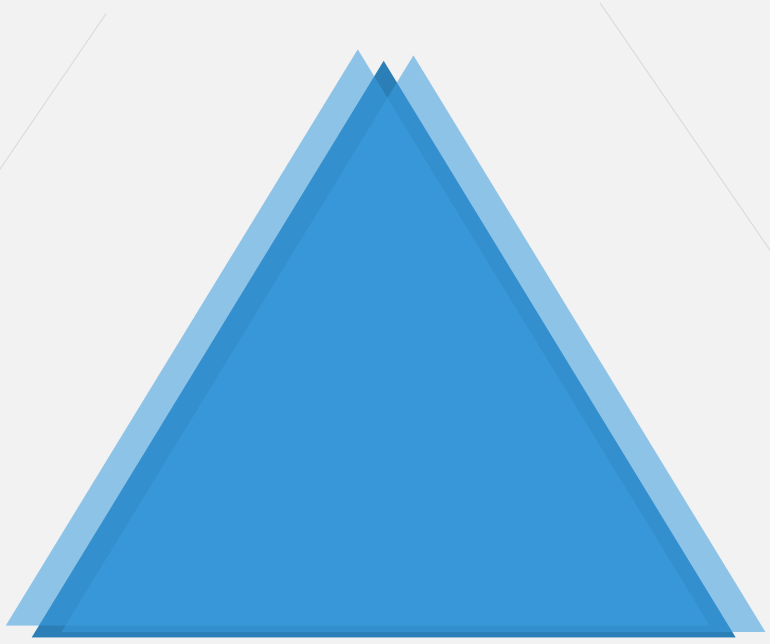
4.4. Controles de Continuidade

Continuidade / Disponibilidade

A segurança da informação lida com a tríade.

O capítulo 17 da ISO/IEC 27002 é denominado "Aspectos de segurança da informação do Gerenciamento de Continuidade de Negócios" (BCM). **O processo BCM dentro de uma organização é obviamente muito mais amplo do que apenas o gerenciamento de incidentes de segurança da informação.**

Confidencialidade



Integridade

Disponibilidade

De uma perspectiva de segurança da informação, o termo continuidade deve ser interpretado como:

- continuidade de segurança quando uma organização enfrenta um problema de continuidade de negócios e;
- disponibilidade de sistemas, procedimentos e serviços de segurança durante a operação normal.

Exemplos de controles de continuidade

12.3.1 Backup de informações
Embora não faça parte de um controle de continuidade de segurança da informação, é mencionado aqui, pois nenhuma organização pode sobreviver à perda de dados quando não são feitos backups. Observe que o ISO 27002 (incorretamente) não menciona explicitamente a necessidade de procedimentos de restauração como um controle separado.

17.1.1 Planejando a continuidade da segurança da informação
Durante a avaliação de risco geral do BCM, também devem ser incluídos os riscos de segurança da informação que podem levar a um problema de continuidade de negócios.

17.1.2 Implementando a continuidade da segurança da informação
Para os riscos de BCM que a organização decide mitigar, os aspectos de segurança da informação devem ser incluídos. Por exemplo; quando, durante uma crise, são contratados recursos humanos extras, esses recursos devem ser treinados primeiro nos procedimentos de segurança.

17.1.3 Verificar, revisar e avaliar a continuidade da segurança da informação
Os aspectos de segurança da informação do BCM devem ser usados para treinamentos periódicos.

17.2.1 Disponibilidade de instalações de processamento de informações
As instalações de processamento de informações devem ser implementadas com redundância suficiente para atender aos requisitos de disponibilidade.

Nota: nem todos os controles ISO/IEC 27002 estão incluídos; Esta lista não é exaustiva, os números se referem à ISO27002.

Planejamento de continuidade de negócios (TI) 1/4

Um plano de recuperação de desastre deve cobrir pelo menos os dois assuntos:

Quando um **incidente grave** leva a danos substanciais ao processamento de informações e serviços relacionados, há uma restrição importante: **tempo**!

O tempo de inatividade máximo permitido (se a organização não conseguir se recuperar por mais tempo) deveria ter sido convertido em objetivo de **tempo de recuperação** (RTO) e **objetivo de ponto de recuperação** (RPO).

RTO

O RTO especifica a duração e o nível de serviço dentro do qual um serviço de TI deve ser restaurado após um desastre ou interrupção.

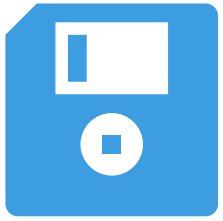
RPO

RPO é o período máximo tolerável em que os dados podem ser perdidos de um serviço de TI devido a um incidente grave.

Planejamento de continuidade de negócios (TI) 2/4

RPO depende muito dos riscos de negócios que uma organização enfrenta quando as transações são perdidas. Ele determina a infraestrutura de TI necessária.

Exemplos de RPOs e infraestrutura de TI necessária:



1 a 2 dias: backup diário usando sistemas de disco para disco, ou de disco para fita.

1 a 2 horas: discos espelhados com log de transações.

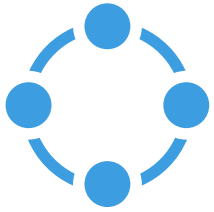
1 a 2 minutos: discos espelhados com registro de transações e registro diário.

Planejamento de continuidade de negócios (TI) 3/4

RTO determina se é necessário o processamento em espera, como a espera a frio, em espera a quente ou espelhado. Como o tempo é a única restrição, as RTOs expressas em horas determinam que todas as atividades de detecção, escalada e mitigação do incidente sejam documentadas e suficientemente treinadas.

O documento que descreve isso é o Plano de Continuidade de Negócios (BCP) ou Plano de Continuidade de TI

Durante um incidente de continuidade de negócios, o pessoal envolvido na solução da situação pode ser diferente do que durante a operação normal. Isso requer que o BCP descreva atividades críticas em grande detalhe.

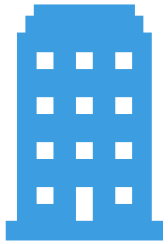


O desenvolvimento de um BCP é feito pelos especialistas com conhecimento que, durante a operação normal, são responsáveis pelos processos de TI ou de negócios. Eles definem as ações, os prazos de entrega e as instalações/serviços necessários para poder executar essas ações. Posteriormente, essas ações são colocadas em um gráfico de Gantt.

Planejamento de continuidade de negócios (TI) 4/4

Exercício Periódico

Qualquer BCP (IT) deve ser exercitado periodicamente. Isso deve levar à restauração completa dos serviços de TI dentro dos requisitos de RTO e RPO. Todo o pessoal envolvido deve ter conhecimento sobre suas funções e atividades.



Mudança organizacional

Qualquer alteração na organização deve levar a alterações no BCP. Isso requer uma interface forte com qualquer processo de gerenciamento de mudanças dentro da organização.

Soluções de disponibilidade

Existem várias soluções de disponibilidade de TI, como invasão, clustering, virtualização e até computação em nuvem. No entanto, essas soluções ainda exigem controles de continuidade. Por exemplo; em um ambiente em cluster, excluir arquivos importantes, por acidente, no sistema 1, também significa exclusão no sistema 2.

Orientação para backup de informações

- Em todos os níveis da organização (TI), deve ser entendido que 'backup' não é o problema.
- O problema é poder restaurar todas as informações relevantes, independentemente da ameaça à perda de dados, em todas as circunstâncias, dentro do prazo exigido.
- Quando for entendido adequadamente que "restauração" é o problema, ficará claro que "backup" é apenas parte da solução.

- Para restauração adequada, existe um grande número de outros requisitos, como:
  - Entender qual é o prazo para restauração
  - Entender a ordem na qual os sistemas devem ser restaurados
  - Disponibilidade de sistemas para restaurar em
  - Pessoal com conhecimento em atividades de restauração
  - Software necessário para fazer a restauração
  - Procedimentos de restauração que descrevem as atividades necessárias
  - Procedimentos de teste após uma restauração para decidir se a produção pode reiniciar

4.5. Controles Técnicos

Exemplos de controles técnicos

- **12.2.1 Controles contra malware**
  O malware é abundante. Software de antivírus e procedimentos para prevenção são obrigatórios.

- **12.4.1 Registro de eventos**
  As atividades de alto risco devem ser registradas na mídia, caso o adversário não tenha acesso. Isso facilita a detecção de incidentes.

- **13.1.3 Segregação em redes**
  Uma abordagem de segurança em camadas significa que a rede da organização deve ser dividida em zonas, com atenção especial às zonas que possuem conexões externas.

- **11.2.2 Utilidades**
  A disponibilidade de serviços públicos (telecomunicações, eletricidade, água etc.) deve ser garantida. Isso pode exigir suprimentos sobressalentes, conexões redundantes, instalações nobreak etc.

- **10.2.2 Gerenciamento de chaves**
  O uso de chaves e certificados eletrônicos deve ser controlado.

- **12.6.1 Gerenciamento técnico de vulnerabilidades**
  Os sistemas de TI falham e contêm bugs. Essas vulnerabilidades devem ser conhecidas sempre que possível e atenuadas por, por exemplo, gerenciamento rigoroso de patches, testes de penetração, etc.

Nota: nem todos os controles ISO/IEC 27002 estão incluídos; Esta lista não é exaustiva, os números se referem à ISO27002.

Controles contra malware

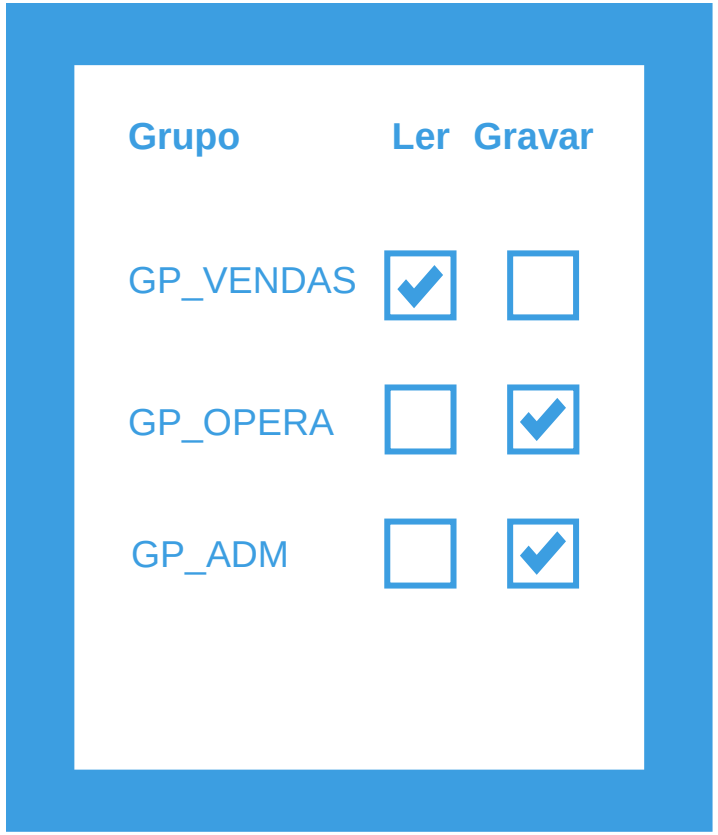
Malware

- O malware vem em vários tipos; eles danificam dados e/ou aplicativos ou roubam informações.
- Os sistemas (baseados em hardware ou software) que detectam código malicioso dependem de assinaturas que representam o código encontrado anteriormente do malware ou detectam o comportamento malicioso do próprio malware.
- Infelizmente, esses sistemas geram falsos positivos e também falham com precisão na detecção de todos os malwares conhecidos.
- Observe que a ISO/IEC 27002 usa o termo mais geral "malware". Isso também denota, por exemplo, backdoors ocultos e bombas lógicas que podem (às vezes!) ser detectados apenas por humanos ao fazer a revisão de código de software.
- Atualmente, muitos malwares são transferidos por pen drives, mas principalmente por sites infectados.

Protegendo a confidencialidade

- A prevenção do vazamento de informações confidenciais depende da prevenção do acesso às informações. Quando isso falha ou não pode ser garantido (em redes públicas, por exemplo), a criptografia é necessária (especialmente ao usar BYOD)

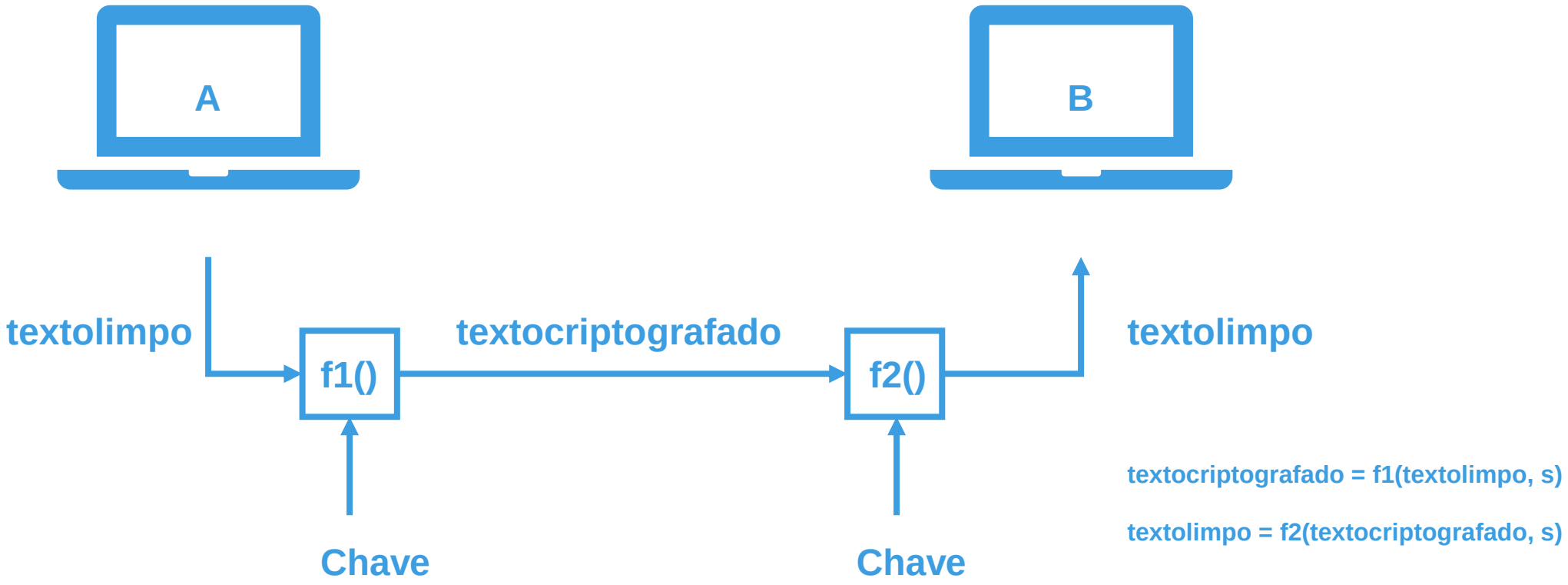
- Impedir o acesso às informações significa identificação e autorização do usuário e acesso subsequente com base nas listas de controle de acesso (ACL) que descrevem que tipo de acesso o usuário tem; ler, escrever, executar, criar, excluir etc.



- Um bom controle de acesso abrange as três categorias: controles técnicos, programas e políticas

- A criptografia de informações se resume a embaralhar as informações de tal maneira que usuários legítimos possam facilmente decifrá-las, mas um adversário não. Isso requer algum tipo de chave digital e uma função unidirecional que não permitirá decodificação.

Criptografia simétrica

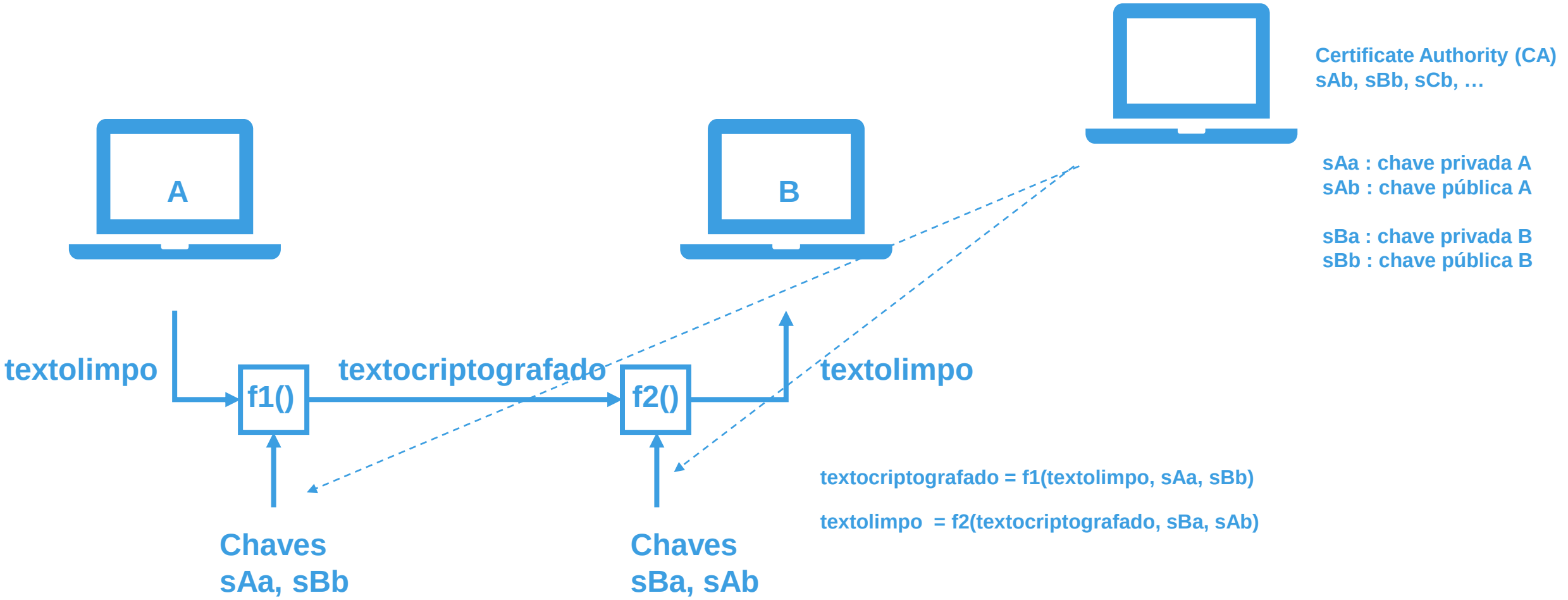


Nota:
f1 () e f2 () são funções matemáticas unidirecionais complexas, fáceis de calcular, mas impossíveis de serem computadas da outra maneira.
Um exemplo; é fácil multiplicar dois números grandes. Mas fatorar o número em seus fatores é muito difícil se o número for grande.

Criptografia simétrica

- Simétrico porque ambas as partes usam a mesma chave.
- Um exemplo da matemática usada é o Data Encryption Standard (DES), ele usa uma chave de 56 bits.
- O DES é considerado inseguro (pelas técnicas de força bruta, a chave pode ser encontrada em minutos), foi substituída pelo AES (Advanced Encryption Standard).
- A criptografia simétrica é rápida e, portanto, muito usada.
- O problema, porém, é o gerenciamento de chaves; Quando muitas partes precisam se comunicar, a distribuição segura de chaves se torna um problema.

Criptografia assimétrica



Criptografia assimétrica

- Toda parte gera duas chaves; uma chave privada que precisa ser mantida em segredo e uma chave pública que todos possam conhecer.
- Quando A(driano) precisa enviar uma mensagem confidencial para B(ianca), ela usa uma fórmula matemática que criptografa a mensagem usando sua chave privada e a chave pública de Bianca.
- Quando Bianca recebe a mensagem, ele pode descriptografá-la usando sua chave privada e a chave pública de Adriano.
- Uma entidade separada, a autoridade de certificação (CA), atua como intermediária responsável por entregar a chave pública de alguém a todos que a solicitarem.
- Para que isso funcione, existem vários pré-requisitos, como:
  - A CA deve garantir que a chave pública solicitada por alguém realmente pertença à parte que a gerou.
  - A matemática envolvida deve garantir 100% que, sem as chaves privadas, ninguém pode decifrar as mensagens daquele que usou a chave pública correspondente para cifrar.
- Um ponto de atenção deve ser dado, caso a autoridade de certificação seja hackeada, certificados falsos podem ser hackeados e/ou todos os certificados podem ser invalidados.

Assinaturas eletrônicas

- Uma chave privada é um identificador exclusivo, portanto, pode ser usada como uma assinatura eletrônica.
- Juntamente com as funções de hash*, elas podem ser usadas para provar a identidade e / ou a integridade.
  - A(driano) gera um hash de um documento e criptografa (assina) um documento e seu hash usando sua chave privada e envia os resultados para B(ianca).
  - B(ianca) descriptografa o documento e o hash usando a chave pública A(driano) e executa novamente a função de hash. Se o resultado no documento descriptografado corresponder ao hash descriptografado que A(driano) enviou, o documento poderá ter se originado apenas de A(driano).
  - É claro que isso só funciona quando A(driano) mantém sua chave privada em segredo e há uma prova definitiva de que ele "possui" sua chave pública.

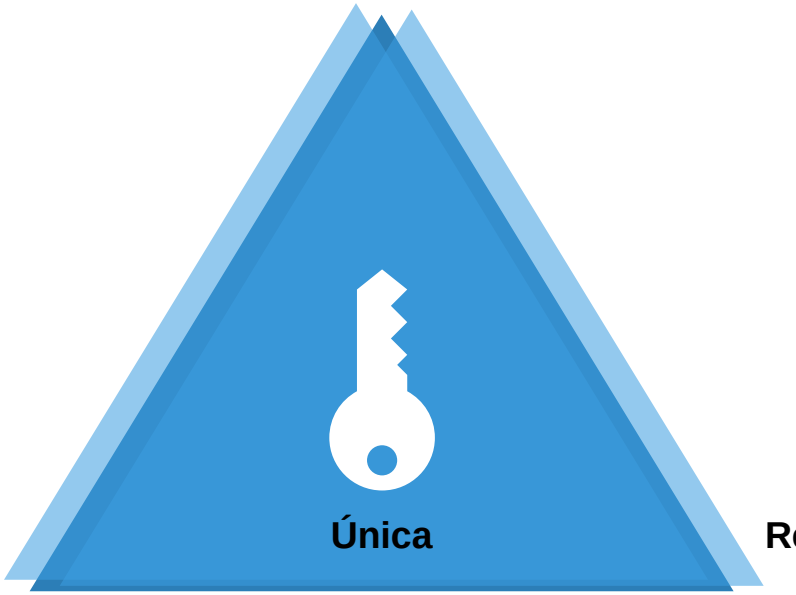
* É um algoritmo matemático que mapeia dados de tamanho arbitrário (geralmente chamado de "mensagem") para uma cadeia de bits de tamanho fixo (o "valor do hash", "hash" ou "resumo da mensagem") e é uma função de via de mão única, ou seja, uma função praticamente inviável de inverter.

Gerenciamento de chaves

Ao usar a criptografia, o problema de manter uma grande quantidade de dados em segredo foi substituído pela manutenção da(s) chave(s) – uma pequena quantidade de dados - secreta. Isso introduz um novo problema; gerenciamento de chaves.

As chaves devem, por exemplo, ser:

Mantidas absolutamente em segredo



Única

Protegidas contra perdas

Revogadas quando uma violação ocorrer ou é suspeita

Protegendo a integridade

0 1 0 1 1 1 0 1 0 1

1 1 1 # # 0 1 0 1 0

0 1 0 1 1 0 1 0 1 0

1 0 1 1 1 1 0 0 1 0

1 0 1 0 0 0 1 1 0 1

- **A integridade das informações pode ser afetada por várias causas.** Os discos rígidos podem falhar ao armazenar bits de maneira confiável, por exemplo. Ou durante a transmissão de dados, pode ocorrer ruído na linha, isto é, as lojas on-line podem enfrentar dificuldades se perderem a integridade das informações de seus produtos.
- Como a informação digital é composta de bits e estes podem ter apenas dois estados possíveis (0 ou 1), um bit danificado precisa ser alterado para o outro estado.
- Contudo; como sabemos quais bits foram alterados erroneamente?

Protegendo a integridade; checksums

- Por exemplo, o número decimal 48577 deve ser armazenado digitalmente, para ser convertido em bits digitais e temporariamente armazenado em uma matriz (eletrônica) que adiciona bits às colunas e linhas:

48577_D

1011 1101 1100 0001

ou

1011
1101
1100
0001 ➔

Os números '1s' seguidos e coluna deve ser uniforme

1	0	1	1	**1**
1	1	0	1	**1**
1	1	0	0	**0**
0	0	0	1	**1**
1	**0**	**1**	**1**	

Protegendo a integridade; checksums

Agora, mudamos o resultado e armazenamos (ou transmitimos) o resultado ...

1011 1110 1111 0000 0011 1011

... E vamos assumir que o bit com a seta está invertido.

Ao receber ou ler os bits, podemos reverter o processo:

1011 1110 1111 0000 1011 1011 ➔

1	0	1	1	**1**
1	1	0	1	**1**
1	1	0	0	**0**
0	1	0	1	1
1	**0**	**1**	**1**	

... e podemos deduzir que esse bit não deve ser 1

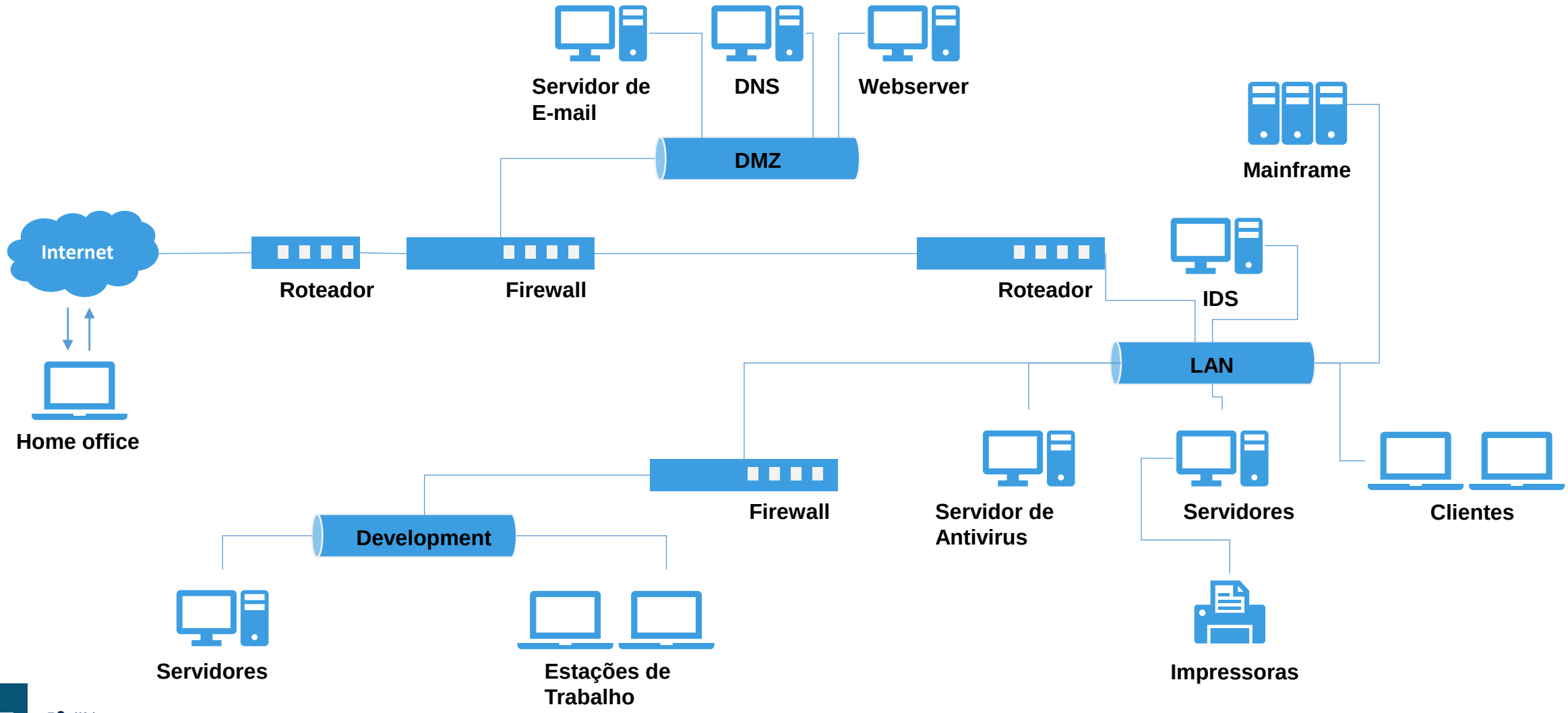
Então mude para 0, descarte todos os bits extras, retire e converta para decimal.

Baseline de Controles Técnicos

- Controles contra malware
- Controles de rede
- Auditar, revisar e proteger informações de log
- Monitorando o uso do sistema
- Segregação em redes
- Identificação e autenticação de usuário
- Controle de processamento interno
- Controle de vulnerabilidades técnicas

4.6. Controles de Rede

Controles de rede, um exemplo de infraestrutura



Componentes de infraestrutura

Comunicações

Roteadores
Firewall
Gateway
DMZ
Mail / Web / Antivirus / Servidores DNS
IDS / IPS

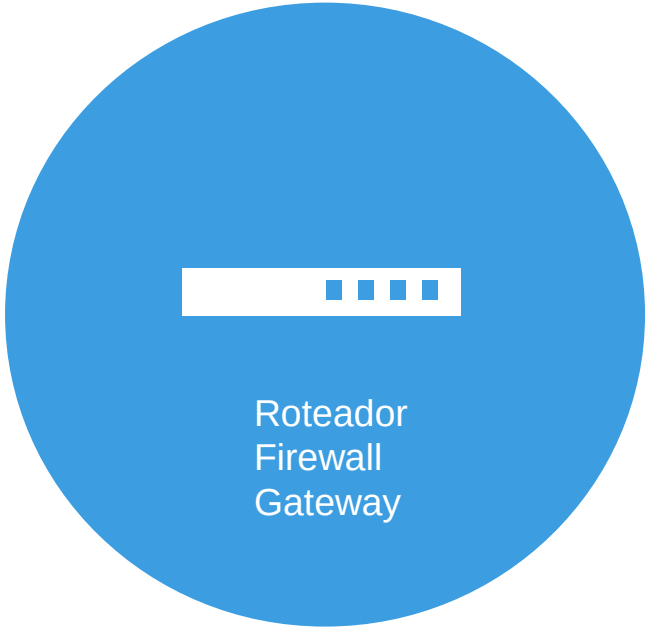
Processando informação

Servidores de aplicativos /
Arquivos de Clientes

Transmissão

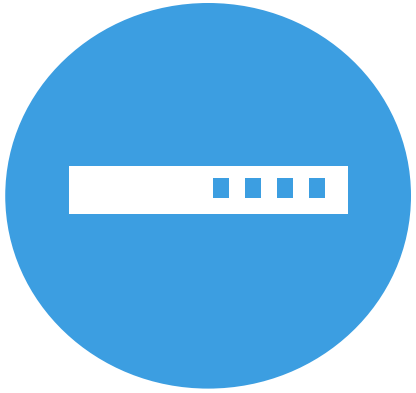
Cabo LAN
Wireless LAN

Componentes de infraestrutura



- Esses dispositivos atuam como filtros de rede. Sua função pode ser combinada.
- Um roteador divide as redes e, com base nos intervalos de endereços, encaminha o tráfego ou o bloqueia. Isso pode ser feito extremamente rápido.
- Um firewall analisa os pacotes de dados e decide, com base em um conjunto de regras, se deve permitir esses pacotes na rede ou não. Geralmente usado para dividir áreas com diferentes requisitos de confidencialidade.
- Um gateway vai um passo além; por exemplo, permite apenas usuários na rede após identificação e autorização.

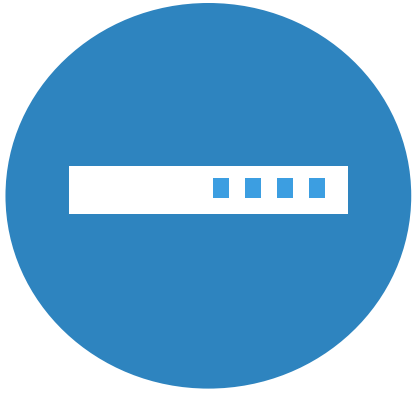
Componentes de infraestrutura – Tipos de Firewall



Firewall de filtragem de pacotes

Eles atuam inspecionando os "pacotes" que são transferidos entre computadores na Internet. Se um pacote corresponder ao conjunto de regras do filtro de pacotes, ele será descartado ou rejeitado.

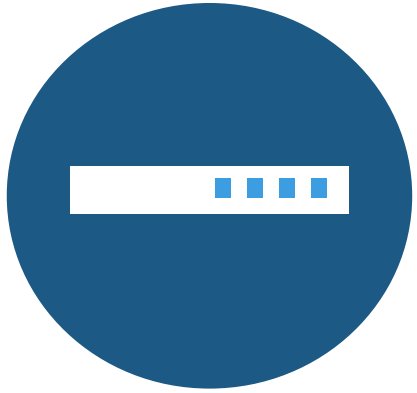
Esse tipo de filtragem de pacotes não presta atenção se um pacote faz parte de um fluxo de tráfego existente. Ele filtra cada pacote com base apenas nas informações contidas no próprio pacote (geralmente usando uma combinação do endereço de origem e destino do pacote, seu protocolo e, para o tráfego TCP e UDP, o número da porta).



Firewall Statefull

Eles registram todas as conexões que passam por ele e determinam se um pacote é o início de uma nova conexão, parte de uma conexão existente ou não faz parte de nenhuma conexão.

Embora as regras estáticas ainda sejam usadas, agora elas podem conter o estado da conexão como um dos critérios de teste.



Firewall da camada de aplicativo

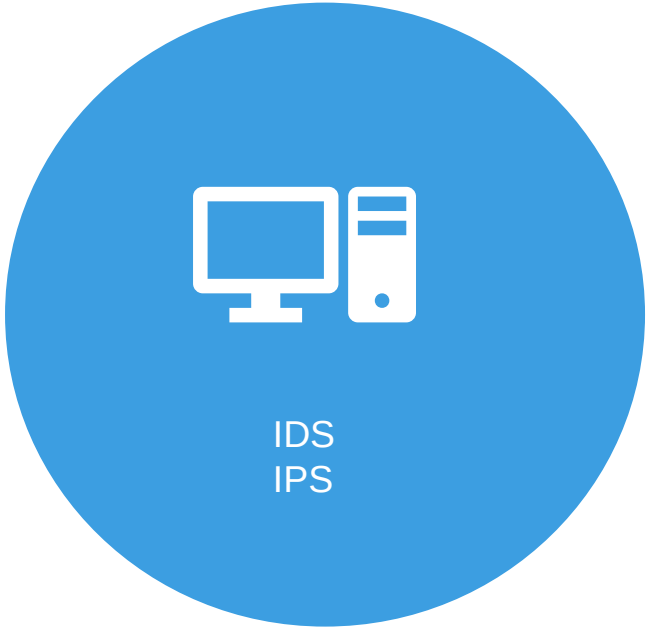
Eles podem "entender" certos aplicativos e protocolos (como FTP, File Transfer Protocol), DNS (Sistema de Nomes de Domínio) ou HTTP (Hypertext Transfer Protocol)).

Isso é útil, pois é capaz de detectar se um protocolo indesejado está tentando ignorar o firewall em uma porta permitida ou detectar se um protocolo está sendo violado de alguma forma prejudicial.

Componentes de infraestrutura

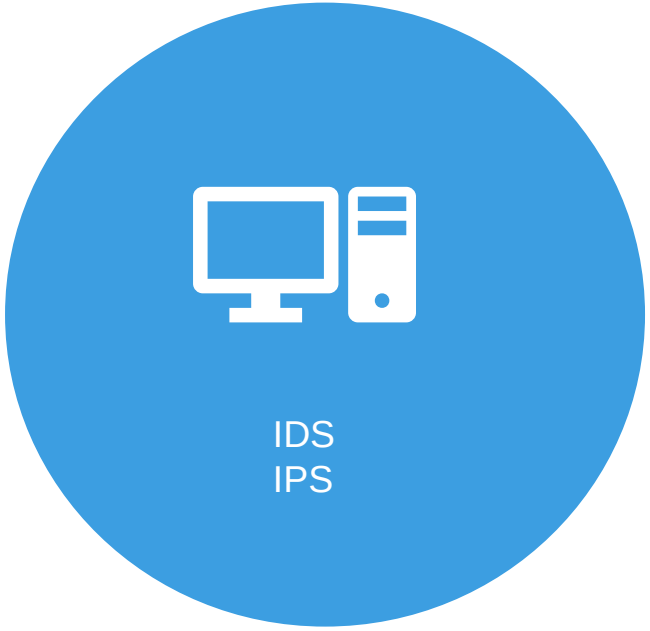
- Os servidores que têm uma função principal em redes públicas, por exemplo, recuperar e-mail ou um servidor da web, devem estar situados na zona desmilitarizada (DMZ).
- Nesta zona de buffer, eles podem ser separados das redes internas (por um firewall) para que, quando comprometidas do lado de fora, ainda haja uma barreira entre a zona comprometida e as informações da organização.

Componentes de infraestrutura



- Esses sistemas, como os de detecção de intrusões e sistemas de prevenção de intrusões tentam tomar decisões inteligentes se a rede ou a DMZ foi comprometida.
- Um IDS analisa o tráfego e, por exemplo, com base em assinaturas ou anomalias estatísticas, pode rejeitá-lo.
- Às vezes, um IDS trabalha em conjunto com o firewall; se perceber um tráfego prejudicial, poderá instruir o firewall a bloquear todo o tráfego dessa fonte.
- Um sistema de prevenção de intrusões se assemelha a um IDS, mas é colocado em linha e é capaz de impedir/bloquear ativamente invasões detectadas.

Componentes de infraestrutura



- O IDPS baseado em host usa agentes que residem em hosts individuais em uma rede. Eles analisam os arquivos de log criados e armazenados nesse host (kernel, sistema, servidor, rede, firewall e outros) e monitoram processos em execução, acesso a arquivos e alterações na configuração - isso é feito com a coleta de dados de vários computadores. O agente usa essa análise para comparar os dados capturados com o banco de dados interno de assinaturas comuns conhecidas para ataques armazenados no servidor de gerenciamento. Esses agentes podem operar apenas no modo de detecção ou na prevenção e agir contra a entidade infratora.
- O IDPS baseado em host pode usar uma combinação de técnicas de detecção baseadas em assinatura e baseadas em anomalias, mas qual dependem do tipo específico de produto usado.

Componentes de infraestrutura

- O filtro de conteúdo é usado para controlar qual tipo de conteúdo pode ser acessado e visualizado, além de ser negado em relação à web e a e-mails.
- Ele funciona com base na especificação de um padrão de conteúdo que pode ou não ser acessado, como textos, expressões, objetos dentro de imagens, entre outros.
- Isso é muito útil para proteger a rede da organização contra sites maliciosos e e-mails, no entanto, será necessária uma extensa configuração e atualizações por operações, uma vez que vários novos sites estão aparecendo continuamente.

Componentes de infraestrutura

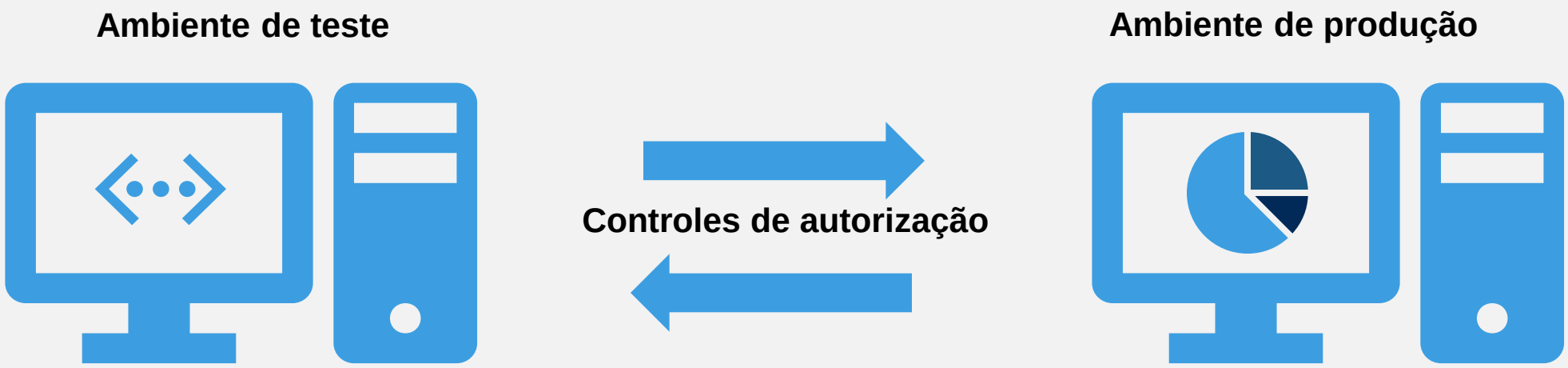
- Esses sistemas contêm os dados e/ou aplicativos e dispositivos da organização para acessar os dados e aplicativos.
- A separação de dados e aplicativos traz benefícios, por exemplo, em processos de backup; os aplicativos são estáticos, os dados são dinâmicos e precisam de backups mais frequentes. Também estão envolvidos papéis diferentes; administradores de banco de dados para gerenciadores de dados e aplicativos funcionais/técnicos.
- Os clientes podem ser “normais" ou os “Thin Clients", dependendo de terem instalações locais de processamento de dados ou se apenas apresentam informações de outro sistema, como um servidor de aplicativos.

Componentes de infraestrutura

Cabo LAN
Wireless LAN

- Nos escritórios hoje em dia, apenas os sistemas de cabeamento Ethernet são usados. Quando o acesso físico a soquetes e cabos é possível, um adversário pode conectar um sistema externo à rede e farejar toda a comunicação.
- A criptografia deste documento pode ser benéfica. Às vezes, a filtragem de endereço MAC é usada, permitindo apenas sistemas com endereços conhecidos na rede; no entanto, os endereços MAC podem ser forjados.
- As redes sem fio eliminam sistemas de cabeamento caros, mas exigem criptografia e autorização para torná-los seguros.
- Em redes sem fio, o WPA2 é considerado seguro (até este momento).

Divisão de produção do ambiente de teste

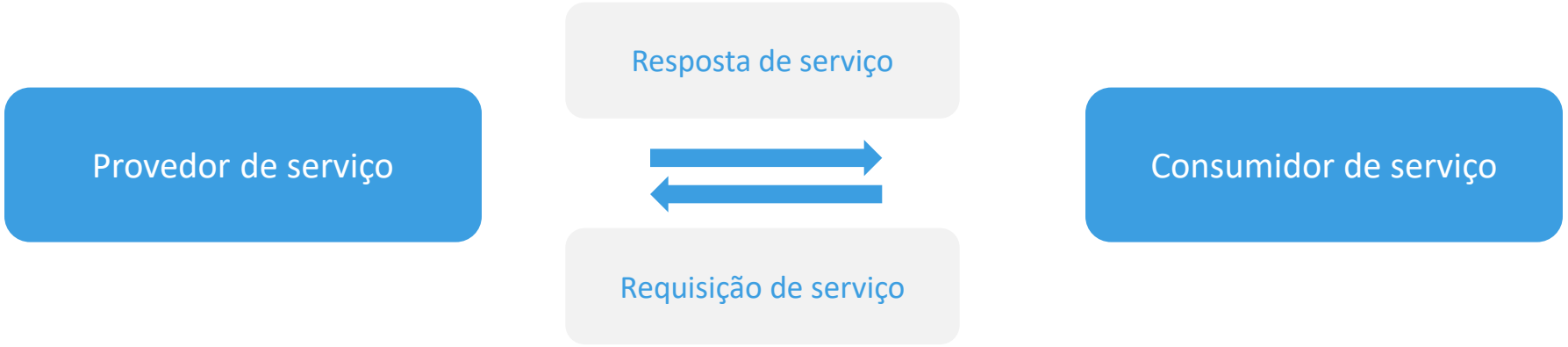


- Os ambientes de teste devem ser controlados por meio de controles de autorização, a fim de proteger a integridade do ambiente de produção.
- Ao implementar esse controle, uma autorização deve ser feita sempre que os dados estão sendo movidos da produção para o teste e do teste para o ambiente.
- Isso aumentará não apenas a integridade dos dados, mas também garantirá que os dados que estão sendo transferidos estejam alinhados com a política de Segurança da Informação da organização.

Infraestrutura Orientada a Serviços (SOA)

Service Oriented Infrastructure (SOA) é uma abordagem arquitetônica na qual os aplicativos utilizam os serviços disponíveis na rede. Na arquitetura orientada a serviços, vários serviços se comunicam entre si, de uma das duas maneiras: passando dados ou através de dois ou mais serviços coordenando uma atividade.

As principais características da SOA são: valor comercial, objetivos estratégicos, interoperabilidade intrínseca, serviços compartilhados, flexibilidade e refinamento evolutivo



Existem duas funções principais na arquitetura orientada a serviços:

Provedor de serviço: O provedor de serviços é o mantenedor do serviço e a organização que disponibiliza um ou mais serviços para outros usarem. Para anunciar serviços, o provedor pode publicá-los em um registro, juntamente com um contrato de serviço que especifica a natureza do serviço, como usá-lo, os requisitos para o serviço e as taxas cobradas.

Consumidor de serviço: O consumidor do serviço pode localizar os metadados do serviço no registro e desenvolver os componentes do cliente necessários para vincular e usar o serviço.

Infraestrutura Orientada a Serviços (SOA) e Segurança da Informação

- Quando se trata de segurança da informação, alguns aspectos devem ser levados em consideração.
- É importante que, ao projetar serviços ou infraestrutura com base em SOA, a equipe de Segurança da Informação esteja envolvida no projeto.
- A definição de quais serviços de segurança serão fornecidos e em qual arquitetura deve ser definida para melhor alinhar os requisitos de segurança da informação e o serviço para os clientes.

Arquitetura de design aberto

- A arquitetura de design aberto defende que o estabelecimento de um catálogo de controle único, consistente e claramente definido forneça um meio excelente para simplificar os requisitos de vários padrões, estruturas de governança, legislação e regulamentos.
- Ao usar os padrões OSA (Open Security Architect), é possível iniciar rapidamente, melhorar a qualidade da solução que deve ser implantada e reduzir o esforço geral.
- Geralmente, o uso da arquitetura de design aberto aumentaria a extensão dos testes, melhorando a segurança dos serviços.

Princípios arquitetônicos

Simplicidade sobre flexibilidade	Usabilidade sobre restrição	Defesa em profundidade

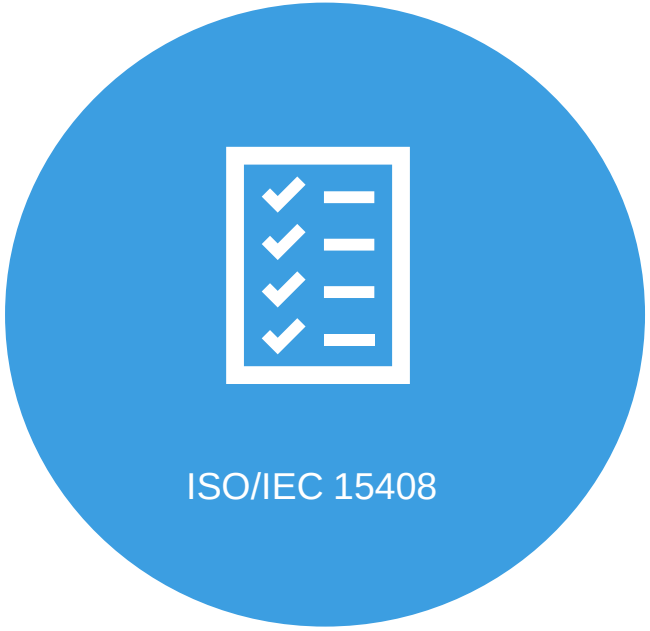
Princípios de implementação

Design aberto	Práticas de codificação segura	Teste de caixa preta e caixa branca

Princípios de operações e configurações

Mediação completa	Ultimo privilégio	Trilhas de auditoria

Critérios Comuns



- Como os firewalls e outros equipamentos de concessão de acesso são os guardiões dos ativos de informação da organização, é necessária uma certificação independente.
- ISO/IEC 15408, ou critérios comuns, "… é uma estrutura na qual os usuários de sistemas de computador podem especificar seus requisitos funcionais e de segurança de segurança, os fornecedores podem implementar e/ou fazer reivindicações sobre os atributos de segurança de seus produtos e os laboratórios de teste podem avaliar os produtos para determinar se eles realmente atendem às reivindicações ". (Fonte: wikipedia.)
- Quando um produto de segurança é testado em relação à ISO/IEC 15408, ele recebe um Nível de Garantia de Avaliação (EAL). Quando os usuários determinam seus requisitos de garantia, eles podem decidir instalar apenas equipamentos com os EAL correspondentes.
- Os níveis de garantia variam de 1 (básico) a 7 (mais rigoroso).

Identificação e autorização do usuário

- Idêntico ao acesso físico; para obter acesso às informações (sistemas), o usuário deve se identificar com algo que possui (por exemplo, um cartão inteligente), possui conhecimento (por exemplo, identificação do usuário/senha) ou é (por exemplo, biometria).
- Quando mais de dois deles são necessários, isso é chamado de autenticação forte.
- Com base nas informações de identificação fornecidas, o acesso a informações, sistemas e redes de informações deve ser concedido. A autorização para acessar esses ativos deve ser regida por um processo seguro.
- Os tipos de acesso também devem ser controlados, isto é, ler, escrever, excluir, criar, imprimir, copiar, arquivar etc.
- Esses direitos de acesso devem ser associados ao papel de alguém na organização; não para funções ou pessoas explícitas, ou seja, acesso baseado em função (RBAC), pois muitas vezes as funções mudam regularmente.
- Deve-se ter cuidado especial com a proteção contra leitura, ou seja, como uma pessoa ou processo classificado para ter acesso a uma determinada classe de informações é protegido contra a leitura de informações classificadas em um nível superior. Na maioria dos casos, a gravação é permitida, mas a leitura é negada.

Senhas

Quase todos os sistemas de identificação contam com o usuário que fornece (apenas) uma senha. O usuário **deve manter essas informações em segredo**, mas a quantidade de senhas que um usuário deve manter em segredo aumenta rapidamente, para que os usuários escolham senhas fáceis ou as anotem. Portanto, a autenticação forte é sempre necessária para o acesso a sistemas e informações confidenciais.

Senhas mais usadas de 2019

1. 123456
2. 123456789
3. qwerty
4. senha
5. 1234567
6. 12345678
7. 12345
8. euamovc
9. 111111
10. 123123

As senhas devem:

- Não consistir em palavras encontradas em um dicionário
- Seja longa e contenha caracteres do conjunto alfanumérico completo
- Ser mudadas regularmente

- Oportunidade de carreira
- Aprenda a lidar com as tendências de segurança no mundo conectado
- Aprenda os princípios básicos de segurança da informação e o uso da ISO / IEC 27001
- Combine Segurança da Informação e Computação em Nuvem

- Promove a consciência de segurança
- Concentre-se nas pessoas, bem como nas ferramentas e processos
- Trabalhe de acordo com a ISO / IEC 27001
- Antecipar legislação e regulamentos
- Crie uma oferta de certificação de carreira no EXIN: EXIN Information Security Officer.

EXIN Information Security Management Professional based on ISO/IEC 27001

Obrigado!