# Análise de risco – ativos, vulnerabilidades e impactos

Conceituar a análise de risco e os principais termos relacionados com o assunto e que são necessários para o entendimento do processo de Analise de Risco como um todo.

Expressão numérica é uma sequência de operações fundamentais: Radiciação, potenciação, divisão, multiplicação, subtração e adição, que podem ser agrupadas com o uso de parênteses, colchetes e chaves.

Em virtude de a informação ser o principal ativo das organizações, estas começaram a implementar uma série de medidas e controles internos que as ajudassem a proteger essas informações contra acessos indevidos, geralmente praticados por pessoas sem autorização.

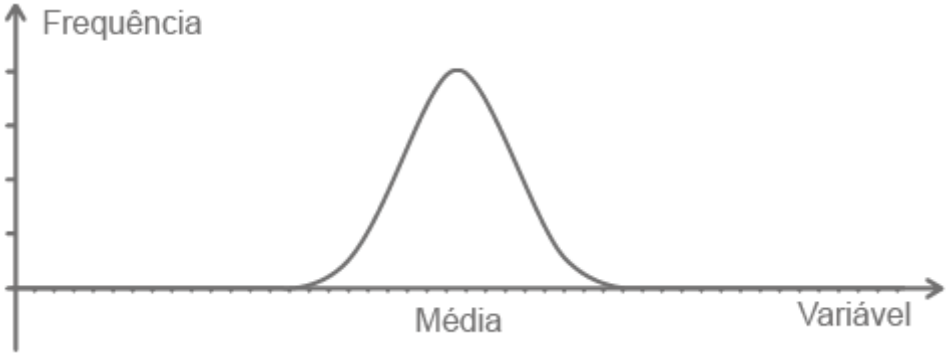
Diversas tecnologias foram aplicadas buscando identificar possíveis acessos não autorizados ou alteração de dados de forma fraudulenta.

A quantidade de computadores e o volume de informações manipuladas todos os dias são de difícil mensuração e, aliado a isso, temos dentro das empresas uma quantidade infinita de processos que interagem entre si para que as atividades empresariais consigam ser realizadas. A quantidade de ameaças e o custo da implantação dessas defesas eram muito grandes, pois a ideia no início era a implantação da segurança 100%.

## Expressões:

A distribuição normal, também chamada de curva de Gauss ou de Moivre representa uma distribuição de probabilidade e é muito utilizada em Pesquisa Operacional, sendo uma distribuição de probabilidade contínua.

Essa curva utiliza dois parâmetros para a determinação de seu gráfico, a média (?) e o desvio-padrão (?).




## Resolução de expressões:

Como não existe segurança 100%, ou seja, proteger tudo contra todos, foi dessa forma criado um grande impasse para as empresas, uma vez que as variáveis de segurança e insegurança mudavam constantemente, bem como os ativos de informação.

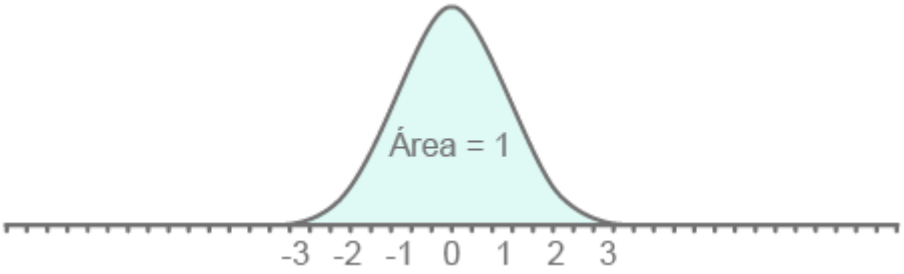
Dessa forma as empresas começaram a sentir a necessidade de identificar a quantidade de seus ativos, em que podemos entender como "ativo" qualquer coisa que tenha algum valor para a organização e da qual ela necessite para realizar alguma atividade de seu processo empresarial.

Podemos citar como um ativo os elementos a seguir:

- Equipamentos (computadores, monitores, laptops, modems);
- Equipamentos de comunicação (roteadores, PABX, Access Point, Switches);
- Mídias magnéticas (fitas e discos);
- Equipamento de proteção de energia (Nobreaks, ar-condicionado);
- Servidores de rede (banco de dados, correio eletrônico, internet);
- Mobília e acomodações;
- Infraestrutura do ambiente computacional;
- Serviços de redes;
- Telefones celulares;
- Mídia removível (fitas, disquetes, CD-ROM, DVDs);
- Senhas de funcionários;
- Relatórios de crédito de consumo do cliente;
- Registros médicos do cliente;

- Dados de contatos de negócios dos funcionários;
- Dados de contrato de parceiros
- Etc.

1. Parênteses: ( )
2. Colchetes: [ ]
3. Chaves: { }




## Operações:

Alguns dos ativos relacionados anteriormente poderiam ser importantes para um processo empresarial. Entenda-se como processo empresarial o conjunto de atividades/tarefas que uma determinada área de uma empresa tem que executar diariamente ou não para atender ou produzir algum serviço que é esperado pela empresa.

Depois da identificação desses ativos, é preciso definir a sua importância, iniciar o processo de verificar os seus pontos fracos e então definir controles de segurança que deveriam ser implantados.

Muitas vezes, para que a organização possa tomar essa atitude, é necessário que seja feita uma atividade conhecida como análise de risco, que terá como função indicar em que ocasião certo contexto pode ou não ser aceito por uma organização.

Quando não se conhece o que deve ser protegido e contra o que deve ser implementada a proteção, fica impossível implementar a medida de segurança correta e por isso podemos afirmar que "não há possibilidade de se proteger de algo que não se conheça". Na medida em que são identificados os ativos a serem protegidos e os seus possíveis agressores, fica mais fácil a implementação dos controles necessários para que seja feita a proteção.

A curva normal é simétrica em torno da média, e a probabilidade de que ocorra um valor maior ou menor que a média é sempre igual a 0,5, ou seja, cada metade da curva representa 50% de probabilidade.

Para determinar a área a seguir, de uma curva normal, calculamos o valor da variável padronizada (z), que representa o número de desvios de afastamento de x em relação à média. Com esse resultado, utilizamos uma tabela padronizada para encontrar a área procurada.

$$z = \frac{x - ?}{s}$$

Exemplo: em uma sala de aula, a nota dos alunos segue uma distribuição normal, com média igual a 7 e desvio-padrão 1,8. Qual a probabilidade de um aluno escolhido ao acaso ter uma nota entre 7 e 8,5?

$$z = \frac{8,5 - 7}{1,8} = \frac{1,5}{1,8} = 0,83$$

***Então, P(7< x < 8,5)=P(0,5 < x < 0,83)***

A probabilidade de um aluno escolhido ao acaso tirar uma nota entre 7 e 8,5 está entre o intervalo de 0,5 a 0,83 (não se esqueça de que estamos analisando o resultado entre a média 7 e 8,5). Para descobrir qual é essa probabilidade, existem tabelas padronizadas específicas, assim, procuramos nessa tabela o valor correspondente a ***z - escore*** de 0,83. A seguir, apresentamos uma parte dessa tabela, que poderá ser encontrada em livros ou na internet.

1. Potenciação ou radiciação
2. Multiplicação ou divisão
3. Adição ou subtração

As organizações, na medida em que identificam e conhecem os seus riscos e as ameaças que as colocam em perigo, conseguem planejar as ações necessárias para a elaboração das políticas de segurança e os procedimentos que poderão ajudá-las na redução dos seus riscos.

Após a realização de uma análise de custo-benefício, a organização poderá tomar qualquer medida que vise diminuir o seu grau de exposição diante de um determinado problema.

Dependendo do custo, se ele for mais alto que o dano que a ameaça poderá causar, essa ameaça não merecerá ser combatida.

A análise de um determinado tipo de risco varia de pessoa para pessoa, assim como também nas organizações, cada uma enxerga o risco sob um determinado ponto de vista e é por isso que existem diversas formas, maneiras e mecanismos para que um risco possa ser avaliado.

Para que possamos tratar do assunto análise de risco, faz-se necessário que algumas palavras que são utilizadas nesse assunto sejam explicadas, pois a má interpretação delas termina por comprometer as ações de segurança a ser implementadas.

- **Risco** – Pode ser definido como um perigo ou possibilidade de que esse perigo ocorra. Também podemos dizer que é a probabilidade de acontecer ou não algo, pela exploração dos pontos fracos que um determinado ambiente possa ter, provocando assim possíveis problemas financeiros e impactos aos negócios da organização.

## Exemplos: resolvendo expressões numéricas com números inteiros

Tabela:



a) - [ - 3 + 2 - (4 - 5 - 6)]=
- [ - 3 + 2 - 4 + 5 + 6 ] =
3 - 2 + 4 - 5 - 6 = 7 - 13 = - 6

Primeiros eliminamos os parênteses; como antes dele tinha um sinal de menos, todos os números saíram com sinais trocados. Logo depois eliminamos os colchetes; como também tinha um sinal de menos, todos os números saíram com os sinais trocados, e somamos os positivos e os negativos.

b) { - 5 + [ - 8 + 3 x (- 4 + 9) - 3 ] } =
{ - 5 + [ - 8 + 3 x (+ 5 ) - 3 ] } =
{ - 5 + [ - 8 + 15 - 3] } =
{ - 5 - 8 + 15 - 3} =
- 5 - 8 + 15 - 3 =
- 16 + 15 = 1

Primeiro resolvemos as operações dentro dos parênteses, depois multiplicamos o resultado por 3 . Logo depois, eliminamos os colchetes; como antes dele tinha um sinal de mais, todos os números saíram sem trocar de sinal, e eliminamos também as chaves. Observe que também não teve troca de sinais pelo mesmo motivo anterior, e juntamos positivo com negativos.

- Uma expressão numérica é algo como se alguém tivesse anotado, em uma única linha, alguns cálculos a serem efetuados.

  Exemplo:

  2 + 3 x 4 – 1 + 8

- O que muitas vezes nos faz errar esses cálculos é a ordem em que devemos efetuar cada uma das contas da expressão numérica.
- Precisamos seguir a ordem certa, para o resultado ser correto.

| z | 0 | 0,01 | 0,02 | 0,03 | 0,04 | 0,05 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0,0040 | 0,0080 | 0,0120 | 0,0160 | 0,0199 |
| 0,1 | 0,0398 | 0,0438 | 0,0478 | 0,0517 | 0,0557 | 0,0596 |
| 0,2 | 0,0793 | 0,0832 | 0,0872 | 0,091 | 0,0948 | 0,0987 |
| 0,3 | 0,1179 | 0,1217 | 0,1255 | 0,1293 | 0,1331 | 0,1368 |
| 0,4 | 0,1554 | 0,1591 | 0,1628 | 0,1664 | 0,1700 | 0,1736 |
| 0,5 | 0,1915 | 0,195 | 0,1985 | 0,2019 | 0,2054 | 0,2088 |
| 0,6 | 0,2257 | 0,2291 | 0,2324 | 0,2357 | 0,2389 | 0,2422 |
| 0,7 | 0,2580 | 0,2611 | 0,2642 | 0,2673 | 0,2704 | 0,2734 |
| 0,8 | 0,2881 | 0,2910 | 0,2939 | 0,2967 | 0,2995 | 0,3023 |
| 0,9 | 0,3159 | 0,3186 | 0,3212 | 0,3238 | 0,3264 | 0,3289 |
| 1,0 | 0,3413 | 0,3438 | 0,3461 | 0,3485 | 0,3508 | 0,3531 |
| 1,1 | 0,3643 | 0,3665 | 0,3686 | 0,3708 | 0,3729 | 0,3749 |
| 1,2 | 0,3849 | 0,3869 | 0,3888 | 0,3907 | 0,3925 | 0,3944 |
| 1,3 | 0,4032 | 0,4049 | 0,4066 | 0,4082 | 0,4099 | 0,4115 |

Encontrando o número 0,8 na coluna à esquerda e depois cruzando a fileira com a coluna 0,03, encontramos o valor 0,2967. Então, a área à esquerda é correspondente a
z = 0,83 é 0,2967.

Exemplo:

15 + 7 + 12 –13 =

22 + 12 – 13 =

34 – 13 = 21

• Efetuamos as multiplicações antes das adições.

Exemplo:

28 + 7 + 15 x 3 =

28 + 7 + 45 =

35 + 45 = 80

• Efetuamos a divisão antes da subtração.

Exemplo:

87 – 36 : 3 – 8 =

87 – 12 – 8 =

75 – 8 = 67

• Efetuamos a multiplicação e a divisão antes da adição e da subtração.

2 + 3 • 4 – 1 + 8 : 2 =

2 + 12 – 1 + 4 =

14 – 1 + 4 =

13 + 4 = 17


- Para determinarmos uma expressão numérica em que apareça potenciação, efetua-se primeiramente a potenciação, logo se efetua as divisões e multiplicações, e por fim a subtração e adição.
- Para chegarmos ao valor numérico de uma expressão numérica, é preciso obedecer às regras de resolução de uma expressão aritmética ou numérica, e quando encontramos em sua estrutura uma potência é preciso dar preferência a ela.

## Exemplos:

Então, a probabilidade de um aluno escolhido ao acaso ter uma nota 7 e 8,5 é de 29,67%.

## Representação gráfica da curva normal

1) $3 \cdot \{ 4^3 - [ 5 \cdot 6^0 + 7 \cdot ( 9^2 - 80 ) ] \} =$
$3 \cdot \{ 64 - [ 5 \cdot 1 + 7 \cdot ( 81 - 80 ) ] \} =$
$3 \cdot \{ 64 - [ 5 + 7 \cdot 1 ] \} =$
$3 \cdot \{ 64 - [ 5 + 7 ] \} =$
$3 \cdot \{ 64 - 12 \} =$
$3 \cdot 52 = 156$

Nessa expressão aritmética ou numérica iremos resolver as potências $4^3$, $6^0$ e $9^2$ antes de qualquer outra operação.

Depois de eliminas todas as potências, é preciso aplicar as regras de resolução.

2) $( 3^3 + 3 \cdot 7 )^2 : \{ 4 \cdot [ 800 - ( 3^2 \cdot 2 + 10 )^2 ] \} =$
$( 27 + 3 \cdot 7 )^2 : \{ 4 \cdot [ 800 - ( 9 \cdot 2 + 10 )^2 ] \} =$
$( 27 + 21 )^2 : \{ 4 \cdot [ 800 - ( 18 + 10 )^2 ] \} =$
$2304 : \{ 4 \cdot [ 800 - 784 ] \} =$
$2304 : \{ 4 \cdot 16 \} =$
$2304 : 64 = 36$

Nessa expressão numérica iremos resolver as potências $3^3$ e $3^2$ antes de qualquer outra operação.

Para resolvermos as potências $( 27 + 3 \cdot 7 )^2$ e $( 9 \cdot 2 + 10 )^2$, é preciso resolver as operações que estão dentro dos parênteses.

Para entender o conceito, assista ao vídeo abaixo. Este vídeo faz parte da sequência desta aula e, portanto, é essencial para a aprendizagem.

objeto disponível apenas na versão web

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

objeto disponível apenas na versão web

Como já dissemos, essa curva é simétrica em relação à média, portanto, os pontos são equidistantes do centro.

Essa é a importância de identificarmos possíveis riscos, poder antecipar os problemas e implementar controles que ajudarão a evitar a realização da situação de insegurança.

É difícil ter uma visão total de todos os aspectos que o risco afetará em um determinado processo, bem como visualizar todas as consequências que a sua incidência acarretará, uma vez que existe a variável probabilidade, que poderá aumentar ou diminuir o grau de incerteza.

Além disso, essa curva tem uma ordenada máxima situada na média.

Em uma distribuição normal podemos ter qualquer média ou desvio-padrão desde que sejam positivos; essas medidas determinam o formato da curva.

## Processo de análise de risco

A média indica o local do eixo de simetria e o desvio-padrão apresenta o quanto os dados estão alargados.

Fica impossível fazer uma análise de risco sem que se conheça o negócio a ser protegido e, dessa forma, existe a necessidade de que sejam estudados minuciosamente os principais processos de negócio que sustentam a organização.

Com a visão dos processos de negócios consegue-se identificar as dependências que eles têm dos ativos que suportam as informações e com isso identificam-se as prioridades das ações de segurança a serem realizadas.

Antes de continuar, sentimos novamente a necessidade de conceituar algumas palavravas que farão parte do nosso processo de análise de risco.

- **Vulnerabilidade –** Pode ser definida como o ponto em que o ativo poderá sofrer um ataque ou ser explorado por parte de uma ameaça. Todo ativo possui seu ponto fraco que, se não for protegido, ficará exposto à ação de algo que possa comprometer a sua integridade e segurança.

## Interpretação gráfica de uma distribuição normal

- **Ameaça –** Pode ser definida como algo que possa resultar em um incidente inesperado e que também possa causar danos e prejuízos a uma organização quando explorar uma determinada vulnerabilidade de um ativo importante de um processo de negócio da organização.

Normalmente é difícil evitar a existência das ameaças, porém podem ser implementadas ações que visem à diminuição da sua existência, bem como a possibilidade de sua ação diante da vulnerabilidade de um ativo.

Podemos classificar os tipos de ameaças como: ameaças geradas pelos fenômenos da natureza, ameaça física, ameaça não intencional e ameaça proposital.

O primeiro tipo de ameaça está relacionado àquelas que envolvem fenômenos de natureza, como: chuva, fogo, furacão, terremoto, raio, tempestade, avalanche, desmoronamento.

As ameaças tipificadas como físicas envolvem um tipo de ação causada por um agente externo, por exemplo: desvio de mensagens; roubo físico de equipamentos; acidentes aéreo, terrestre, industrial ou marítimo; explosões e acidentes.

No tipo de ameaça não intencional, a situação ocorre sem que o envolvido geralmente saiba, em virtude de sua ignorância durante o momento em que a ameaça se concretiza, por exemplo: o não entendimento de um manual ou documentação; esquecimento de um micro destravado com informação sigilosa sendo exibida; documentos jogados nos lixo sem a devida proteção.

O pior tipo de ameaça é o último a ser explicado e está relacionado a uma ação de algo ou alguém contra uma vulnerabilidade existente de forma proposital, com fins claros de causar algum dano ao alvo.

Podemos citar como exemplos: roubo de arquivos, discos, fitas, listagens, cópia ou pirataria de dados, pessoas mal-intencionadas alterando informações dos sistemas desprotegidos. Geralmente esse tipo de ameaça está associado a uma ação física do atacante contra o seu alvo, por exemplo:

Observamos na curva de distribuição normal que, conforme vamos nos afastando da média, as frequências vão diminuindo, portanto, a probabilidade de encontrar valores mais afastados da média diminui.

- **Impactos –** É o conceito utilizado para medir os efeitos, positivos ou negativos, que uma determinada atividade pode causar. Isso mesmo, existem situações em que um impacto pode ter efeito positivo, como o impacto de uma vitória aos últimos minutos do jogo de futebol para o time vencedor, que será o oposto do que é sentido pelo time que veio a perder e com certeza esse impacto será negativo no emocional desse grupo. Perdas financeiras, abalo na imagem, multas ou sanções, perda de investidores, prejuízo operacional, paradas no negócio da empresa, redução da margem de lucro etc. são alguns exemplos de impactos.

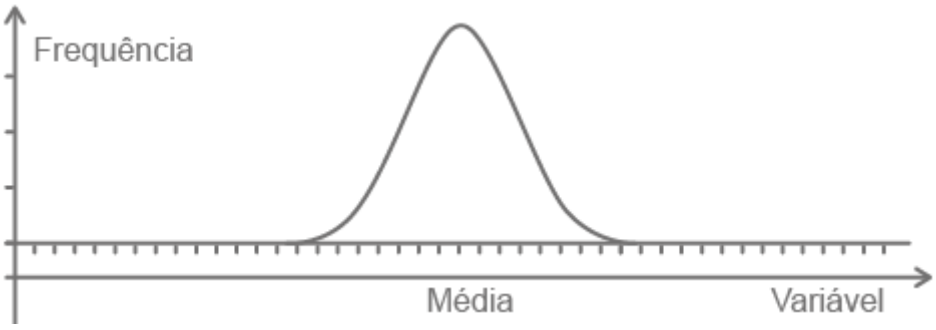
Para finalizar, é importante que tenhamos em mente as principais etapas do processo de análise de risco, que consiste em: entender/conhecer o escopo do projeto e dentro desse escopo identificar os principais ativos que suportam os processos de negócio. Identificar as principais vulnerabilidades dos ativos, bem como as ameaças que possam explorar os pontos fracos. Reconhecer os impactos ao negócio, caso o risco se concretize e determine a probabilidade da sua ocorrência.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento.
Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

objeto disponível apenas na versão web

A seguir, preencha a(s) lacuna(s) com a(s) palavra(s) adequada(s) às afirmações.

objeto disponível apenas na versão web




Como já dissemos, uma curva normal é simétrica em torno da média, dessa forma, podemos fazer estimativas a partir de uma dada probabilidade ou área.

Estimule seu raciocínio com o jogo da forca, clique no botão a seguir.

objeto disponível apenas na versão web

Para memorizar os conhecimentos adquiridos nesta aula, clique no botão a seguir e resolva o teste proposto.


Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.


## Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação*: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de Serviços de TI na Prática*: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2003.