ISO/IEC 27005:2011

TECNOLOGIA DA INFORMAÇÃO - TÉCNICAS DE SEGURANÇA
GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

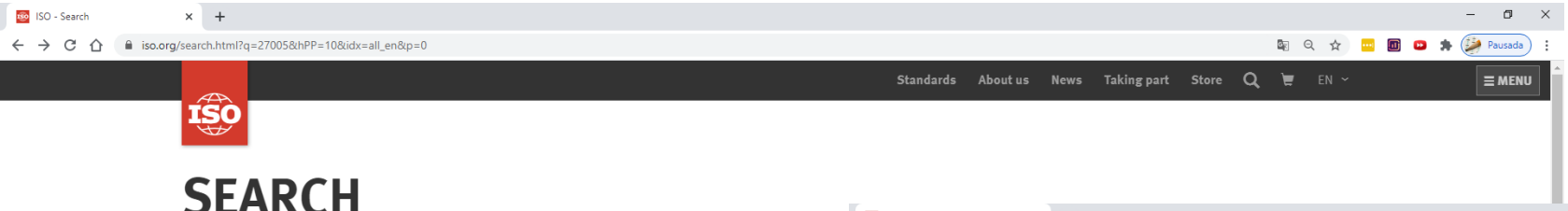
Prof. Luis Claudio, M.Sc., PMP®

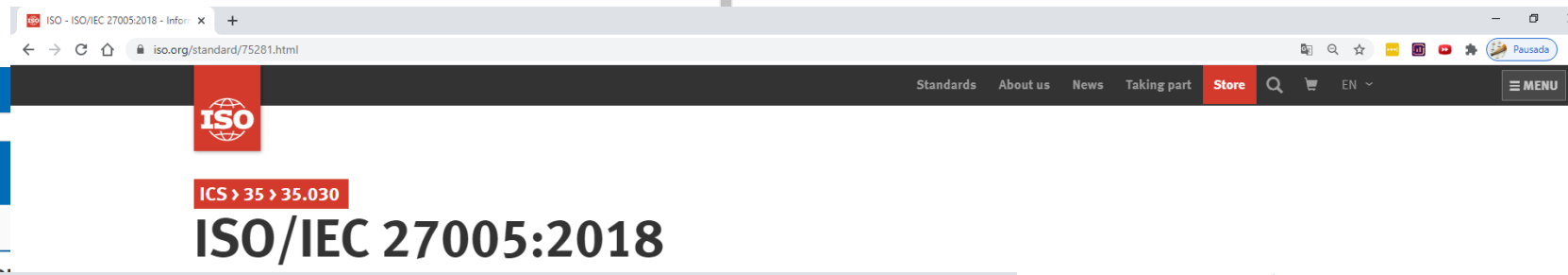
A Família 27000

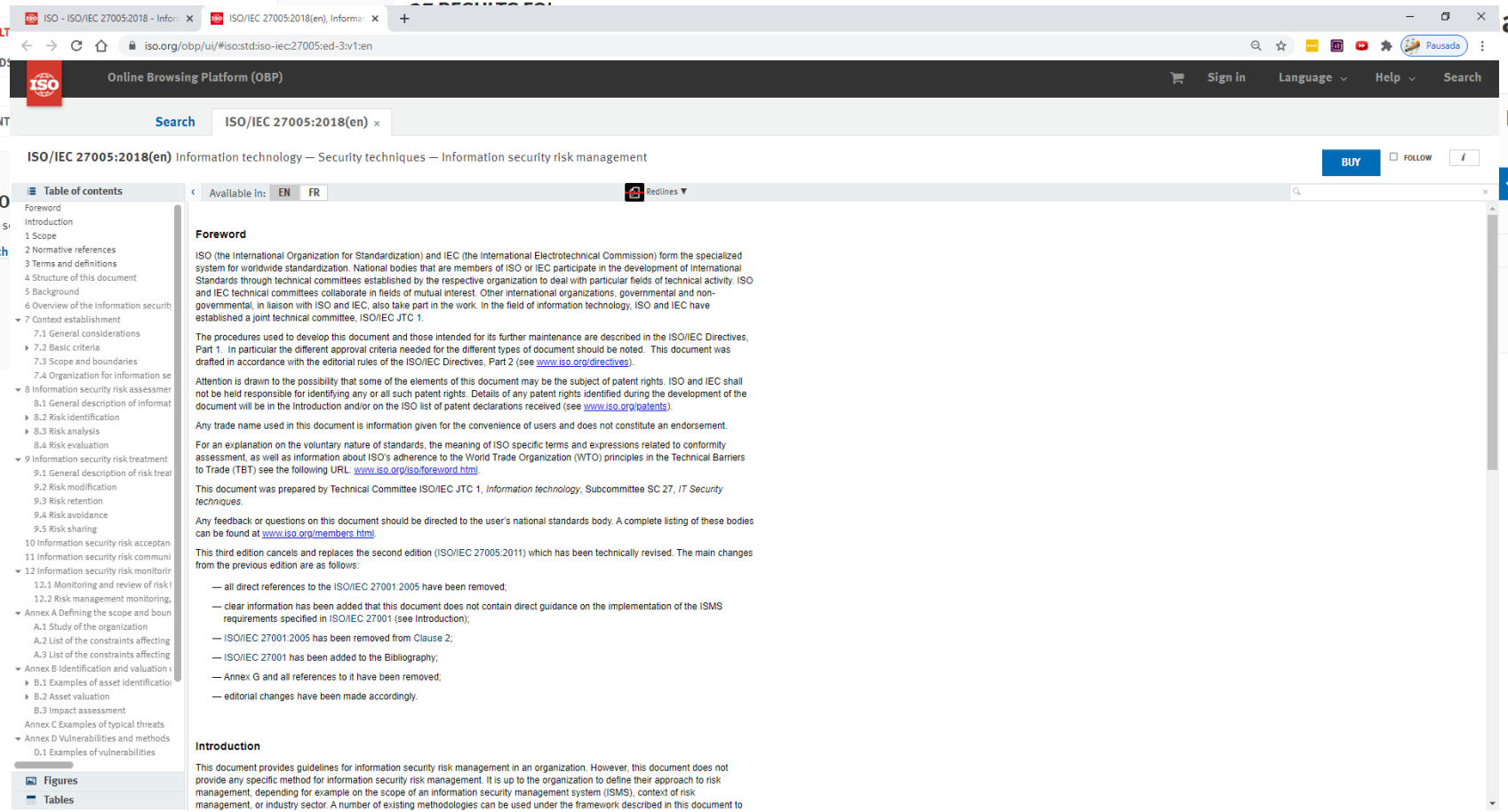
ISO/IEC 27000:2018
Information security management systems — Overview and vocabulary
ISO/IEC 27001:2013
Information security management systems — Requirements
ISO/IEC 27002:2013
Code of practice for information security controls
ISO/IEC 27003:2017
Information security management systems — Guidance
ISO/IEC 27004:2016
Information security management — Monitoring, measurement, analysis and evaluation
ISO/IEC 27005:2018
Information security risk management
ISO/IEC 27006:2015/AMD 1:2020
Requirements for bodies providing audit and certification of information security management systems — Amendment 1

A Família 27000

ISO/IEC 27007:2020
Information security, cybersecurity and privacy protection — Guidelines for information SMS auditing
ISO/IEC TS 27008:2019
Guidelines for the assessment of information security controls
ISO/IEC 27009:2020
Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements
ISO/IEC 27010:2015
Information security management for inter-sector and inter-organizational communications
…
ISO/IEC TR 27015:2012
Information security management guidelines for financial services [*Withdrawn*]
…
ISO/IEC CD 27030
Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT)Title missing [*Under development*]

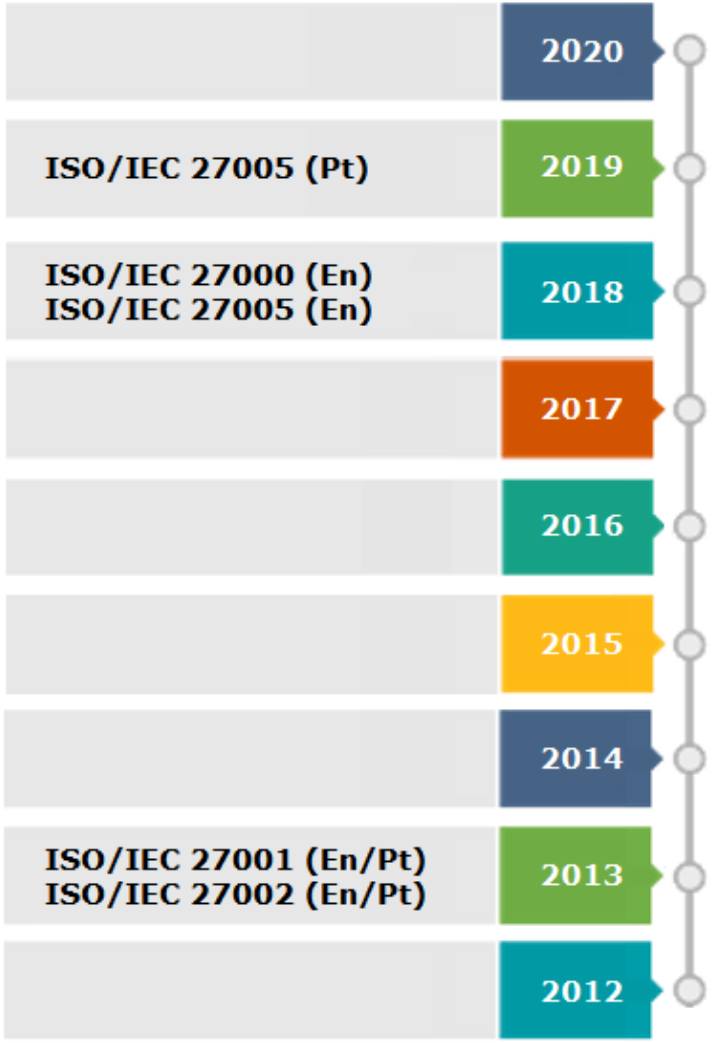

ISO - Search
iso.org/search.html?q=27005&hPP=10&idx=all_en&p=0
Standards
About us
News
Taking part
Store
EN
MENU
SEARCH
I'M LOOKING FOR
27005
FILTER
ALL RESULT
STANDARD
NEWS (2)
DOCUMENT
LOOKING FO
Customize your s
Advanced search


ISO - ISO/IEC 27005:2018 - Infor
iso.org/standard/75281.html
Standards
About us
News
Taking part
Store
EN
MENU
ICS › 35 › 35.030
ISO/IEC 27005:2018
ation security risk


ISO - ISO/IEC 27005:2018 - Infor
ISO/IEC 27005:2018(en), Informa
iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en
Online Browsing Platform (OBP)
Sign in
Language
Help
Search
Search
ISO/IEC 27005:2018(en)
ISO/IEC 27005:2018(en) Information technology — Security techniques — Information security risk management
BUY
FOLLOW
Table of contents
Available in: EN FR
Redlines
Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this document
5 Background
6 Overview of the information securit
7 Context establishment
7.1 General considerations
7.2 Basic criteria
7.3 Scope and boundaries
7.4 Organization for information se
8 Information security risk assessmer
8.1 General description of informat
8.2 Risk identification
8.3 Risk analysis
8.4 Risk evaluation
9 Information security risk treatment
9.1 General description of risk treat
9.2 Risk modification
9.3 Risk retention
9.4 Risk avoidance
9.5 Risk sharing
10 Information security risk acceptan
11 Information security risk communi
12 Information security risk monitorir
12.1 Monitoring and review of risk
12.2 Risk management monitoring,
Annex A Defining the scope and boun
A.1 Study of the organization
A.2 List of the constraints affecting
A.3 List of the constraints affecting
Annex B Identification and valuation
B.1 Examples of asset identificatio
B.2 Asset valuation
B.3 Impact assessment
Annex C Examples of typical threats
Annex D Vulnerabilities and methods
D.1 Examples of vulnerabilities
Figures
Tables
Foreword
ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).
Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).
Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.
For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.
This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.
This third edition cancels and replaces the second edition (ISO/IEC 27005:2011) which has been technically revised. The main changes from the previous edition are as follows:
— all direct references to the ISO/IEC 27001:2005 have been removed;
— clear information has been added that this document does not contain direct guidance on the implementation of the ISMS requirements specified in ISO/IEC 27001 (see Introduction);
— ISO/IEC 27001:2005 has been removed from Clause 2;
— ISO/IEC 27001 has been added to the Bibliography;
— Annex G and all references to it have been removed;
— editorial changes have been made accordingly.
Introduction
This document provides guidelines for information security risk management in an organization. However, this document does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of an information security management system (ISMS), context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this document to
BUY THIS STANDARD
FORMAT
LANGUAGE
PDF + EPUB
English
PDF + REDLINE
English
PAPER
English
CHF 178
BUY


ABNT Catalogo
abntcatalogo.com.br/default.aspx
Conheça a ABNT
Catálogo
Coleção
Fale Conosco
ABNTCatálogo
Segurança, Qualidade, Padrão e Confiança
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS
Início
Meu cadastro
Meus pedidos
Meu carrinho
Perguntas Frequentes
ONLINE
Curso Lead Implementer para a Gestão da Privacidade da Informação (Baseado na ABNT
ABNTCOLEÇÃO, CONHEÇA!
Normas
Cursos
ABNT Catalogo
abntcatalogo.com.br/norma.aspx?ID=429058
ABNT - ABNTColeção
Não seguro | abnt.org.br/assinatura-de-normas-tecnicas
Seguir
Like 599K
PESQUISAR
Número da norma ou palavra chave
HOME
INSTITUCIONAL
NORMALIZAÇÃO
CERTIFICAÇÃO
CURSOS
ASSOCIE-SE
INFORMAÇÕES TECNOLÓGICAS
LOJA
CONTATO
Página Principal
ABNTColeção
Assinatura Normas Técnicas
ABNTCOLEÇÃO
ABNTColeção
O que é o ABNTColeção?
É um sistema digital multiusuário que permite acesso as Normas Técnicas totalmente via web.
Para quem o ABNTColeção foi desenvolvido?
Profissionais que precisam de acesso rápido as Normas Técnicas em formato digital de onde estiverem. O ABNTColeção foi criado para facilitar e ajudar estes profissionais a serem mais eficientes e eficazes em seus processos.
Loja
ABNTColeção
Certificação
Cursos
Normas Técnicas
Publicações
Normas ABNT
Normas Internacionais/Estrangeiras
Normas Personalizadas
Parcerias
Meu carrinho
Perguntas Frequentes
ABNTCOLEÇÃO, CONHEÇA!
CURSOS (1 item)
PUBLICAÇÕES (2 itens)
Acesso online às normas técnicas de onde você estiver!
DEMONSTRAÇÃO GRATUITA
CLIQUE AQUI!
Para mais informações:
colecao@abnt.org.br
(11) 3017-3652

A Família 27000



Seção 0 - Introdução

A Norma fornece diretrizes para a criação do processo de Gestão de Riscos, MAS, não fornece uma metodologia.

“Há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita nesta Norma” ISO/IEC 27005/2018.

Seção 1 - Escopo

É importante conhecer a ISO 27001 e a 27002.

A Norma se aplica a todo tipo de Organização.

Seção 2 - Referências

São indispensáveis para a correta aplicação da 27005:

ABNT NBT ISO/IEC 27001:2006

ABNT NBT ISO/IEC 27002:2005

Seção 3 - Termos e Definições

3.1 consequência
resultado de um evento (3.3) que afeta os objetivos

[ABNT ISO GUIA 73:2009]
NOTA 1 Um evento pode levar a uma série de consequências.
NOTA 2 Uma consequência pode ser certa ou incerta e, no contexto da segurança da informação, é, normalmente, negativa.
NOTA 3 As consequências podem ser expressas qualitativa ou quantitativamente.
NOTA 4 As consequências iniciais podem desencadear reações em cadeia.

Seção 3 - Termos e Definições

3.7 probabilidade (likelihood)
chance de algo acontecer

[ABNT ISO GUIA 73:2009]
NOTA 1 Na terminologia de gestão de riscos, a palavra "probabilidade" é utilizada para referir-se à chance de algo acontecer, não importando se, de forma definida, medida ou determinada, objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo).
NOTA 2 O termo em Inglês "likelihood" não têm um equivalente direto em algumas línguas; em vez disso, o equivalente do termo "probability" é frequentemente utilizado. Entretanto, em Inglês, "probability" é muitas vezes interpretado estritamente como uma expressão matemática. Portanto, na terminologia de gestão de riscos, "likelihood" é utilizado com a mesma ampla interpretação de que o termo "probability" tem em muitos outros idiomas além do Inglês.

Seção 3 - Termos e Definições

3.9 risco
efeito da incerteza nos objetivos

[ABNT ISO GUIA 73:2009]
NOTA 1 Um efeito é um desvio em relação ao esperado – positivo e/ou negativo.
NOTA 2 Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).
NOTA 3 O risco é muitas vezes caracterizado pela referência aos eventos (3.3) potenciais e às consequências (3.1), ou uma combinação destes.
NOTA 4 O risco em segurança da informação é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade (likelihood) (3.7) associada de ocorrência.
NOTA 5 A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.
NOTA 6 O risco de segurança da informação está associado com o potencial de que ameaças possam explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, consequentemente, causar dano a uma organização.

Seção 3 - Termos e Definições

3.6 nível de risco
magnitude de um risco (3.9), expressa em termos da combinação das consequências (3.1) e de suas probabilidades (likelihood) (3.7)

[ABNT ISO GUIA 73:2009]

Seção 3 - Termos e Definições

3.2 controle
medida que está modificando o risco (3.9)

[ABNT ISO GUIA 73:2009]
NOTA 1 Os controles da segurança da informação incluem qualquer processo, política, procedimento, diretriz, prática ou estrutura organizacional, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modificam o risco da segurança da informação.
NOTA 2 Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.
NOTA 3 O controle também é usado como um sinônimo de salvaguarda ou contramedida.

Seção 3 - Termos e Definições

3.17 tratamento de riscos
processo para modificar o risco

[ABNT ISO GUIA 73:2009]
NOTA 1 O tratamento de risco pode envolver:
- *a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco;*
- *assumir ou aumentar o risco, a fim de buscar uma oportunidade;*
- *a remoção da fonte de risco;*
- *a alteração da probabilidade (likelihood);*
- *a alteração das consequências;*
- *o compartilhamento do risco com outra parte ou partes [incluindo contratos e financiamento do risco]; e*
- *a retenção do risco por uma escolha consciente.*

NOTA 2 Os tratamentos de riscos relativos a consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos".
NOTA 3 O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

Seção 3 - Termos e Definições

3.8 risco residual
risco (3.9) remanescente após o tratamento do risco (3.17)

[ABNT ISO GUIA 73:2009]
NOTA 1 O risco residual pode conter riscos não identificados.
NOTA 2 O risco residual também pode ser conhecido como "risco retido".

Seção 3 - Termos e Definições

3.3 evento

ocorrência ou mudança em um conjunto específico de circunstâncias

[ABNT ISO GUIA 73:2009]
NOTA 1 Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas.
NOTA 2 Um evento pode consistir em alguma coisa não acontecer.
NOTA 3 Um evento pode algumas vezes ser referido como um "incidente" ou um "acidente".

Seção 3 - Termos e Definições

3.4 contexto externo

ambiente externo no qual a organização busca atingir seus objetivos

[ABNT ISO GUIA 73:2009]
NOTA O contexto externo pode incluir:
— o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local;
— os fatores–chave e as tendências que tenham impacto sobre os objetivos da organização; e
— as relações com partes interessadas externas e suas percepções e valores.

Seção 3 - Termos e Definições

3.5 contexto interno

ambiente interno no qual a organização busca atingir seus objetivos

[ABNT ISO GUIA 73:2009]
NOTA O contexto interno pode incluir:
— governança, estrutura organizacional, funções e responsabilidades;
— políticas, objetivos e estratégias implementadas para atingi-los;
— capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);
— sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);
— relações com partes interessadas internas, e suas percepções e valores;
— cultura da organização;
— normas, diretrizes e modelos adotados pela organização; e
— forma e extensão das relações contratuais.

Seção 3 - Termos e Definições

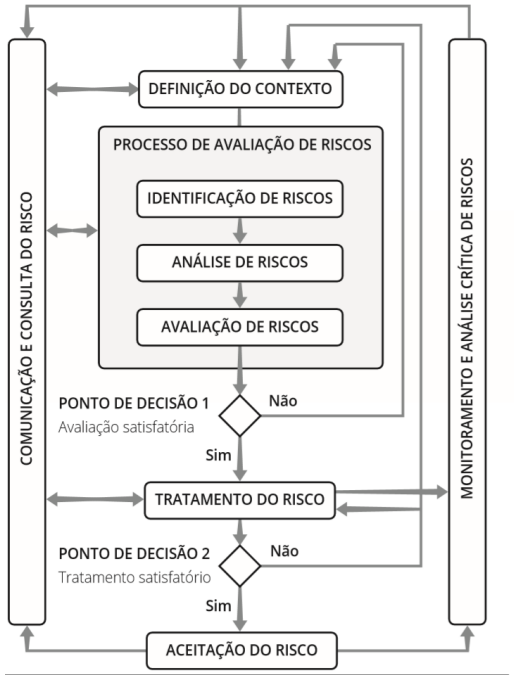
3.18 parte interessada
pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade

[ABNT ISO GUIA 73:2009]
NOTA Um tomador de decisão pode ser uma parte interessada.

Seção 3 - Termos e Definições

3.16 gestão de riscos
atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos

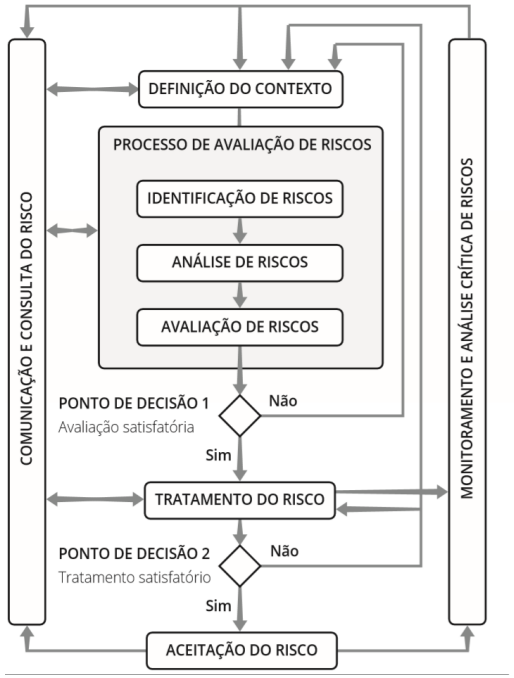
[ABNT ISO GUIA 73:2009]
NOTA Esta Norma usa o termo "processo" para descrever toda a gestão de riscos. Os elementos contidos no processo de gestão de riscos foram chamados de "atividades".



Seção 3 - Termos e Definições

3.11 processo de avaliação de riscos
processo global de identificação de riscos (3.15), análise de riscos (3.10) e avaliação de riscos (3.14)

[ABNT ISO GUIA 73:2009]

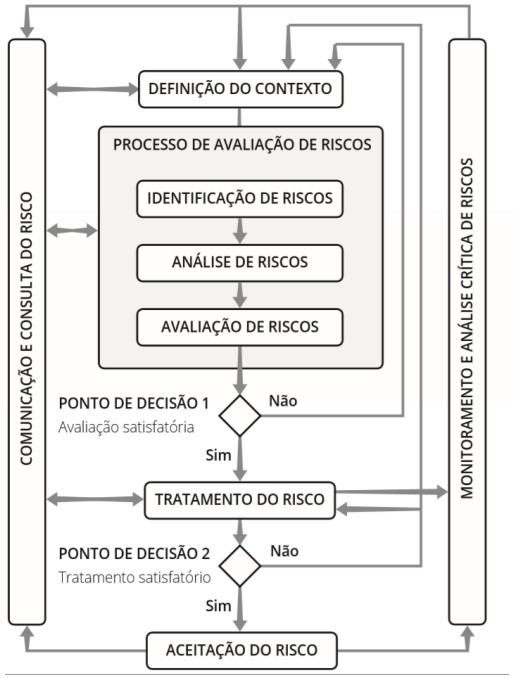


Seção 3 - Termos e Definições

3.13 critérios de risco
termos de referência contra os quais a significância de um risco (3.9) é avaliada

3.15 identificação de riscos
processo de busca, reconhecimento e descrição de riscos

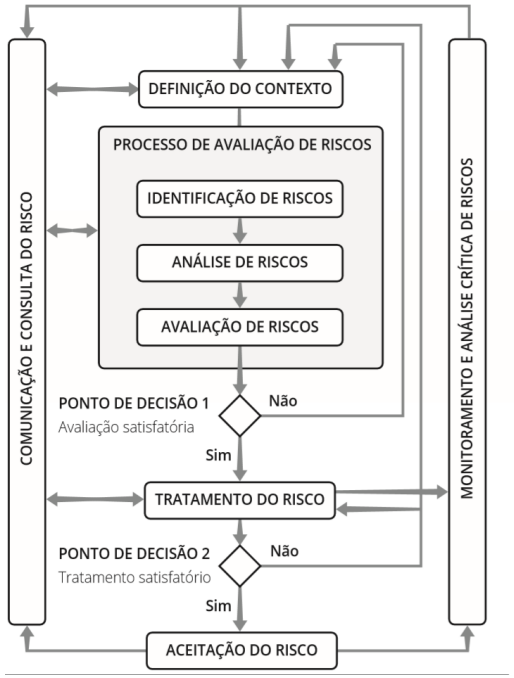
3.14 avaliação de riscos
processo de comparar os resultados da análise de riscos (3.10) com os critérios de risco (3.13) para determinar se o risco e/ou sua magnitude é aceitável ou tolerável



Seção 3 - Termos e Definições

3.10 análise de riscos
processo de compreender a natureza do risco e determinar o nível de risco (3.6)

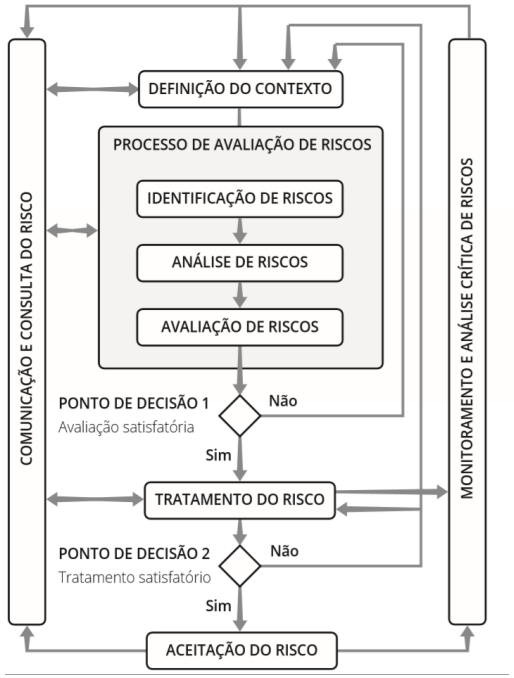
3.12 comunicação e consulta
processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações, e se envolver no diálogo com as partes interessadas (3.18), com relação a gerenciar riscos (3.9)



Seção 4 – Organização da Norma

A norma contém a descrição do processo e de suas atividades.
Seção 5 – Contextualização
Seção 6 – Visão geral do processo de gestão de riscos de SI.

As atividades descritas na seção 6, compõem as seções:
Seção 7 – Definição do contexto
Seção 8 – Análise/avaliação de riscos
Seção 9 – Tratamento do risco
Seção 10 – Aceitação do risco
Seção 11 – Comunicação do risco
Seção 12 – Monitoramento e análise crítica de riscos



Seção 5 – Contextualização

A abordagem de gestão de riscos de segurança da informação deve ser sistemática e adequada ao ambiente da organização.

A gestão de riscos de SI precisa ser parte integrante do próprio sistema de gestão de segurança da informação.

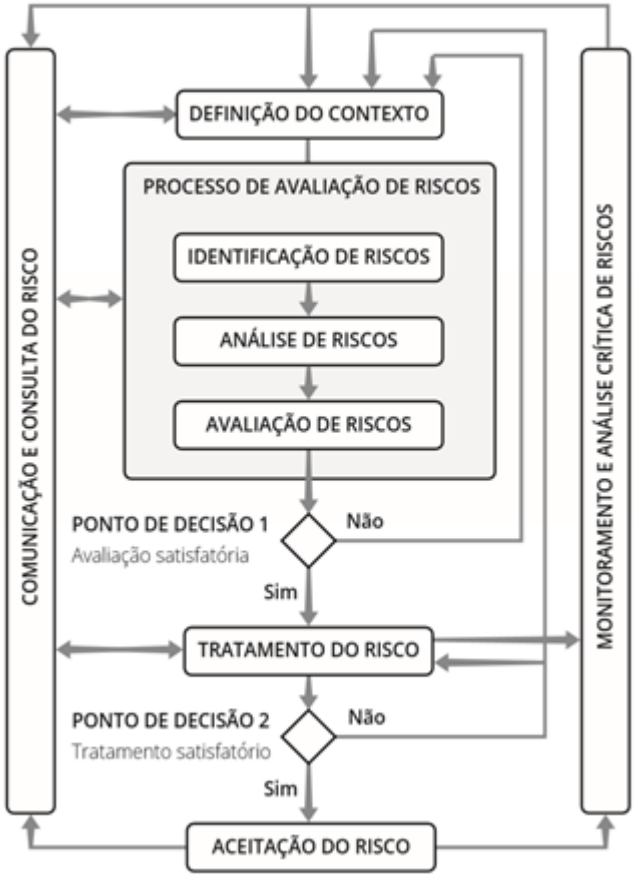
O processo de Gestão de Riscos de Segurança da Informação pode ser aplicado à **organização como um todo**, a uma **área específica da organização**, a **um sistema de informações**, a **controles já existentes**, planejados ou **apenas a aspectos particulares** de um controle.

Seção 5 – Contextualização

A Gestão de Riscos de SI deve contribuir para:

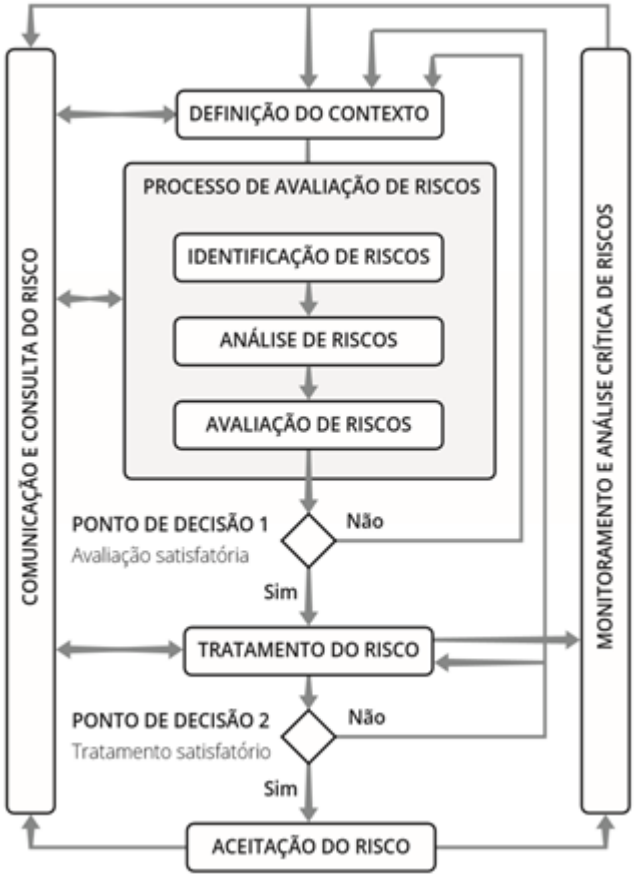
1) Identificação de riscos;
2) Análise/avaliação de riscos;
3) Comunicação e entendimento dos riscos;
4) Estabelecimento prioridade para tratamento do risco;
5) Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas;
6) Eficácia do monitoramento do tratamento do risco;
7) Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos;
8) Coleta de informações de forma a melhorar a gestão de riscos;
9) Treinamento de gestores e pessoal.

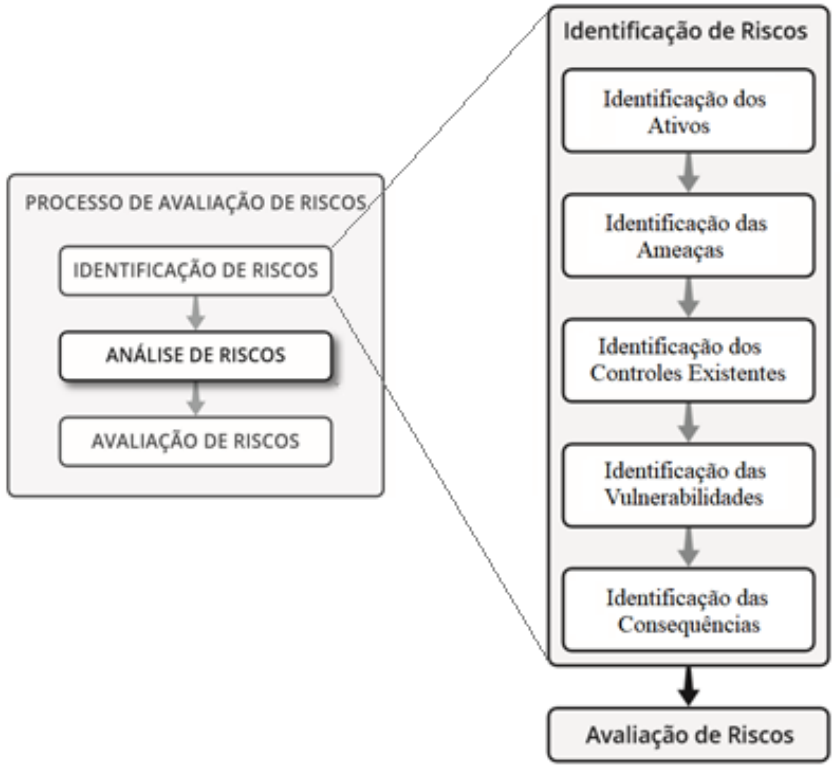
Seção 6 – Visão Geral da Gestão de Riscos de SI



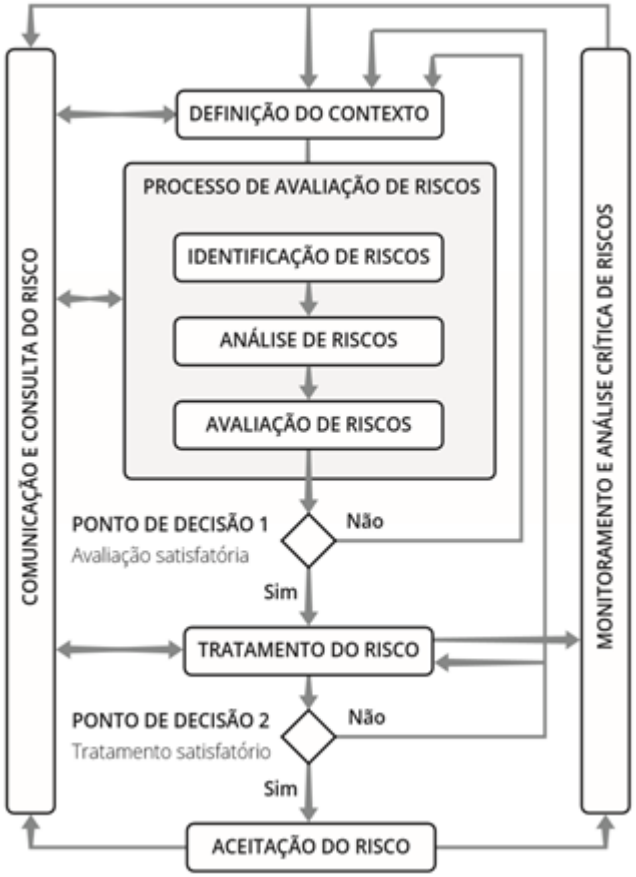
Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Análise/avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

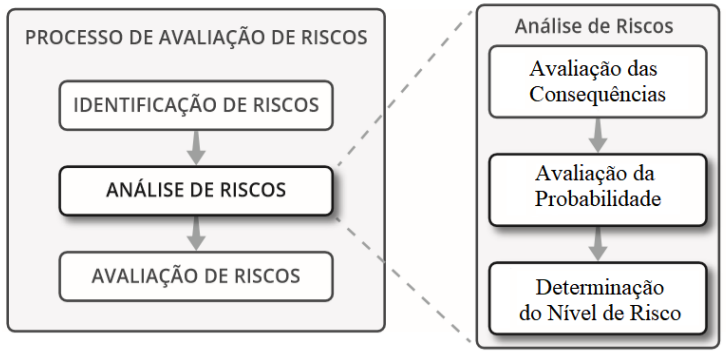
Seção 6 – Visão Geral da Gestão de Riscos de SI



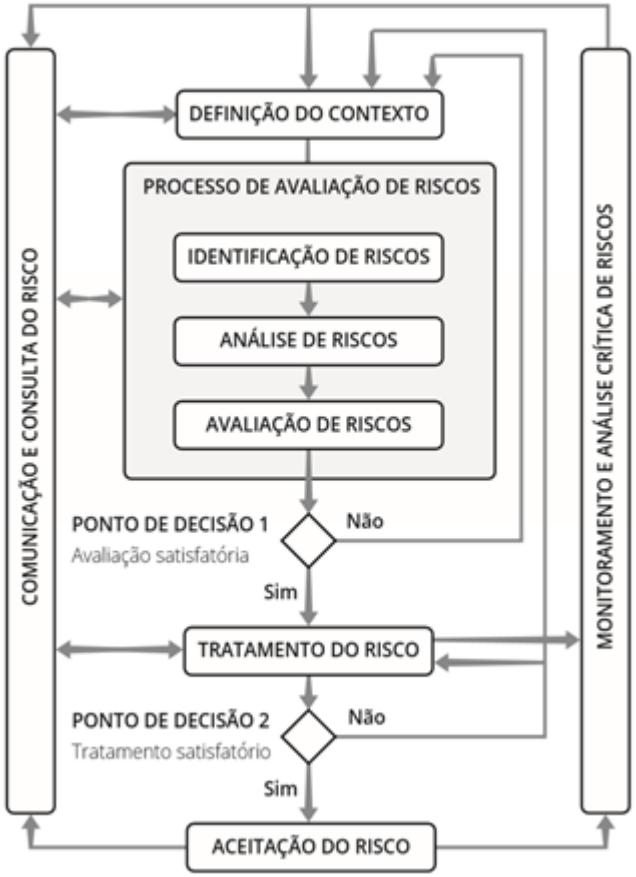


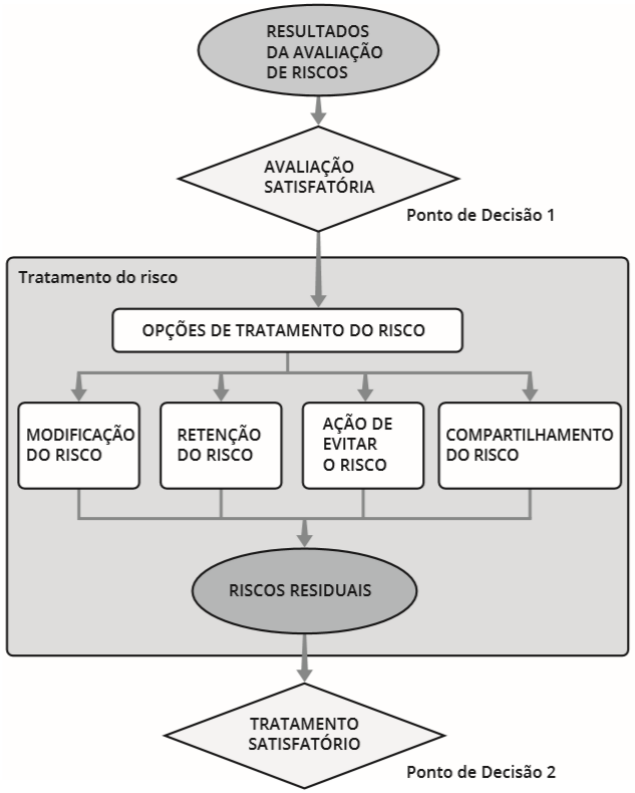
Seção 6 – Visão Geral da Gestão de Riscos de SI





Seção 6 – Visão Geral da Gestão de Riscos de SI





Questão 01

Com relação à Norma NBR 27005:2011, julgue o item a seguir

A Gestão de Riscos de Segurança da Informação pode ser aplicada de forma abrangente a toda uma organização ou, por outro lado, de forma mais específica a apenas uma área e até mesmo a apenas um único sistema.

Questão 02

A Norma NBR 27005:2011 descreve um processo de gestão de riscos de segurança da informação composto por diversas atividades. Neste contexto, analise as colunas abaixo:

1- Plan	A- Definição do Contexto
2- Do	B- Aceitação do Risco
3- Check	C- Implementação do Plano de Tratamento
4- Act	D- Monitoramento e Análise Crítica

Qual alternativa relaciona corretamente a primeira coluna (Plan – Do – Check - Act) com a segunda coluna (atividades do processo de gestão de riscos) de acordo com esta Norma?

A- 1-A; 2-B; 3-C; 4-D;
B- 1-A; 1-B; 2-C; 3-D;
C- 1-A; 2-B; 3-C; 3-D;
D- 2-A; 2-B; 3-C; 4-D;
E- 2-A; 2-B; 2-C; 3-D;

Questão 03

Julgue os itens subsequentes, relativos às Normas NBR ISO/IEC 15999 e 27005.

A norma NBR ISO/IEC 27005 prescreve que o gerenciamento de incidentes pode ser realizado iniciando-se com uma definição de contexto, seguido por uma análise e avaliação, tratamento, aceitação, comunicação, monitoramento e análise crítica dos incidentes.

Questão 04

Com referência às normas NBR ISO/IEC 15999 e 27005 e a respeito de gestão de riscos, julgue os itens a seguir.

Os processos que fazem parte da análise/avaliação de riscos são identificação de riscos, estimativa de riscos e avaliação de riscos.

Questão 05

De acordo com as normas NBR/ISO/IEC 15999 e 27005, julgue os próximos itens.

De acordo com a norma NBR/ISO/IEC 27005, a comunicação de riscos visa assegurar que as informações sobre os riscos sejam compartilhadas entre os tomadores de decisão e outros *stakeholders,* buscando-se, assim, alcançar um entendimento de todos sobre como os riscos serão gerenciados.

Questão 06

De acordo com as normas NBR/ISO/IEC 15999 e 27005, julgue os próximos itens.

Uma ameaça pode causar impacto em vários ativos ou apenas em parte de um deles, podendo ter efeitos imediatos (operacionais) ou futuros (negócios).

Questão 07

De acordo com a norma NBR ISO/IEC 27005, julgue os próximos itens.

(I) Uma fraqueza em um controle pode ser considerada uma vulnerabilidade;
(II) Fogo, poluição e poeira são exemplos de vulnerabilidades;
(III) Evitar o risco envolve a decisão de não se envolver com uma situação de risco.

Está(ão) correta(s):
A) I, somente.
B) II, somente.
C) I e II, somente.
D) I e III, somente.
E) I, II e III, somente.

Questão 08

Segundo a NBR ISO/IEC 27005, no processo de gestão de riscos da segurança da informação, a definição dos critérios de avaliação de riscos é realizada na atividade

A- definição do contexto.
B- identificação de riscos.
C- análise de riscos.
D- avaliação de riscos.
E- tratamento do risco.

Questão 09

A Norma ISO 27005 fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização. Em relação aos termos e às definições da Norma ISO 27005, numerar a 2ª coluna de acordo com a 1ª e, após, assinalar a alternativa que apresenta a sequência CORRETA:

(1) Comunicação do risco.
(2) Estimativa de riscos.
(3) Transferência do risco.
(4) Retenção do risco.

( ) Aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco.
( ) Troca ou compartilhamento de informação sobre risco entre o tomador de decisão e outras partes interessadas.
( ) Processo utilizado para atribuir valores à probabilidade e às consequências de um risco.
( ) Compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco.

A- 4 - 1 - 2 - 3.
B- 1 - 2 - 3 - 4.
C- 2 - 3 - 4 - 1.
D- 3 - 4 - 1 - 2.

Questão 10

De acordo com a NBR ISO/IEC n.º 27005:2011, o processo para gestão de riscos de segurança da informação consiste em uma série de etapas, e a primeira delas é

A- definir o contexto.
B- avaliar os riscos.
C- tratar os riscos.
D- aceitar as oportunidades.
E- monitorar os riscos.

Questão 11

Julgue o próximo item, relativo à gestão de segurança da informação.

De acordo com a norma NBR ISO/IEC 27005, considera-se risco residual aquele remanescente após o tratamento do risco, podendo o risco residual conter riscos não identificados.

Questão 12

A Norma NBR ISO/IEC 27005 (Tecnologia da Informação – Técnicas de segurança – Gestão de riscos da segurança da informação) estabelece como uma das entradas, em sua seção de Identificação dos Ativos,

A- a lista de componentes, incluindo seus responsáveis.
B- as informações sobre ameaças.
C- o plano de tratamento do risco.
D- uma lista de cenários de incidentes relevantes.
E- uma lista de riscos com prioridades.

Questão 13

A Norma NBR ISO/IEC 27005 (Tecnologia da Informação – Técnicas de segurança – Gestão de riscos da segurança da informação) define, em sua seção de termos e definições, o risco residual como sendo

A- a magnitude do risco, considerando as consequências e suas probabilidades.
B- o risco remanescente após o tratamento do risco inicialmente observado.
C- o processo de compreender a natureza do risco.
D- o processo global de identificação, análise e avaliação de riscos.
E- o processo de busca, reconhecimento e descrição de riscos.

Questão 14

Segundo a NBR ISO/IEC 27005, a opção de tratamento de risco que consiste na possibilidade de aceitação do ônus da perda ou do benefício do ganho associado a determinado risco é denominada

A- redução do risco.
B- retenção do risco.
C- ação de evitar o risco.
D- compartilhamento do risco.
E- transferência do risco.

Gabarito

01 – CORRETO

02 – Alternativa B

03 – INCORRETO

04 – CORRETO

05 – CORRETO

06 – INCORRETO para o CESPE. Acho que foi muito mal escrita...

07 – Alternativa D

08 – Alternativa A

09 – Alternativa A

10 – Alternativa A

11 – CORRETO

12 – Alternativa A

13 – Alternativa B

14 – Alternativa B