Os Termos e Definições da atual **ISO/IEC 27000:2016** (em inglês) podem ser extraídos do próprio site da ISO em https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Há muito mais termos neste glossário do que naqueles que havia anteriormente em cada norma, pois o glossário aqui se preocupa com a definição de termos para toda a família.

Segue abaixo apenas a Seção 2…

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1 - access control
means to ensure that access to assets is authorized and restricted based on business and security requirements (2.63)

2.2 - analytical model
algorithm or calculation combining one or more base measures (2.10) and/or derived measures (2.22) with associated decision criteria (2.21)

2.3 - attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

2.4 - attribute
property or characteristic of an object (2.55) that can be distinguished quantitatively or qualitatively by human or automated means
[SOURCE: ISO/IEC 15939:2007, 2.2, modified — “entity” has been replaced by “object” in the definition.]

2.5 - audit
systematic, independent and documented process (2.61) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).
Note 2 to entry: “Audit evidence” and “audit criteria” are defined in ISO 19011.

2.6 - audit scope
extent and boundaries of an audit (2.5)
[SOURCE: ISO 19011:2011, 3.14, modified — Note 1 to entry has been deleted.]

2.7 - authentication
provision of assurance that a claimed characteristic of an entity is correct

2.8 - authenticity
property that an entity is what it claims to be.

2.9 - availability
property of being accessible and usable upon demand by an authorized entity.

2.10 - base measure
measure (2.47) defined in terms of an attribute (2.4) and the method for quantifying it
[SOURCE: ISO/IEC 15939:2007, 2.3, modified — Note 2 to entry has been deleted.]
Note 1 to entry: A base measure is functionally independent of other measures (2.47).

2.11 - competence
ability to apply knowledge and skills to achieve intended results.

2.12 - confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes (2.61).

2.13 - conformity
fulfilment of a requirement (2.63)
Note 1 to entry: The term “conformance” is synonymous but deprecated.

2.14 - consequence
outcome of an event (2.25) affecting objectives (2.56)
[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified]
Note 1 to entry: An event (2.25) can lead to a range of consequences.
Note 2 to entry: A consequence can be certain or uncertain and in the context of information security (2.33) is usually negative.
Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.
Note 4 to entry: Initial consequences can escalate through knock-on effects.

2.15 - continual improvement
recurring activity to enhance performance (2.59).

2.16 - control
measure that is modifying risk (2.68)
[SOURCE: ISO Guide 73:2009, 3.8.1.1]
Note 1 to entry: Controls include any process (2.61), policy (2.60), device, practice, or other actions which modify risk (2.68).
Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

2.17 - control objective
statement describing what is to be achieved as a result of implementing controls (2.16).

2.18 - correction
action to eliminate a detected nonconformity (2.53).

2.19 - corrective action
action to eliminate the cause of a nonconformity (2.53) and to prevent recurrence.

2.20 - data
collection of values assigned to base measures (2.10), derived measures (2.22) and/or indicators (2.30).
[SOURCE: ISO/IEC 15939:2007, 2.4, modified — Note 1 to entry has been added.]
Note 1 to entry: This definition applies only within the context of ISO/IEC 27004.

2.21 - decision criteria
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result.
[SOURCE: ISO/IEC 15939:2007, 2.7]

2.22 - measure
measure (2.47) that is defined as a function of two or more values of base measures (2.10).
[SOURCE: ISO/IEC 15939:2007, 2.8, modified — Note 1 to entry has been deleted.]

2.23 - documented information
information required to be controlled and maintained by an organization (2.57) and the medium on which it is contained.
Note 1 to entry: Documented information can be in any format and media and from any source.
Note 2 to entry: Documented information can refer to
— the management system (2.46), including related processes (2.61);
— information created in order for the organization (2.57) to operate (documentation);
— evidence of results achieved (records).

2.24 - effectiveness
extent to which planned activities are realized and planned results achieved.

2.25 - event
occurrence or change of a particular set of circumstances
[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry has been deleted.]
Note 1 to entry: An event can be one or more occurrences, and can have several causes.
Note 2 to entry: An event can consist of something not happening.
Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.

2.26 - executive management
person or group of people who have delegated responsibility from the governing body (2.29) for implementation of strategies and policies to accomplish the purpose of the organization (2.57).
Note 1 to entry: Executive management is sometimes called top management (2.84) and can include Chief Executive Officers, Chief Financial Officers, Chief Information Officers, and similar roles.

2.27 - external context
external environment in which the organization seeks to achieve its objectives (2.56)
[SOURCE: ISO Guide 73:2009, 3.3.1.1]
Note 1 to entry: External context can include the following:
— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
— key drivers and trends having impact on the objectives (2.56) of the organization (2.57);
— relationships with, and perceptions and values of, external stakeholders (2.82).

2.28 - governance of information security
system by which an organization’s (2.57)information security (2.33) activities are directed and controlled.

2.29 - governing body
person or group of people who are accountable for the performance (2.59) and conformance of the organization (2.57).
Note 1 to entry: Governing body can in some jurisdictions be a board of directors.

2.30 - indicator
measure (2.47) that provides an estimate or evaluation of specified attributes (2.4) derived from an analytical model (2.2) with respect to defined information needs (2.31).

2.31 - information need
insight necessary to manage objectives (2.56), goals, risks and problems.
[SOURCE: ISO/IEC 15939:2007, 2.12]

2.32 - information processing facilities
any information processing system, service or infrastructure, or the physical location housing it.

2.33 - information security
preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information.
Note 1 to entry: In addition, other properties, such as authenticity (2.8), accountability, non-repudiation (2.54), and reliability (2.62) can also be involved.

2.34 - information security continuity
processes (2.61) and procedures for ensuring continued information security (2.33) operations.

2.35 - information security event
identified occurrence of a system, service or network state indicating a possible breach of information security (2.33) policy (2.60) or failure of controls (2.16), or a previously unknown situation that may be security relevant.

2.36 - information security incident
single or a series of unwanted or unexpected information security events (2.35) that have a significant probability of compromising business operations and threatening information security (2.33).

2.37 - information security incident management
processes (2.61) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (2.36).

2.38 - information sharing community
group of organizations (2.57) that agree to share information
Note 1 to entry: An organization (2.57) can be an individual.

2.39 - information system
applications, services, information technology assets, or other information handling components.

2.40 - integrity
property of accuracy and completeness.

2.41 - interested party
person or organization (2.57) that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

2.42 - internal context
internal environment in which the organization (2.57) seeks to achieve its objectives
[SOURCE: ISO Guide 73:2009, 3.3.1.2]

Note 1 to entry: Internal context can include the following:
— governance, organizational structure, roles and accountabilities;
— policies (2.60), objectives (2.56), and the strategies that are in place to achieve them;
— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes (2.61), systems and technologies);
— information systems (2.39), information flows and decision-making processes (2.61) (both formal and informal);
— relationships with, and perceptions and values of, internal stakeholders (2.82);
— the organization's (2.57) culture;
— standards, guidelines and models adopted by the organization (2.57);
— form and extent of contractual relationships.

2.43 - ISMS project
structured activities undertaken by an organization (2.57) to implement an ISMS.

2.44 - level of risk
magnitude of a risk (2.68) expressed in terms of the combination of consequences (2.14) and their likelihood (2.45)
[SOURCE: ISO Guide 73:2009, 3.6.1.8, modified — “or combination of risks” has been deleted in the definition.]

2.45 - likelihood
chance of something happening
[SOURCE: ISO Guide 73:2009, 3.6.1.1, modified — Notes 1 and 2 to entry have been deleted.]

2.46 - management system
set of interrelated or interacting elements of an organization (2.57) to establish policies (2.60) and objectives (2.56) and processes (2.61) to achieve those objectives
Note 1 to entry: A management system can address a single discipline or several disciplines.
Note 2 to entry: The system elements include the organization’s structure, roles and responsibilities, planning, operation.
Note 3 to entry: The scope of a management system may include the whole of the organization (2.57), specific and identified functions of the organization (2.57), specific and identified sections of the organization (2.57), or one or more functions across a group of organizations (2.57).

2.47 - measure
variable to which a value is assigned as the result of measurement (2.48)
[SOURCE: ISO/IEC 15939:2007, 2.15, modified]
Note 1 to entry: The term “measures” is used to refer collectively to base measures (2.10), derived measures (2.22), and indicators (2.30).

2.48 - measurement
process (2.61) to determine a value.
Note 1 to entry: In the context of information security (2.33), the process (2.61) of determining a value requires information about the effectiveness (2.24) of an information security (2.33)management system (2.46) and its associated controls (2.16) using a measurement method (2.50), a measurement function (2.49), an analytical model (2.2), and decision criteria (2.21).

2.49 - measurement function
algorithm or calculation performed to combine two or more base measures (2.10).
[SOURCE: ISO/IEC 15939:2007, 2.20]

2.50 - measurement method
logical sequence of operations, described generically, used in quantifying an attribute (2.4) with respect to a specified scale (2.80).

[SOURCE: ISO/IEC 15939:2007, 2.22, modified — Note 2 to entry has been deleted.]
Note 1 to entry: The type of measurement method depends on the nature of the operations used to quantify an attribute (2.4). Two types can be distinguished as follows:
— subjective: quantification involving human judgment;
— objective: quantification based on numerical rules.

2.51 - measurement results
one or more indicators (2.30) and their associated interpretations that address an information need (2.31).

2.52 - monitoring
determining the status of a system, a process (2.61) or an activity.
Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

2.53 - nonconformity
non-fulfilment of a requirement (2.63).

2.54 - non-repudiation
ability to prove the occurrence of a claimed event (2.25) or action and its originating entities.

2.55 - object
item characterized through the measurement (2.48) of its attributes (2.4).

2.56 - objective
result to be achieved
Note 1 to entry: An objective can be strategic, tactical, or operational.
Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process (2.61).
Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security (2.33) objective or by the use of other words with similar meaning (e.g. aim, goal, or target).
Note 4 to entry: In the context of information security (2.33) management systems (2.46), information security (2.33) objectives are set by the organization, consistent with the information security (2.33)policy (2.60), to achieve specific results.

2.57 - organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (2.56).
Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

2.58 - outsource
make an arrangement where an external organization (2.57) performs part of an organization’s (2.57) function or process (2.61).
Note 1 to entry: An external organization is outside the scope of the management system (2.46), although the outsourced function or process (2.61) is within the scope.

2.59 - performance
measurable result
Note 1 to entry: Performance can relate either to quantitative or qualitative findings.
Note 2 to entry: Performance can relate to the management of activities, processes (2.61), products (including services), systems or organizations (2.57).

2.60 - policy
intentions and direction of an organization (2.57) as formally expressed by its top management (2.84).

2.61 - process
set of interrelated or interacting activities which transforms inputs into outputs.

2.62 - reliability
property of consistent intended behaviour and results.

2.63 - requirement
need or expectation that is stated, generally implied or obligatory.
Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization (2.57) and interested parties that the need or expectation under consideration is implied.
Note 2 to entry: A specified requirement is one that is stated, for example in documented information (2.23).

2.64 - residual risk
risk (2.68) remaining after risk treatment (2.79).
Note 1 to entry: Residual risk can contain unidentified risk (2.68).
Note 2 to entry: Residual risk can also be known as "retained risk".

2.65 - review
activity undertaken to determine the suitability, adequacy and effectiveness (2.24) of the subject matter to achieve established objectives (2.54).
[SOURCE: ISO Guide 73:2009, 3.8.2.2, modified — Note 1 to entry has been deleted.]

2.66 - review object
specific item being reviewed.

2.67 - review objective
statement describing what is to be achieved as a result of a review (2.65).

2.68 - risk
effect of uncertainty on objectives
[SOURCE: ISO Guide 73:2009, 1.1, modified]
Note 1 to entry: An effect is a deviation from the expected — positive or negative.
Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event (2.25), its consequence (2.14), or likelihood (2.45).
Note 3 to entry: Risk is often characterized by reference to potential events (2.25) and consequences (2.14), or a combination of these.
Note 4 to entry: Risk is often expressed in terms of a combination of the consequences (2.14) of an event (2.25) (including changes in circumstances) and the associated likelihood (2.45) of occurrence.
Note 5 to entry: In the context of information security (2.33)management systems (2.46), information security (2.33) risks can be expressed as effect of uncertainty on information security (2.33)objectives (2.56).

Note 6 to entry: Information security (2.33) risk is associated with the potential that threats (2.83) will exploit vulnerabilities (2.89) of an information asset or group of information assets and thereby cause harm to an organization (2.57).

2.69 - risk acceptance

informed decision to take a particular risk (2.68).
[SOURCE: ISO Guide 73:2009, 3.7.1.6]
Note 1 to entry: Risk acceptance can occur without risk treatment (2.79) or during the process (2.61) of risk treatment (2.79).
Note 2 to entry: Accepted risks (2.68) are subject to monitoring (2.52) and review (2.65).

2.70 - risk analysis

process (2.61) to comprehend the nature of risk (2.68) and to determine the level of risk (2.44).
[SOURCE: ISO Guide 73:2009, 3.6.1]
Note 1 to entry: Risk analysis provides the basis for risk evaluation (2.74) and decisions about risk treatment (2.79).
Note 2 to entry: Risk analysis includes risk estimation.

2.71 - risk assessment

overall process (2.61) of risk identification (2.75), risk analysis (2.70) and risk evaluation (2.74).
[SOURCE: ISO Guide 73:2009, 3.4.1]

2.72 - risk communication and consultation

continual and iterative processes (2.61) that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (2.82) regarding the management of risk (2.68).
Note 1 to entry: The information can relate to the existence, nature, form, likelihood (2.45), significance, evaluation, acceptability and treatment of risk (2.68).
Note 2 to entry: Consultation is a two-way process (2.51) of informed communication between an organization (2.57) and its stakeholders (2.82) on an issue prior to making a decision or determining a direction on that issue. Consultation is
— a process (2.61) which impacts on a decision through influence rather than power and
— an input to decision making, not joint decision making.

2.73 - risk criteria

terms of reference against which the significance of risk (2.68) is evaluated
[SOURCE: ISO Guide 73:2009, 3.3.1.3]
Note 1 to entry: Risk criteria are based on organizational objectives, and external (2.27) and internal context (2.42).
Note 2 to entry: Risk criteria can be derived from standards, laws, policies (2.60) and other requirements (2.63).

2.74 - risk evaluation

process (2.61) of comparing the results of risk analysis (2.70) with risk criteria (2.73) to determine whether the risk (2.68) and/or its magnitude is acceptable or tolerable
[SOURCE: ISO Guide 73:2009, 3.7.1]
Note 1 to entry: Risk evaluation assists in the decision about risk treatment (2.79).

2.75 - risk identification

process (2.61) of finding, recognizing and describing risks (2.68).
[SOURCE: ISO Guide 73:2009, 3.5.1]
Note 1 to entry: Risk identification involves the identification of risk sources, events (2.25), their causes and their potential consequences (2.14).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' (2.82) needs.

2.76 - risk management

coordinated activities to direct and control an organization (2.57) with regard to risk (2.68).
[SOURCE: ISO Guide 73:2009, 2.1]

2.77 - risk management process

systematic application of management policies (2.60), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk (2.68).
[SOURCE: ISO Guide 73:2009, 3.1, modified — Note 1 to entry has been added.]
Note 1 to entry: ISO/IEC 27005 uses the term "process" (2.61) to describe risk management overall. The elements within the risk management (2.76)process (2.61) are termed "activities".

2.78 - risk owner

person or entity with the accountability and authority to manage a risk (2.68).
[SOURCE: ISO Guide 73:2009, 3.5.1.5]

2.79 - risk treatment

process (2.61) to modify risk (2.68).
[SOURCE: ISO Guide 73:2009, 3.8.1, modified — "decision" has been replaced by "choice" in Note 1 to entry.]
Note 1 to entry: Risk treatment can involve the following:
— avoiding the risk (2.68) by deciding not to start or continue with the activity that gives rise to the risk (2.68);
— taking or increasing risk (2.68) in order to pursue an opportunity;
— removing the risk (2.68) source;
— changing the likelihood (2.45);
— changing the consequences (2.14);
— sharing the risk (2.68) with another party or parties (including contracts and risk financing);
— retaining the risk (2.68) by informed choice.
Note 2 to entry: Risk treatments that deal with negative consequences (2.14) are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".
Note 3 to entry: Risk treatment can create new risks (2.68) or modify existing risks (2.68).

2.80 - scale

ordered set of values, continuous or discrete, or a set of categories to which the attribute (2.4) is mapped.
[SOURCE: ISO/IEC 15939:2007, 2.35, modified]
Note 1 to entry: The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined as follows:
— nominal: the measurement (2.48) values are categorical;
— ordinal: the measurement (2.48) values are rankings;
— interval: the measurement (2.48) values have equal distances corresponding to equal quantities of the attribute (2.4);
— ratio: the measurement (2.48) values have equal distances corresponding to equal quantities of the attribute (2.4), where the value of zero corresponds to none of the attribute.
These are just examples of the types of scale.

2.81 - security implementation standard

document specifying authorized ways for realizing security.

2.82 - stakeholder
person or organization (2.57) that can affect, be affected by, or perceive themselves to be affected by a decision or activity
[SOURCE: ISO Guide 73:2009, 3.2.1.1, modified — Note 1 to entry has been deleted.]

2.83 - threat
potential cause of an unwanted incident, which may result in harm to a system or organization (2.57).

2.84 - top management
person or group of people who directs and controls an organization (2.57) at the highest level.
Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization (2.57).
Note 2 to entry: If the scope of the management system (2.46) covers only part of an organization (2.57), then top management refers to those who direct and control that part of the organization (2.57).

2.85 - trusted information communication entity
autonomous organization (2.57) supporting information exchange within an information sharing community (2.38).

2.86 - unit of measurement
particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity.
[SOURCE: ISO/IEC 15939:2007, 2.40, modified]

2.87 - validation
confirmation, through the provision of objective evidence, that the requirements (2.63) for a specific intended use or application have been fulfilled.
[SOURCE: ISO 9000:2015, 3.8.12, modified]

2.88 - verification
confirmation, through the provision of objective evidence, that specified requirements (2.63) have been fulfilled.
[SOURCE: ISO 9000:2015, 3.8.4]
Note 1 to entry: This could also be called compliance testing.

2.89 - vulnerability
weakness of an asset or control (2.16) that can be exploited by one or more threats (2.83).

Os Termos e Definições da antiga Norma **ABNT NBR ISO/IEC 27001:2006** (em português) só podem ser extraídos da própria norma. Há muito menos termos, pois o glossário aqui se preocupa só com as definições necessárias à 27001, especificamente.

Há muito mais termos neste glossário do que naqueles que havia anteriormente em cada norma, pois o glossário aqui se preocupa com a definição de termos para toda a família.

Segue abaixo apenas a Seção 3…

3 - Termos e definições
Para os efeitos desta Norma, aplicam-se os seguintes termos e definições.

3.1 - ativo
qualquer coisa que tenha valor para a organização.
[ISO/IEC 13335-1:2004]

3.2 - disponibilidade
propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
[ISO/IEC 13335-1:2004]

3.3 - confidencialidade
propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
[ISO/IEC 13335-1:2004]

3.4 - segurança da informação
preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.
[ABNT NBR ISO/IEC 17799:2005]

3.5 - evento de segurança da informação
uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
[ISO/IEC TR 18044:2004]

3.6 - incidente de segurança da informação
um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

3.7 - sistema de gestão da segurança da informação
SGSI
a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.
NOTA O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

3.8 - integridade
propriedade de salvaguarda da exatidão e completeza de ativos.
[ISO/IEC 13335-1:2004]

3.9 - risco residual
risco remanescente após o tratamento de riscos.
[ABNT ISO/IEC Guia 73:2005]

3.10 - aceitação do risco
decisão de aceitar um risco.
[ABNT ISO/IEC Guia 73:2005]

3.11 - análise de riscos
uso sistemático de informações para identificar fontes e estimar o risco.
[ABNT ISO/IEC Guia 73:2005]

3.12 - análise/avaliação de riscos
processo completo de análise e avaliação de riscos.
[ABNT ISO/IEC Guia 73:2005]

3.13 - avaliação de riscos
processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
[ABNT ISO/IEC Guia 73:2005]

3.14 - gestão de riscos
atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.
NOTA A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.
[ABNT ISO/IEC Guia 73:2005]

3.15 - tratamento do risco
processo de seleção e implementação de medidas para modificar um risco.
[ABNT ISO/IEC Guia 73:2005]
NOTA Nesta Norma o termo “controle” é usado como um sinônimo para “medida”.

3.16 - declaração de aplicabilidade
declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização.
NOTA Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.