SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

AULA 1

Prof. Douglas Eduardo Basso

TEMA 1 – HISTÓRIA E CONCEITOS

A revolução tecnológica iniciada no século XX criou novos paradigmas relacionados à informação, uma nova etapa na história da humanidade, que, segundo Galvão (2015), a era da informação se desenvolve no momento em que é estabelecida uma plataforma por meio da qual se torna possível a todos os indivíduos com acesso a ela, independentemente de onde estejam, trocar experiências, compartilhar formas diferentes de fazer as coisas, comprar, vender e criar coletivamente.

Na era moderna, os ciclos de produção e consumo presentes em nossa economia estão cada vez mais velozes, a inovação tem sido muito presente e está vinculada ao sucesso, a qualidade dos produtos criados, o consumismo acelerado, o ritmo cada vez mais rápido, todo esse cenário torna as informações um ativo muito valioso. A disputa, e toda essa competição nesse novo contexto, estão muito dependentes do compartilhamento de informações entre os mais diversos atores, como fornecedores, produtores, parceiros, clientes, colaboradores, entre outros.

Dentro desse aspecto, com todo esse mar de informações sendo criado diariamente por essas entidades, hoje não é mais possível estar participando dessa disputa por inovações e armazenar as informações geradas em cofres, armários, gavetas e trancá-las com chaves e segredos, desenvolver a acessibilidade e a disponibilidade de tudo isso é a maneira encontrada para se manter no páreo, quando falamos de instituições públicas, o governo torna o processo mais complexo. Existe uma série de princípios a serem respeitados, nossas legislações, proteção de dados, princípios de segurança e defesa nacional, as informações são toda a base para a operação e funcionamento das organizações, empresas, órgãos públicos, governo e demais entidades.

1.1 Informação

Com o surgimento da internet, a comunicação a nível mundial ficou muito mais rápida, o intercâmbio de informações, a colaboração, a globalização, enfim, todo esse cenário criou facilidades relacionadas com a troca de dados, porém esse intercâmbio de informações criou problemas de acessibilidade, disponibilidade, integridade, entre outros.

Em nossa vida diária estamos convivendo com diversas formas de informações, ela pode estar presente como uma figura, um texto, um vídeo, voz etc. Quando solicitamos informações de alguém: um endereço, um telefone, o número de um documento, ou mesmo quando perguntamos o preço de um produto no comércio, ao ler um livro, assistir a um filme, em todos esses momentos estamos em um processo de troca de informações.

Sendo assim, informação, no âmbito geral, significa receber ou fornecer dados, independente do resultado ou raciocínio sobre esses dados, de maneira lógica ou não. Dentro do contexto da Tecnologia da Informação (TI), esse tipo de conceito é visto de outra maneira.

No âmbito computacional, informações e dados são coisas distintas. Dados são elementos ainda não analisados e não processados. Já as informações são o resultado do processamento desses dados pelo computador (Galvão, 2015).

Segundo Baars (2018), é essencial compreender a diferença entre dado e informação. O dado pode ser processado pela TI, mas ele se torna informação após adquirir certo significado.

A informação é um grande ativo que, como qualquer outro componente valioso e importante de uma empresa, é essencial para os negócios de uma organização, que antes disso requer e necessita de proteção adequada. A informação pode existir de diversas formas, seja qual for a sua apresentação ou meio ao qual está vinculada, é altamente recomendado que esteja sempre segura e protegida.

1.2 Ciclo de vida da informação

Todas as informações de uma empresa têm um ciclo de vida. Dessa forma, em alguns momentos, nos quais a informação é colocada em risco, temos que observar e ter atenção ao tempo de vida que essa informação necessita ter. Em relação às fases do ciclo de vida das informações, podemos elencar as seguintes:

- manuseio – quando a informação é criada, coletada, gerada ou alterada;
- armazenamento – quando a informação é consolidada, gravada ou retida;
- transporte – quando a informação é transferida, comunicada, transportada; e

- descarte – quando a informação perde seu valor e é inutilizada ou descartada.

Em cada uma das etapas do ciclo de vida da informação a atenção necessária para garantir confidencialidade, integridade, autenticidade, disponibilidade e até mesmo legalidade à informação deve ser dada de maneira eficaz (Galvão, 2015).

Existe a necessidade de proteger as informações em todas as fases de seu ciclo de vida, por mais que em alguns momentos as informações tenham maior ou menor importância.

1.3 Sistemas de Informação

Os dados possuem muito valor, mesmo que ainda não usados ou formatado e lapidado como "informação", a necessidade de proteger os dados depende muito do grau de importância dado por seus. A informação carrega consigo o conhecimento, muitos conseguem extrair valiosos conhecimentos de um grupo de informações, depende muito da atribuição que colocamos nelas.

Para Baars (2018), os fatores de produção normais de uma empresa ou organização são o capital, o trabalho e as matérias-primas. Em Tecnologia da Informação, é comum também considerar a informação como fator de produção. Empresas não podem existir sem informação. Um armazém que perde suas informações de estoque e clientes normalmente não seria capaz de operar sem elas. Para algumas empresas, como um escritório de contabilidade, a informação é, na verdade, seu único produto.

Dentro desse contexto estão os sistemas de informação, são eles os responsáveis pela transferência e o processamento de dados e informações, são sistemas formados por meio da interação entre usuários, processos, tecnologia e dados. Quando se referimos a sistemas de informação não se trata apenas de tecnologia e comunicação que as entidades utilizam, mas também de toda a maneira como esses atores se relacionam apoiando sempre o processamento de um negócio.

Os sistemas de informação podem ser bases de dados, arquivos gravados em um disco, documentos físicos armazenados em armários, equipamentos de comunicação, impressoras, computadores portáteis, servidores, redes, equipamentos de comunicação, telefones, entre outros, esses

sistemas são a combinação de todos esses componentes, envolvendo regras, processos, usuários, equipe técnica, devem atender demandas de informações para determinado processo operacional de uma organização.

1.4 Gestão da Informação

A tarefa de organizar todas informações de uma empresa, criar, coletar, controlar, planejar, utilizar, difundir e descartar suas informações de maneira eficaz e eficiente é da gestão da informação. A missão da gestão é promover e garantir o valor das informações, explorar de uma maneira inteligente em todos os seus aspectos.

No campo interdisciplinar temos alguns recursos combinados para essa árdua tarefa: a tecnologia da informação, o gerenciamento de registros, a ciência da computação, a biblioteconomia, a administração geral e o arquivamento, a informação é encarada como um recurso, independente da maneira que ela esteja disponível.

As fontes de dados podem ser as mais diversificadas possíveis: informações armazenadas em computadores, mídias audiovisuais, livros, revistas, periódicos, o conhecimento dos colaboradores de uma empresa, microformas, entre outras, todas essas fontes de "recursos" devem estar alinhadas no mesmo escopo, alguns tópicos elencados a seguir mostram os pontos de atenção de profissionais de tecnologia da informação em relação a todo esse cenário:

- classificação e codificação;
- índices e palavras-chave;
- criação de dicionários e vocabulários controlados;
- catálogos de dados (nomes, endereços, locais, eventos);
- estruturas de dados organizadas (banco de dados);
- armazenamento de arquivos, fotos, imagens, arquivos digitalizados;
- depósito e guarda-livros e registros físicos;
- auditoria de informações; e
- documentação de objetos, procedimentos e demais recursos.

1.5 Computação distribuída

Com o advento da computação distribuída, criou-se um grande desafio em relação à eficácia do controle das informações, e em uma grande rede de computadores isso se torna muito mais complexo.

Em geral, a computação distribuída é qualquer computação que envolve vários computadores distantes um do outro, onde cada um tem um papel no processo computacional ou no processamento da informação (Baars, 2018).

1.6 Privacidade

Com a modernização dos meios de comunicação e com a evolução dos equipamentos de informática surge a necessidade de armazenar informações de forma cada vez mais inteligente, a utilização de recursos avançados de interação com várias interfaces de acesso, a relação homem-máquina tem mudado muito com a inclusão digital das mais diversas classes da sociedade.

Segundo Alves (2021), toda essa interação, acessibilidade, mobilidade e facilidade na transposição dos conteúdos digitais de diferentes equipamentos fazem com que a segurança da informação seja um desafio a ser mantido perante o usuário proprietário desses dispositivos eletrônicos que estão ligados a algum tipo de rede ou mesmo a internet (como os celulares, computadores, Smarts TV, entre outros), integrando-se ainda com outros aplicativos, outros usuários, bem como os fabricantes desses diversos dispositivos eletrônicos.

Com todo esse novo cenário criado em torno da privacidade dos dados de quem faz a utilização ou esteja envolvido, faz raciocinar em relação aos tipos de comportamento, atitudes, ações e reações perante a tantos dados, além das informações que são disponibilizadas diariamente, pois somos ao mesmo tempo simples utilizadores de sistemas de informação e detentores de dados, informações e conhecimento.

TEMA 2 – INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Em relação aos conceitos relacionados à Ciência da Computação, a diferença entre segurança e proteção deve ser bem esclarecida. Assim, proteção é considerada como um mecanismo e a segurança como uma política, o mecanismo apresenta o “como” fazer e a política de uma maneira mais estratégica, “o que fazer”.

Para Alves (2021), não basta ter todo um arsenal de mecanismos altamente tecnológicos de última geração se não se sabe ao certo suas proporções de ação e reação, bem como sua eficiência naquilo que realmente é necessário para se conseguir, por exemplo, a privacidade. A privacidade dos dados é focada no uso e controle de dados pessoais – coisas como implementar políticas para garantir que as informações pessoais dos consumidores sejam coletadas, compartilhadas e usadas de maneiras apropriadas. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade se tornou uma das grandes preocupações.

A segurança da informação está relacionada à proteção de um conjunto de dados, no sentido de preservar o valor que eles possuem para um indivíduo ou uma organização.

Segundo Fraga (2019), a segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa; isto é, aplica-se tanto às informações corporativas como às pessoas. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem a utiliza, pelo ambiente ou infraestrutura que a cerca, ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

2.1 Atributos da Segurança e Proteção de Dados

Segundo alguns padrões internacionais, existem alguns pilares que acabam criando toda a base em relação à segurança e à proteção de dados. Dessa maneira, para que seja possível chegar a índices adequados de privacidade, podemos destacar os seguintes.

- Confidencialidade – é a propriedade que atua com limites de acesso à informação somente às entidades legítimas, ou seja, somente a pessoas autorizadas pelo proprietário da informação. A confidencialidade deve garantir que o acesso seja restrito apenas ao público-alvo, quanto mais sensível e importante a informação for, mais rigorosa deve ser as medidas de segurança. As leis de privacidade estão intimamente ligadas à confidencialidade para se colocar os requisitos legais.

- Integridade – é o atributo que garante que toda informação manipulada tem todas as características originais intactas e estabelecidas pelo proprietário da informação, incluindo os controles de mudança e a garantia de todo o seu ciclo de vida (criação, manutenção, destruição). Trata de proteger os dados de alterações por pessoas não autorizadas, ocorre também de forma acidental ou por fatos não humanos, como problemas de energia elétrica, falhas e descargas eletromagnéticas ou falha no servidor. Nessa propriedade, o vínculo é mais forte com a proteção de dados.

- Disponibilidade – atributo relacionado com a disponibilidade da informação para a utilização legítima a quem realmente está autorizado a acessar pelo proprietário da informação, dentro dessa propriedade é desejável que o nível de segurança seja estabelecido em cima dos princípios organizacionais. Alguns aspectos devem ser levados em conta na criação desse critério, como: custos de implantação, riscos associados, benefícios, entre outros, e é imprescindível manter hardware e softwares funcionando de maneira correta e manter um fornecimento ininterrupto de conectividade de rede.

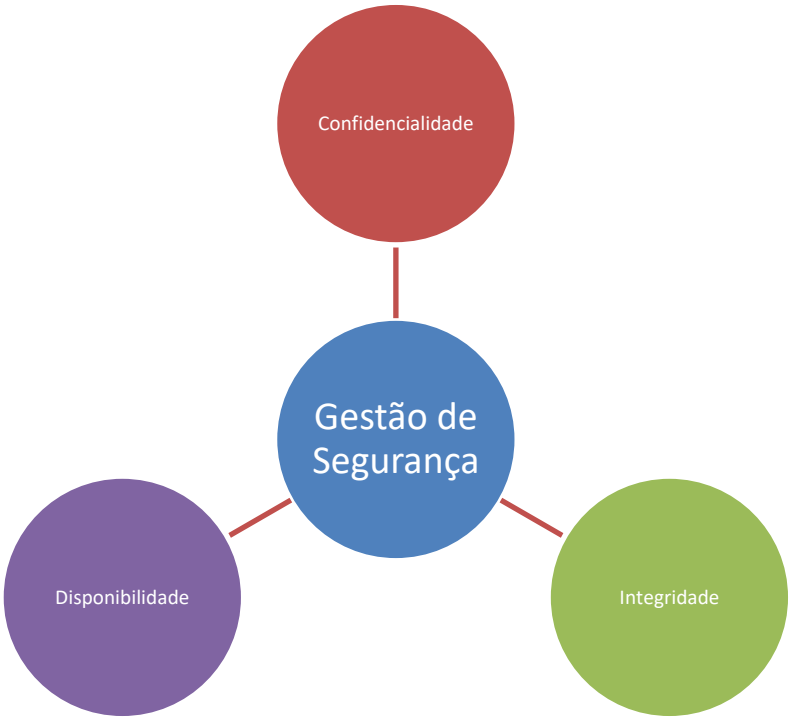
- Autenticidade – essa propriedade deve garantir que as informações sejam verdadeiras, de fonte confiável, porém é necessário manter registros de autoria da informação, visando sempre validar a sua veracidade.

- Irretrabilidade (não repúdio) – propriedade que impede que algum usuário negue a autoria de determinada informação e, dessa forma, garantindo sua autenticidade. Autor e receptor não podem contestar qualquer tipo de transação realizada por eles.

- Legalidade – essa propriedade tem o intuito de estabelecer a legalidade jurídica da informação, com alinhamento e aderência à legislação vigente, sendo caracterizado o valor legal dentro de um tipo de comunicação, em que ativos se coloquem em acordo com diretrizes, regras e cláusulas contratuais definidas pela lei.

A confidencialidade, integridade e disponibilidade são consideradas a tríade da gestão de segurança da informação, conforme figura 1 a seguir.

Figura 1 – Tríade da Segurança da Informação



Fonte: Baars, 2018.

2.2 Classificação da informação

A classificação de informações é essencial para as organizações, é uma atividade relacionada à diferenciação das informações, bem como estipula critérios e níveis apropriados de proteção, critérios esses que devem englobar as propriedades citadas anteriormente: confidencialidade, integridade, disponibilidade etc. Outro aspecto a ser observado é a sua relevância para a organização.

Segundo Galvão (2015), o grau de sigilo é uma classificação concedida a cada tipo de informação e baseada em critérios como nível de importância e de sigilo, pessoas com permissão de acesso, entre outros. Não existe um padrão de classificação que possa ser adotado em todas as organizações, pois cada organização tem suas particularidades, no entanto, é comum a maioria das empresas privadas utilizar como classificação os seguintes graus: confidencial, privada, sigilosa e pública.

Na administração pública existe uma legislação específica, de acordo com o Decreto n. 7.724/2012, no art. 26, informando sobre a classificação das

informações em órgãos públicos como ultrassecreto, secreto ou reservado. A seguir a tabela 1 serve como um comparativo.

Tabela 1 – Grau de sigilo

Órgãos e entidades públicas	Empresas Privadas
Ultrassecreto	Confidencial
Secreto	Privada
Reservado	Sigilosa
Público	Pública

Fonte: Galvão, 2015.

2.3 Ameaças à segurança

Para Fraga (2019), as ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três características principais (tríade da gestão de segurança da informação).

- Perda da confidencialidade – geralmente ocorre quando um evento relacionado à quebra de sigilo de determinada informação acontece (quebra de senhas, modificação de acessos), permitindo que as informações restritas sejam abertas e expostas, tendo em vista que apenas um grupo específico de usuários possam acessar.
- Perda de integridade – a ameaça de integridade acontece quando alguma informação fica aberta e exposta ao manuseio de um usuário não autorizado, que faz alterações que não são aprovadas ou que não estão no controle do dono (privado ou corporativo) das informações.
- Perda de disponibilidade – quando uma informação deixa de ser acessível para quem está solicitando, ocorre com a falha de comunicação, com um sistema importante, algo que impeça que os utilizadores acessem a informação, falhas de servidores, problemas elétricos, com a rede de dados, ou até mesmo a internet, alguns problemas como esses podem ser internos empresa ou externos, seja por ação não autorizada ou por pessoas mal-intencionadas.

2.4 Aspectos legais

A área de segurança da informação é alinhada com diversos padrões internacionais de segurança, seguidos por muitas corporações e tem suas regras e políticas aplicadas diariamente em suas atividades.

Em termos jurídicos, a segurança da informação no Brasil é o resultado da relação entre a ciência do direito e a ciência da computação, sempre empregando novas tecnologias. Trata-se do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital. Como consequência dessa interação e da comunicação ocorrida em meio virtual, surge a necessidade de se garantir a validade jurídica das informações prestadas, bem como transações, por meio do uso de certificados digitais.

TEMA 3 – ISO 15408

A norma ISO/IEC 15408 é uma modelagem bem flexível com um grupo de métodos para a análise e avaliação de aspectos relacionados com a segurança de produtos e sistemas de Tecnologia da Informação, tais como: hardware, software e firmware. Em relação aos conceitos de segurança observados pela norma ISO 15408, apresenta-se a tríade da segurança da informação: confidencialidade, integridade e disponibilidade da informação.

Dentro do atributo confiabilidade são analisadas as permissões de visualização e captura de algum tipo de conteúdo a usuários que não estejam na lista de autorizados, já no quesito integridade são avaliadas as permissões de alteração de um conteúdo de maneira indevida, e, por fim, a disponibilidade da informação testa se o sistema é resiliente e tolerante a falhas mantendo a disponibilidade de acesso pelo maior tempo possível.

A norma ISO 15408 é um modelo que orienta diferentes tipos de atividades, dentre as quais os principais beneficiados são os utilizadores, os consumidores, desenvolvedores, parceiros e avaliadores. O consumidor tira proveito da utilização da norma, para avaliar com mais propriedade algum tipo de produto, seja ele software ou hardware de TI, e a partir dessa avaliação e resultados, faz a tomada de decisão se o produto de TI é de boa qualidade e se atende a todas as necessidades e premissas de segurança.

Os desenvolvedores de produtos de TI podem fazer uso da norma como parâmetro para a boa elaboração, execução e desenvolvimento de produtos e sistemas, tornando-os mais seguros, além de elencar e identificar uma série de requisitos relacionados à segurança. Os avaliadores e analisadores podem tirar

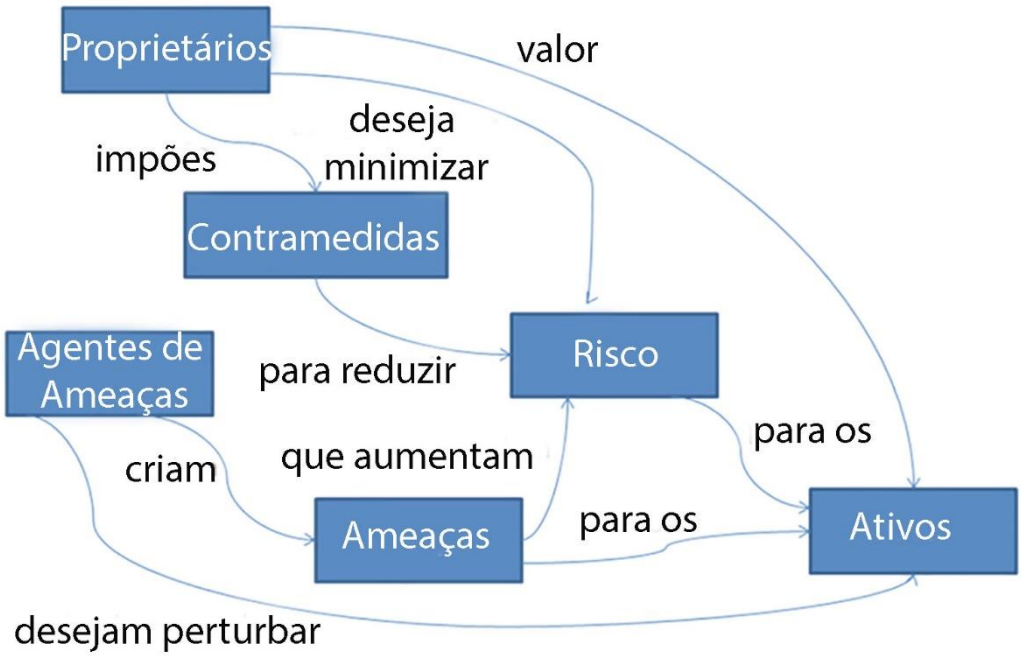
proveito da norma ao fazerem julgamentos sobre toda a conformidade de produtos e sistemas, avaliando se as necessidades de segurança estão sendo atendidas, embora a norma não oriente os procedimentos a serem adotados.

A área que abrange a norma ISO 15408 mostra o quão útil pode ser esse material de referência para os envolvidos, áreas interessadas ou até mesmo áreas responsáveis pela segurança e auditoria de produtos de TI, que não se limita apenas aos usuários, consumidores, desenvolvedores, analistas e avaliadores, como também auxilia a auditoria, seja ela feita de maneira interna ou externa, responsáveis pelo alinhamento e adequação da segurança de TI, apoiando a arquitetura e engenharia de softwares, designers de produtos, entre outros atores relacionados.

3.1 Modelo geral

O modelo geral da norma trata dos pacotes e perfis de proteção, da análise e avaliação de resultados, da especificação e dos requisitos dos pontos de segurança, perfis de proteção, requerimentos e diretrizes de segurança e da conformidade. O modelo geral apresenta uma série de conceitos de segurança e relacionamento, conforme figura 2.

Figura 2 – Conceitos de segurança e relacionamento



Fonte: ISO/IEC 15408.

3.2 Componentes funcionais de segurança

Os componentes de segurança são toda a base dos requisitos funcionais de segurança apresentados no perfil de proteção do ativo de segurança. Os requisitos funcionais de segurança são apresentados em classes, grupos e componentes. As classes expressas são as seguintes:

- auditoria de segurança;
- proteção das funcionalidades de segurança;
- utilização dos recursos;
- acesso aos alvos de avaliação;
- canais e caminhos confiáveis;
- proteção de dados de usuário;
- identificação e autenticação;
- gerenciamento de segurança;
- privacidade;
- comunicação; e
- suporte à criptografia.

3.3 Componentes de garantia de segurança

São os componentes de garantia de segurança que formam um caminho padrão a ser seguido para mostrar os requisitos de segurança para os alvos de avaliação. Essa etapa da norma foi criada e desenvolvida para os usuários, clientes, desenvolvedores, analistas e avaliadores de segurança de produtos de TI.

3.4 Desenvolvimento seguro

Ao avaliar essa norma, é possível apontar três pontos positivos na norma ISO 15408, que são concatenados entre si e devem ser discutidos em relação à segurança no desenvolvimento de software, na qual é possível mostrar procedimentos que se mostram eficientes em sua aplicação na manutenção de software. Eles estão elencados a seguir.

- Segurança de ambiente – ambientes sem nenhum tipo de segurança apresentam sérios risco relacionados à perda de códigos-fontes, modificação de códigos-fontes, problemas de versionamento, ou falha de qualquer arquivo importante para o correto funcionamento de um produto de TI, dentre outros problemas que venham a impactar na confidencialidade do produto em si, somente com um ambiente de desenvolvimento seguro é possível desenvolver um software de maneira confiável. A norma apresenta a necessidade de controles de espaços físicos, atividades relacionadas à gerência de configuração de todos os códigos-fontes, com níveis e controle de acesso, podendo ser físicos e lógicos, assim como ter procedimentos bem controlados e estabelecidos, evidenciando todos esses controles.
- Segurança da aplicação – compreende a parte de qualidade do código-fonte do software, o emprego de boas práticas de programação cria um código-fonte confiável e garante a segurança de uma aplicação. O ambiente seguro é a base para o desenvolvimento seguro, boas especificações de segurança, além da realização de testes de aplicação.
- Garantia de aplicação segura – além de criar uma aplicação segura, ainda é necessário apresentar ações e provas que permitam aos clientes e usuários saber se a aplicação é confiável e segura. A garantia pode ser feita por meio de testes acompanhados e validados pelo usuário, que devem ser checados em ambientes diferentes. Nessa etapa, é necessária uma boa especificação de segurança, abordando de maneira objetiva e clara o desenvolvimento alinhado com essa especificação e, posterirormente, a realização de testes para garantir os requisitos de especificação.

A norma ISO 15408 está voltada para a avaliação de segurança. A identificação do ambiente e de seguros procedimentos na manutenção de software é essencial para a confiabilidade do conteúdo a ser alterado assim como seus meios de comunicação, observando a ocorrência de problemas e falhas em outras áreas, assim, a integridade das informações tende a ser muito maior.

TEMA 4 – FAMÍLIA ISO 27000

A família ISO/IEC 27000 apresenta uma séria de normas relacionadas à segurança de ativos de informações das empresas, assim, com a utilização dessas normas, as organizações tornam todo seu ambiente computacional mais seguro, como a proteção a dados financeiros, propriedades intelectuais, informações empresariais, segredos de negócios, entre outros.

Essas normas são criadas, produzidas e desenvolvidas pela *International Organization for Standardization* (ISO) e *International Electrotechinical Commission* (IEC). Existe uma grande variedade de normas focadas na gestão de segurança da informação.

- ISO/IEC 27000: é uma norma que apresenta uma visão geral, termos e condições para a gestão de segurança da informação. Possui um glossário que serve como base para as demais normas da família.
- ISO/IEC 27001: a segunda norma da família busca alinhar todos os requisitos que uma organização possa utilizar para um Sistema de Gestão da Segurança da Informação (SGSI). Leva em conta toda a segurança física do ambiente, fatores técnicos, procedimentais e de comportamento das pessoas. Também orienta processos de levantamento de riscos e estipula valores de ativos.
- ISO 27001: é a norma principal de segurança de informação, as organizações devem alinhar como base para obtenção de certificações empresariais em gestão da segurança da informação. É reconhecida internacionalmente e é passível de auditoria, veremos essa norma com mais detalhes ao longo desta aula.
- ISO/IEC 27002: apresenta uma série de códigos de práticas com um grupo completo de controles que servem como base para a aplicação do Sistema de Gestão da Segurança da Informação. Mostra um grande número de controles de segurança e foi criada e desenvolvida por especialistas da indústria e do comércio em prol de organizações de qualquer tamanho. Também será apresentada com mais detalhes no decorrer deste tema.
- ISO/IEC 27003: traz um conjunto de diretrizes para a elaboração do SGSI. Ela é baseada no ciclo PDCA, esse ciclo é uma ferramenta de gestão que

tem como objetivo ajudar na melhoria contínua dos processos por meio de quatro ações: planejar (*plan*), fazer (*do*), checar (*check*) e agir (*act*).

- ISO/IEC 27004: apresenta algumas métricas para a gestão da segurança da informação. É essencial em situações de definição de métrica de níveis de serviço para a segurança da informação, ela ajuda a medir os processos empresariais. Também tem alinhamento com o ciclo PDCA.
- ISO/IEC 27005: trata de forma detalhada a gestão de riscos.
- ISO/IEC 27006: apresenta uma série de requisitos para as organizações que desejam atuar com auditoria e certificações de sistemas de gestão.
- ISO/IEC 27007: apresenta um grupo de instruções para orientar auditorias sobre os requisitos do SGSI. Deve estar alinhada com a ISO 27006. Elenca diretrizes e tem um guia para a auditoria de sistemas de gestão da segurança da informação.
- ISO/IEC 27008: serve de complemento para a ISO 27007 ao concatenar a auditoria dos controles em segurança da informação, faz um link entre as normas 27001 e 27007. Seus temas principais são a auditoria dos requisitos a do SGSI.
- ISO/IEC 27009: responsável por apoiar e dar suporte às indústrias específicas que buscam trabalhar com as normas ISO 27000.
- ISO/IEC 27010: apresenta um guia que trata da comunicação em gestão da segurança da informação tanto no escopo da organização como no mercado de cibersegurança. O objetivo da norma é promover a comunicação em relação aos controles de segurança da informação, criar um ambiente de colaboração entre as empresas do segmento, com o intuito de aprimorar a gestão da segurança da informação, compartilhar informações, disseminar o conhecimento de cibersegurança, seja com empresas privadas, órgão públicos, governo e indústria.
- ISO/IEC 27011: apresenta um guia de gestão da segurança para as empresas da área de telecomunicações.
- ISO 27012: criada para a gestão da segurança da informação para organizações da administração pública. Entretanto, teve sua validade cancelada e não é mais encarada uma norma oficial.

- ISO/IEC 27013: apresenta um alinhamento entre a norma ISO 27001 em uma organização concatenada com a ISO 20000.
- ISO/IEC 27014: apresenta técnicas para a boa governança da segurança da informação. Cria um guia de como avaliar, dirigir, controlar e comunicar todas as práticas internas da organização que têm vínculo com a área de segurança da informação, de maneira que estejam compreendidas e alinhadas com necessidades da área de negócio.
- ISO/IEC 27015: traz uma abordagem de gestão da segurança da informação para atividades e serviços financeiros. Fornece diretrizes e controles de segurança para o segmento financeiro.
- ISO/IEC 27016: traz uma abordagem de gestão da segurança da informação para atividades e serviços do setor de economia. Fornece diretrizes e controles de segurança para o segmento econômico.
- ISO/IEC 27017: essa norma apresenta alguns controles específicos para computação em nuvem (*cloud computing*).
- ISO/IEC 27018: apresenta assuntos relacionados de forma específica para os serviços em computação em nuvem. É uma norma que traz complementos à ISO 27017.
- ISO 27019: define controles de forma específica para a indústria de energia.
- ISO 27031: trata de conceitos e princípios relacionados ao papel da segurança da informação para a área de Tecnologia da Informação com o enfoque de garantia para a continuidade dos negócios. Apresenta algumas diretrizes de mensuração do nível de proteção da organização concatenadas com a gestão da continuidade na visão da tecnologia e comunicação.
- ISO 27032: apresenta todos os temas relacionados à cibersegurança e suas especialidades. Trata da definição de atributos como confidencialidade, integridade e disponibilidade da informação em cibersegurança.
- ISO 27033-1: essa norma apresenta uma breve introdução e conceitos gerais para segurança em redes.

- ISO 27033-2: criada com o intuito de planejar, desenhar, implementar e documentar toda a segurança em redes.
- ISO 27033-3: tem por finalidade definir os riscos específicos, apresenta técnicas de projetos e controles vinculados com a segurança em redes.
- ISO 27033-4: traz um esquema geral de requisitos para análise e identificação de ameaças para a segurança da informação relacionadas a gateways de segurança da informação e componentes que façam parte da arquitetura de segurança em redes.
- ISO 27033-5: apresenta conteúdo relacionado com a comunicação entre redes usando *Virtual Private Networks* (VPNs).
- ISO 27033-6: apresenta algumas definições relacionadas a riscos, técnicas de projeto e desenho, traz também alguns controles específicos relacionados com a segurança da informação em redes *wireless*.
- ISO 27034-1: apresenta algumas definições e conceitos em torno da segurança da informação em aplicações.
- ISO 27034-2: apresenta em seu conteúdo uma organização normativa de segurança sobre aplicações.
- ISO 27034-3: essa norma apresenta um guia relacionado ao processo de gestão da segurança em aplicações.
- ISO 27034-4: traz uma série de requisitos para a validação de segurança em aplicações.
- ISO 27034-5: especifica alguns protocolos e estrutura de dados de controle de segurança de aplicativos.
- ISO 27034-6: mais uma norma que traz um guia de segurança da informação para aplicações específicas.
- ISO 27035: essa norma apresenta um guia bem detalhado relacionado com a gestão de incidentes de segurança da informação, atendendo a processos de mapeamento de eventos, gestão de incidentes e vulnerabilidades de segurança da informação.
- ISO 27036: trata de assuntos de segurança da informação relacionados com fornecedores. Apresenta orientações sobre a avaliação e tratamento

de riscos de segurança da informação incluídos na aquisição de informações ou produtos relacionados à TI.

- ISO 27037: apresenta algumas orientações relacionadas à identificação, coleta, aquisição e preservação de evidências forenses digitais de caráter judicial. Ela está vinculada com a manutenção de integridade de evidências. Tem grande relevância para profissionais que perseguem uma carreira na área de perícia forense.
- ISO 27038: apresenta um guia para redação digital. Mostra alguns requisitos para redação e compartilhamento de informações digitais de maneira adequada, seja ela publicada de forma interna na organização ou interessados externos.
- ISO 27039: essa norma apresenta um guia para sistemas de detecção de intrusos, mostra como fazer seleção, contratação, desenho, operação e administração de sistemas IDS (*Intrusion Detection Systems*).
- ISO 27040: aborda sistemas da informação para infraestrutura de armazenamento e traz alguns aspectos relacionados à segurança da informação em dispositivos de armazenamento (*storages*).
- ISO 27041: tem a responsabilidade de regulamentar os métodos de investigação de evidências digitais. Ainda, ela atua na conformidade de métodos para investigação digital, é mais um guia disponível relacionado com a análise forense computacional.
- ISO 27042: é mais uma norma relacionada à computação forense, apresenta algumas diretrizes na análise e interpretação de evidências digitais.
- ISO 27043: traz alguns princípios e processos relacionados com a investigação de incidentes da segurança da informação. Mais um guia voltado exclusivamente para gestão de incidentes de segurança.
- ISO 27044: mostra uma série de diretrizes de maneira específica para o Gerenciamento de Eventos de Segurança da Informação (SIEM).
- ISO 27799: trata do gerenciamento de segurança da informação para o segmento de saúde.

4.1 ISO 27001

A ISO 27001, como mencionada anteriormente, é um guia que apresenta requisitos em relação à coleta, armazenamento, tratamento e compartilhamento de dados pessoais, com o intuito de garantir a segurança da informação nas organizações que trabalham com dados sensíveis. Garantindo sempre a tríade da segurança da informação (integridade, disponibilidade e confidencialidade).

4.1.1 Controles

Os controles de segurança são salvaguardas ou contramedidas técnicas ou administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidades devido a ameaças e agindo sobre a sua correspondente vulnerabilidade, o risco à segurança. Controles são referenciados o tempo todo na segurança, mas são raramente definidos (Baars, 2018).

4.1.2 Tratamento de riscos

Toda a organização deve definir algumas convenções e critérios para determinar os riscos que podem ser aceitos ou não, e ao ser avaliado o risco precisa ser classificado, qual é o custo para o seu tratamento – todas essas decisões precisam ser documentadas e todas essas tratativas em relação aos riscos também. Alguns controles são desejáveis dentro deste cenário:

- aplicação de controles adequados para redução de riscos;
- entendimento em relação aos riscos, política clara de aceitação de riscos;
- evitar as ocorrências de riscos, identificar e mitigar as causas;
- aplicar controles apropriados e fazer a transferências de riscos a outras partes como fornecedores, parceiros e seguradoras;
- desenvolver e atender requisitos identificados em avalições de risco;
- reduzir os riscos a níveis aceitáveis;
- atender aos requisitos e restrições relacionados com a legislação nacional e internacional; e
- criar um equilíbrio na relação de riscos e o tratamento para a redução, tendo em vista sempre as exigências e limitações da organização, o

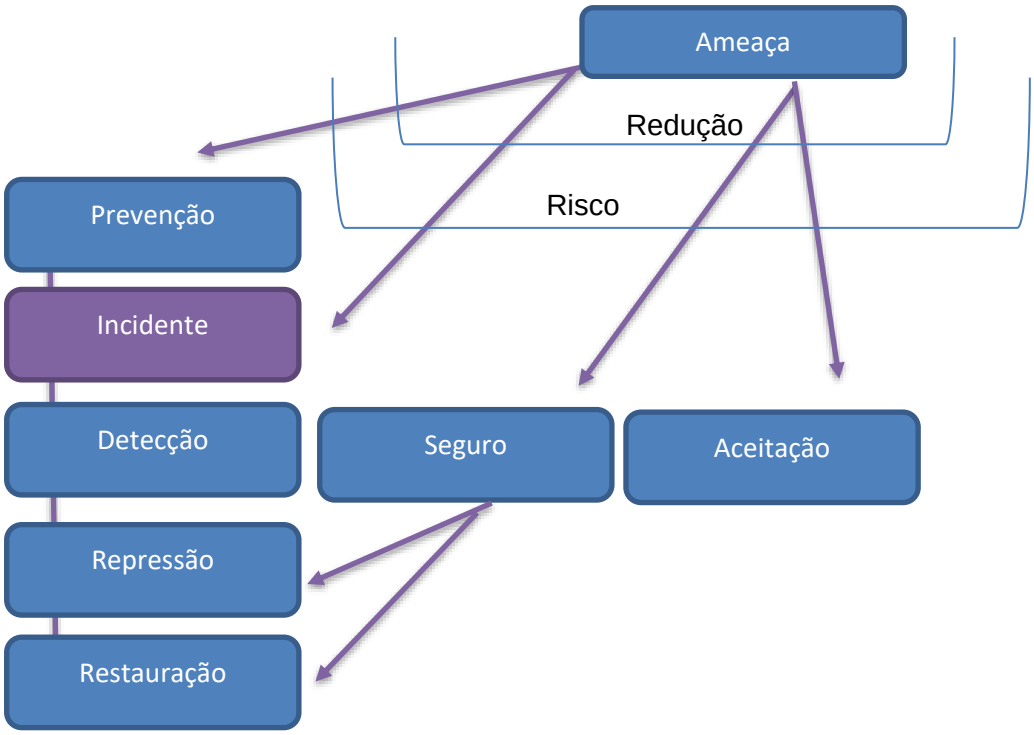
investimento e a operação de controles que podem causar falhas de segurança.

4.1.3 Contramedidas

Durante a análise de riscos são levantadas uma série de ameaças relacionadas com sua respectiva importância. Ao avaliarmos as ameaças, é necessária a criação de contramedidas que possam minimizar as ameaças, essas contramedidas visam mitigar as chances de alguns eventos ocorrerem e minimizar as consequências. Para Baars (2018), existem seis categorias diferentes:

- contramedidas preventivas visam evitar acidentes;
- contramedidas de redução visam diminuir a probabilidade de uma ameaça ocorrer;
- contramedidas de detecção visam detectar incidentes;
- contramedidas repressivas visam limitar um incidente;
- contramedidas corretivas visam recuperar os danos causados por um incidente; e
- a aceitação de riscos também é uma possibilidade. Alguns investimentos em contramedidas podem ser caros e de difícil justificativa.

Figura 3 – Medidas de segurança



Fonte: Baars, 2018.

4.1.4 Tipos de ameaças

Em se tratando dos tipos de ameaças, identificar, classificar e enumerar são atividades frequentes dos profissionais de segurança da informação, e as listas de ameaças podem ser classificadas como humanas e não humanas.

- Ameaça humana intencional: as pessoas podem de maneira intencional danificar sistemas de informação por diversas razões, intrusos, hackers ou pessoas que são contra a empresa, funcionários insatisfeitos.
- Ameaça humana não intencional: é quando um funcionário pressiona algum botão errado (deleção, por exemplo), operando algum sistema de maneira descuidada, inserções de dispositivos móveis infectados, instalação de programas indevidos (sem intenção de ameaçar a estrutura de TI).
- Ameaças não humanas: incluem as influências externas, como tempestades, inundações, raios, blecautes, catástrofes naturais. Existem boas práticas em relação à localização da sala de equipamentos, refrigeração, proteção física, redundâncias da rede elétrica, entre outros.

4.1.5 Estratégias de riscos

Existem algumas estratégias comuns para combater os riscos, podemos elencar algumas.

- Prevenção de riscos – definir medidas de segurança de modo a neutralizar as ameaças antes que elas aconteçam ou se tornem um incidente de segurança, atuar de maneira proativa, manter softwares atualizados e antivírus operacionais são métodos com caráter preventivo.
- Redução de riscos – tomar algumas medidas de modo que a ameaça não se manifeste ou que o dano resultante seja minimizado.
- Tolerância aos riscos – tendo em vista os custos relacionados com as medidas de segurança, em alguns casos, os riscos são aceitos. Esse tipo de estratégia torna a área de segurança da informação reativa, atuando de maneira repressiva.

4.2 ISO 27002

A ISO 27002 é uma norma internacional que apresenta um guia com as melhores práticas e serve como base para a criação de um Sistema de Gestão de Segurança da Informação (SGSI), estabelece algumas diretrizes e princípios gerais para implantação, manutenção e melhoria da gestão de segurança da informação. Essa norma pode ser implantada em qualquer tipo organização, seja ela pública ou privada, de qualquer segmento, pequeno, médio ou grande porte, com ou sem fins lucrativos e não apenas em empresas da área de tecnologia da informação.

4.2.1 Vantagens e benefícios da ISO 27002

Por se tratar de uma norma reconhecida mundialmente, apresenta muitas vantagens, dentre elas, podemos citar:

- melhor conscientização sobre a segurança da informação;
- maior controle de ativos e informações sensíveis;
- oferece uma abordagem para implantação de políticas de controles;

- oportunidade de identificar e corrigir pontos fracos;
- redução do risco de responsabilidade pela não implementação de um SGSI ou determinação de políticas e procedimentos;
- torna-se um diferencial competitivo para a conquista de clientes que valorizam a certificação;
- melhor organização com processos e mecanismos bem desenhados e geridos;
- promove redução de custos com a prevenção de incidentes de segurança da informação; e
- conformidade com a legislação e outras regulamentações.

4.2.2 Composição da ISO 27002

A ISO 27002 é a norma composta por alguns tópicos, e que correspondem a diretrizes e controles de segurança da informação. Toda essa composição pode ser utilizada como diretrizes e servir como base para o implemento de um SGSI. Podemos elencar os seguintes tópicos.

- Política de Segurança da Informação – a política de segurança deve ser criada pela área de TI da organização alinhada com a área de recursos humanos, apresentar os conceitos de segurança da informação, uma estrutura para apontar os objetivos e as formas de controle e ter apoio da alta administração.
- Organização da Segurança da Informação – nesse tópico é necessário montar uma estrutura e gerenciar de maneira eficiente. As atividades de segurança da informação precisam ser coordenadas por líderes de departamentos, atribuir responsabilidades, definir toda a equipa que estará envolvida e ter sempre o intuito de proteção a dados e informações de caráter sigiloso.
- Gestão de ativos – os ativos de uma organização precisam ser protegidos. É necessário todo um trabalho para identificação e levantamento de ativos, de tal maneira que esse inventário seja estruturado e posteriormente manutenido e atualizado. Com isso, há algumas técnicas

para que documentação seja útil, uma definição em relação as atividades de cada ativo, e permissões de acesso são bem importantes para o SGSI.

- Segurança em Recursos Humanos – a contratação de colaboradores e os vínculos com fornecedores requerem uma avaliação prévia pela área de recursos humanos e setores da administração, a ideia é sempre minimizar o risco de roubo, fraude ou má utilização de recursos. Os colaboradores devem estar cientes das ameaças relativas à segurança da informação, das suas responsabilidades e obrigações e da política de segurança da informação da organização.
- Segurança física e do ambiente – o concentrador de equipamentos e as instalações da central de processamento de dados são áreas críticas que requerem cuidados e atenção, devem ser manutenidas e ocuparem locais seguros, com níveis e controles de acesso, energia elétrica redundante, monitores de temperatura, incluindo proteção contra ameaças físicas e ambientais.
- Segurança das operações e comunicações – a definição de manuais, documentação e procedimentos, bem como o elenco de responsabilidades pela gestão e operação de processamento das informações é essencial. Isso engloba todo o gerenciamento de serviços terceirizados, a parte de planejamento dos recursos dos sistemas para mitigar o risco de falhas, rotinas diárias, semanais e mensais de cópias de segurança, a sua recuperação e a administração resiliente e segura das redes de comunicações.
- Controle de acesso – toda a acessibilidade à informação, como todos os recursos de processamento de dados e as informações que suportam os processos de negócios devem receber um controle bem implementado, pautado nos requisitos de negócio e na segurança da informação. Deve ser cadastrado e registrado todo o acesso de usuário, autorizações, granularidade de acesso, sempre identificando e prevenindo acessos não autorizados, com a finalidade de evitar os danos a documentos e recursos de dados e informações das organizações.
- Aquisição, desenvolvimento e manutenção de sistemas – requisitos de segurança de sistemas de informação devem ser analisados, identificados

e alinhados antes do seu desenvolvimento e implementação, para que estejam protegidos vislumbrando sempre a manutenção de sua confidencialidade, autenticidade ou integridade, utilizando meios seguros e criptografados.

- Gestão de incidentes de segurança da informação – toda a documentação e registros de incidentes, bem como o fluxo deles por parte da equipe técnica deve ser bem definido e estabelecido, os colaboradores, os fornecedores e parceiros devem estar alinhados em relação aos procedimentos para notificação de eventos de segurança da informação, para atender e assegurar que sejam comunicados o mais rápido possível e que a correção e a resolução dos incidentes seja feita de maneira eficiente e eficaz.
- Gestão da continuidade do negócio – o planejamento de continuidade do negócio deve ser criado e desenvolvido com o intuito de impedir a interrupção das atividades de negócio, com a finalidade de assegurar que todas as operações essenciais sejam rapidamente recuperadas, sem problemas relacionados com a disponibilidade de sistemas, redes de computadores e demais recursos computacionais.
- Conformidade – é essencial impedir qualquer tipo de violação a leis criminais ou cíveis, respeitando sempre os estatutos, normas, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. As organizações podem contratar uma consultoria especializada em segurança da informação para garantir toda a sua conformidade e aderência a requisitos legais e regulamentares.

TEMA 5 – ISO 31000

Entidades de todos os tamanhos e segmentos se deparam com fatos e influências internas e externas que colocam um clima de incerteza em relação ao atingimento de metas e objetivos. Os efeitos dessas incertezas sobre os objetivos das empresas são identificados como risco.

Todos os processos de negócios de uma organização envolvem risco. As empresas tentar controlar o risco, fazendo a identificação, analisando seus impactos, na sequência, é possível fazer uma análise desses riscos, tentar mitigá-los, a fim de minimizar os efeitos, elaborar um tratamento dos riscos. Ao

longo dessa atividade, é necessária a comunicação entre os interessados, assegurar que esses riscos não modifiquem ou impeçam o bom funcionamento das empresas.

Essa norma trata do processo sistemático e lógico com todas as suas especialidades. Mesmo que todas as organizações gerenciem os riscos de alguma maneira, ela traz um número de princípios que precisam ser atendidos para tornar a gestão de riscos mais eficaz. Esse guia recomenda que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cuja finalidade é integrar o processo para gerenciar riscos na governança, estratégia, planejamento e gestão, processos esses que devem reportar dados e resultados, políticas, valores e cultura em toda a organização.

5.1 Princípios

A gestão de riscos deve atender alguns princípios, dos quais podemos destacar que ela:

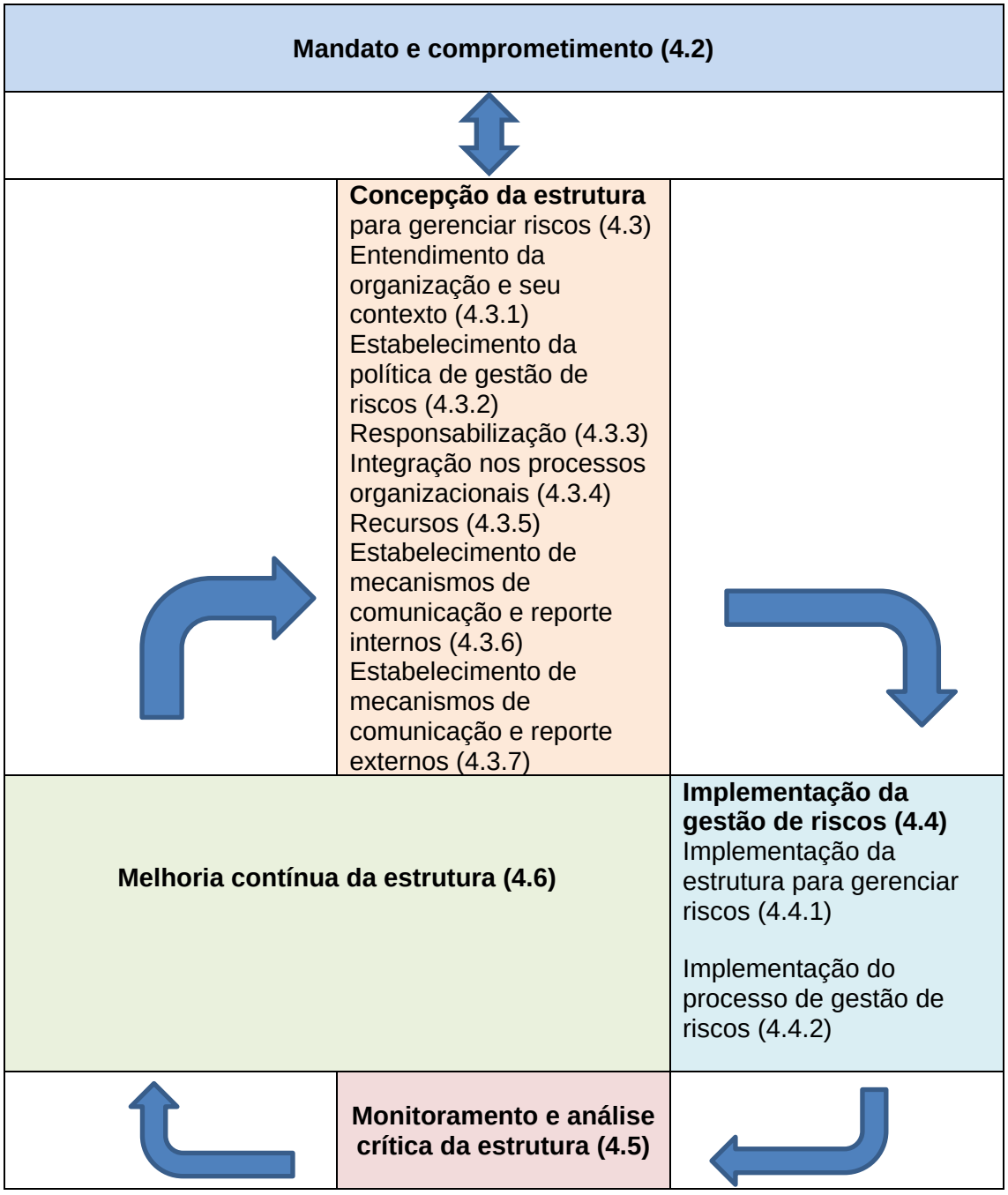
- cria e protege valor;
- é parte integrante de todos os processos organizacionais;
- é parte da tomada de decisões;
- aborda explicitamente a incerteza;
- é sistemática, estruturada e oportuna;
- baseia-se nas melhores informações disponíveis;
- é feita sob medida;
- considera fatores humanos e culturais;
- é transparente e inclusiva;
- é dinâmica, interativa e capaz de reagir a mudanças; e
- facilita a melhoria contínua da organização.

5.2 Estrutura

Para atingir os objetivos da gestão de riscos, é necessária uma boa estrutura e gestão para o fornecimento de fundamentos e os arranjos necessários para que essa gestão seja incorporada à organização, em todas as

suas áreas e níveis. Ao gerenciar os riscos em todos os níveis da organização, a estrutura deve assegurar que as informações provenientes dessa gestão criem processos adequados e alinhados com a segurança da informação, melhorando a tomada de decisões e criando responsabilidades dentro de cada nível organizacional. Os componentes envolvidos nessa estrutura são apresentados na figura a seguir, bem como os seus relacionamentos.

Figura 4 – Relacionamento entre componentes da estrutura de gerência de riscos

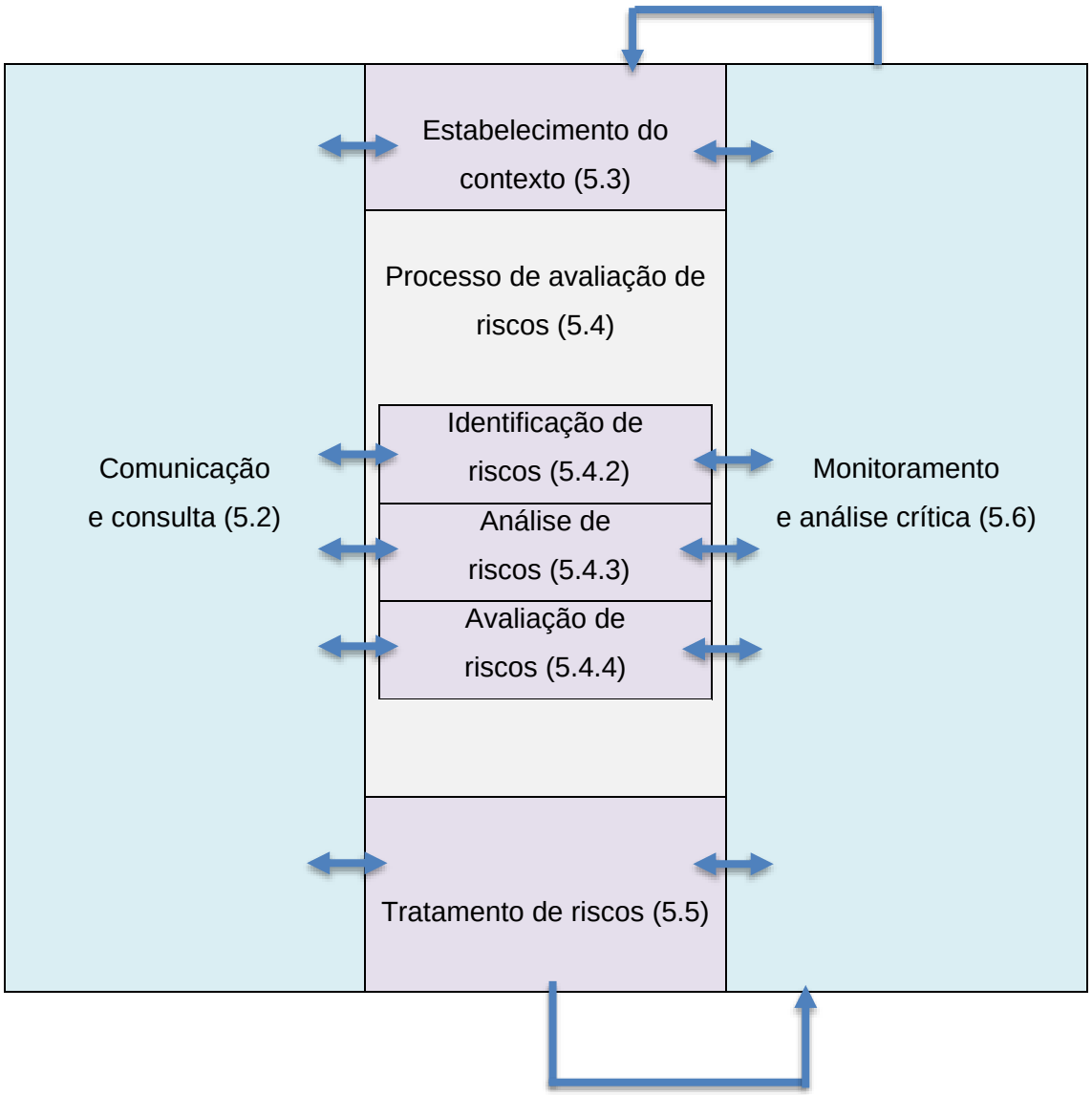


Fonte: ABNT ISO 31000.

5.3 Processo

Os processos relacionados com a gestão de riscos devem estar integrados com a gestão, deve fazer parte da cultura organizacional, nos processos, na prática e alinhado aos processos de negócios da organização. A figura a seguir apresenta as etapas do processo de gestão de risco.

Figura 5 – Processo de gestão de riscos



Fonte: ABNT ISO 31000.

5.4 Monitoramento e registros de gestão de riscos

O monitoramento e a análise da gestão de riscos requerem uma vigilância regular, as responsabilidades desse monitoramento devem estar bem definidas, a fim de garantir controles eficientes ao longo da operação da empresa, sempre obter novas informações para a melhoria contínua do processo de avalição de riscos, análise continuada de eventos, incidentes, problemas, mudanças, tendências, falhas e acerto, alterações de critérios de riscos, revisão dos tratamentos de risco, prioridades e identificação de riscos emergentes.

Em relação aos registros de atividades relacionados com a gestão de riscos, podemos destacar alguns fundamentos que ajudam na melhoria dos métodos, as ferramentas utilizadas, e a criação de registro. Devem ser levados em conta alguns itens como:

- desenvolver a cultura dentro da organização de aprendizado contínuo;
- as vantagens na reutilização de informações para fins de gestão;
- os valores e tempos envolvidos na criação e manutenção de registros;
- a obrigação em relação a registros legais, regulatórios e operacionais;
- os guias de acesso, a facilidade de recuperação e meios de armazenamento;
- o tempo e período de retenção;
- a sensibilidade e a importância das informações.

FINALIZANDO

Em nossa aula sobre segurança da informação, estudamos alguns conceitos relacionados com a segurança da informação, o ciclo de vida dos dados, a classificação da informação, as premissas de segurança, e apresentamos algumas normas e ISOs da família 27000 e a ISSO 31000, as quais são normas que estão intimamente relacionadas com a segurança da informação. O objetivo foi demostrar os principais conceitos de segurança que servirão como base para o desenvolvimento de nosso estudo.

REFERÊNCIAS

ABNT. Gestão de Riscos – Princípios e diretrizes. **NBR ISO 31000**. Associação Brasileira de Normas Técnicas, 2009.

ALVES, D. **Internet das Coisas (IoT)**: segurança e privacidade de dados pessoais. Rio de Janeiro: Alta Books, 2021.

BAARS, H. **Foundations of Information Security**: based on ISO 27001 and 27002. Rio de Janeiro: Brasport, 2018.

FRAGA, B. **Técnicas de invasão**: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Labrador, 2019.

GALVÃO, M. da C. **Fundamentos em Segurança da Informação**. São Paulo: Pearson Education do Brasil, 2015.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 15408-1:2005. **Information technology** – Security techniques – Evaluation criteria for IT security – Part 1: introduction and general model, 2005.