EAD UNISANTA

AUDITORIA DE SISTEMAS

Me. Luiz Antonio Ferraro Mathias

GUIA DA
DISCIPLINA

Objetivo:

A disciplina de Auditoria de Sistemas tem como objetivo desenvolver habilidades para realização de auditoria de sistemas de informação, estudar os conceitos que envolvem a auditoria, prover o conhecimento da organização de um trabalho de auditoria, dos diversos componentes de uma política de segurança, permitindo a identificação da necessidade e as características de um processo de gestão de continuidade de negócios e da identificação das etapas de um trabalho de auditoria de sistemas de informação.

Introdução:

A auditoria de sistemas pretende assegurar que os ativos de informação, estejam absolutamente sob controle da organização. Para tal, é preciso verificar que os controles estejam de acordo com as normas e políticas de segurança estabelecidas para esses ativos, bem como se o que está em operação alcança os objetivos de segurança definidos. A auditoria de segurança de informação envolve também o provimento de uma avaliação independente dos controles da organização (normas, políticas, padrões, procedimentos, práticas, métricas e mecanismos) empregados para salvaguardar a informação, em formato eletrônico ou não, contra perdas, danos, divulgação não intencional e indisponibilidades. Neste contexto, a auditoria é realizada na forma de ações planejadas e que visam produzir resultados dentro de custos, prazos e qualidades esperadas.

O aluno participante da disciplina de Auditoria de Sistemas do Curso de Análise e Desenvolvimento de Sistemas, na modalidade de Ensino à Distância (EaD) da UNISANTA, compreenderá os fundamentos de auditoria de sistemas, conceitos básicos da auditoria, conceitos fundamentais da auditoria, planejamento da auditoria, auditoria em sistemas de informação, o papel do auditor, modelos para segurança da informação, certificações em segurança da informação, Privacidade de dados.

1. FUNDAMENTOS DA AUDITORIA DE SISTEMAS

1.1. Conceito de auditoria

A auditoria é uma função independente que busca priorizar a qualidade dos processos e otimizar os resultados operacionais, envolvendo uma técnica, uma análise, um levantamento criterioso, um estudo e uma forma de avaliação sistemática dos procedimentos, práticas e rotinas internas de uma organização.

O objetivo da auditoria é em primeiro lugar compreender e reconhecer como o negócio da organização opera, quais são suas vantagens, dificuldades e seu processo de desenvolvimento, que são voltados aos trabalhos para proporcionar informações sólidas e seguras que muito contribuirão com desenvolvimento organizacional. A responsabilidade de um processo de auditoria vai além de um simples parecer, uma vez que se propõem é manter uma preocupação contínua com os resultados da organização, envolvendo a postura dos dirigentes quanto a tomada de decisões, observando a confiabilidade das informações e sua transparência junto aos acionistas, sociedade e ao público em geral.

1.2. Tipos de auditoria

1.2.1. Auditoria contábil

A auditoria contábil é um processo de análise da situação financeira da empresa que permite atestar a precisão dos registros contábeis, identificar falhas de controle ou mesmo fraudes e irregularidades na gestão.

Ela é realizada a partir do exame de documentos contábeis e de inspeções internas, contando ainda com a apuração de informações junto a fontes externas. Podem ser auditados o fluxo de caixa, o balanço patrimonial e a Demonstração de Resultado de Exercício (DRE).

Por suas características, a auditoria é capaz de apresentar ao empreendedor uma opinião embasada sobre a realidade financeira do negócio, com segurança e transparência, permitindo a ele conhecer os problemas, suas causas e consequências, além de receber orientações sobre possíveis correções a implantar.

1.2.2. Auditoria de controles internos

Toda empresa visa à continuidade, ou seja, a capacidade de produzir riqueza e gerar valor continuadamente sem interrupções. Porém, para que isto ocorra, é necessário a criação de mecanismos de controle interno. Dentre esses mecanismos, está a auditoria de controles internos. Pode-se definir como controle interno o conjunto de normas, políticas, procedimentos, instrumentos e ações estabelecidas pela empresa, com o objetivo de enfrentar riscos, visando:

a) Garantir a segurança e a integridade dos ativos e dos sistemas de informação;
b) Reduzir a possibilidade de perdas financeiras e do desgaste da imagem institucional;
c) Desenvolver o negócio, a fim de atingir o resultado das operações;
d) Prover eficiência e eficácia das operações;
e) Dar conformidade às leis, regulamentos, normas e dispositivos estatutários aplicáveis à organização;
f) Incrementar a qualidade das informações financeiras ou contábeis.

O controle interno, para ser prático, deve ser adequado ao tamanho e ao porte das operações da empresa. Além disso, precisa ser objetivo no que se pretende controlar e ser simples em sua aplicação. Precisa, principalmente, ser econômico, levando em consideração a relação custo-benefício.

Bons controles internos, acompanhados de uma auditoria independente, adicionam valor à sua empresa, e dão maior credibilidade aos clientes, fornecedores e investidores. Na ausência de controles internos, existe o risco de a administração tomar decisões (operacionais ou estratégicas) incorretas.

1.2.3. Auditoria ambientais

As auditorias ambientais são um processo sistemático no qual a empresa avalia a sua adequação aos critérios estabelecidos, que podem ser requisitos legais, normas ou exigências definidas pelos seus clientes ou pela própria empresa.

Pode-se dizer que a auditoria ambiental é uma ferramenta para levantamento, controle e monitoramento dos aspectos ambientais das empresas. Ela é realizada de forma clara e objetiva, sendo que os resultados do processo são comunicados para as partes interessadas.

Em relação aos objetivos, alguns exemplos de auditorias são descritos a seguir:

a) Auditoria de Conformidade Legal: a auditoria de conformidade legal tem o objetivo de avaliar a adequação da empresa às normas legais aplicáveis à sua atividade. Esse tipo de auditoria é empregado pelas empresas para prevenir eventuais penalidades pelo não atendimento à legislação ambiental. Pode ser utilizada também para verificação em auditorias de fornecedores, que tem como objetivo verificar o atendimento dos requisitos legais de seus fornecedores. De certa forma, toda a auditoria ambiental tem em sua base a avaliação da conformidade legal, uma vez que este é um requisito fundamental da organização;

b) Auditoria Ambiental de Acompanhamento: a auditoria ambiental de acompanhamento tem por objetivo verificar se as condições estabelecidas em uma auditoria estão sendo cumpridas. Por exemplo, uma empresa que deseja se certificar pode ter algumas não conformidades e/ou pontos de melhorias para serem tratados. Nesse caso, a auditoria de acompanhamento irá verificar se estes pontos levantados foram sanados para o processo de certificação;

c) Auditoria Ambiental de Responsabilidade ou *Due Diligence*: o principal objetivo desse tipo de auditoria é avaliar a existência de passivos ambientais da empresa que possam impactar o negócio em um processo de compra e venda. Estas auditorias também podem ser requeridas por investidores ou bancos em processos de garantias, que desejam verificar os riscos relacionados à determinada empresa.

1.3. Conceito de sistemas

Um sistema é um conjunto de elementos inter-relacionados com um objetivo: produzir relatórios que nortearão a tomada de decisões gerenciais. Neste percurso, pode-se identificar o processo de transforma dados de entrada, agregados aos comandos gerenciais, em saídas. Assim, o feedback do sistema faz com que, no meio da manutenção do ciclo operacional, sejam ativadas novas estratégias empresariais visando à geração de informações qualitativas ou quantitativas para suportar o alcance do sucesso.

Os sistemas são abertos ou fechados. Os sistemas abertos podem receber dados controlados ou não controlados, uma vez que recebem influência do ambiente interno e externo onde operam, enquanto os sistemas fechados, devido à sua natureza, não têm interferência do ambiente e somente poderiam receber os dados controlados. As

delimitações dos sistemas são feitas propositadamente durante seu desenho simplesmente para fomentara segregação das funções dos sistemas incompatíveis. Podem ser tanto adaptáveis, quando implantados para produzir um resultado desejado em um ambiente de grandes mudanças rotineiras, como também corretivos, implantados para produzir um resultado específico e não rotineiro.

1.4. Evolução dos sistemas computacionais

Um sistema computacional é um conjunto de dispositivos eletrônicos utilizados para todo um processamento de alguma informação, ou seja, união de hardware (parte física) e software (parte lógica). Cronologicamente falando, a evolução do sistema computacional se deu em 5 (cinco) gerações, que foram elas: computadores a válvula, computadores a transistor, circuitos integrados, circuitos VLSI e a dos computadores invisíveis.

O primeiro computador digital (figura 1) foi projetado pelo matemático Charles Babbage (1792-1871). Embora Babbage tenha dispendido muito de sua vida e de sua fortuna tentando construir sua "máquina analítica", ele jamais conseguiu pôr o seu projeto em funcionamento porque era simplesmente um modelo matemático e a tecnologia da época não era capaz de produzir rodas, engrenagens, dentes e outras partes mecânicas para a alta precisão que necessitava.

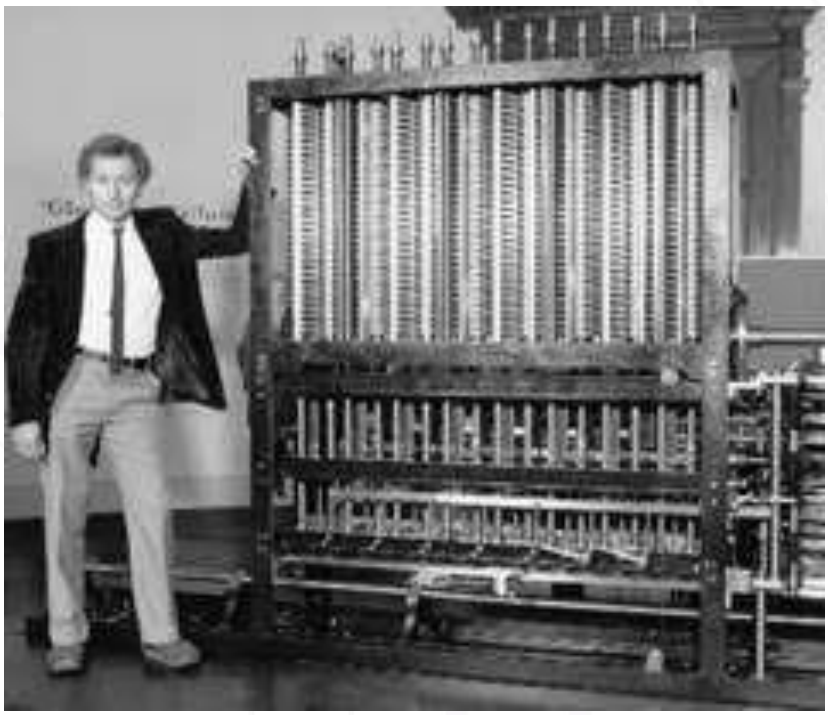


Figura 1 – Charles Babbage ao lado de sua criação.

1.4.1. A primeira geração (1945-1955): Válvulas e painéis

Após os esforços de Babbage, quase não houve progresso nesta área até o início da Segunda Grande Guerra. Em torno de 1940, pesquisadores tiveram sucesso na construção de computadores baseados em válvulas. Tais máquinas eram enormes, ocupavam salas imensas e empregavam dezenas de milhares de válvulas em sua construção.

No ano de 1946, ocorreu uma revolução no mundo da computação com o lançamento do computador ENIAC (figura 2). A principal inovação nesta máquina é a computação digital, muito superior aos projetos mecânicos-analógicos desenvolvidos até então. Com o ENIAC, a maioria das operações era realizada sem a necessidade de movimentar peças de forma manual, mas sim pela entrada de dados no painel de controle. Cada operação podia ser acessada através de configurações-padrão de chaves e switches.

Figura 2 – ENIAC (Electrical Numerical Integrator and Calculator).

Toda a programação era feita em código absoluto, muitas vezes através da fiação de painéis para controlar as funções básicas da máquina. No início dos anos 50, houve uma sensível melhora no uso de tais máquinas como o advento do cartão perfurado que tornou possível a codificação de programas em cartões e leitura pela máquina, dispensando a programação através de painéis.

1.4.2. A segunda geração (1955-1965): Transistores e Sistema Batch

O desenvolvimento do transistor em meados dos anos 50 veio a alterar substancialmente o quadro descrito na segunda geração. Com o emprego desta nova tecnologia, os computadores tornaram-se confiáveis a ponto de serem comercializados.

Os computadores da segunda geração eram usados maciçamente na realização de cálculos científicos e de engenharia, tal como a obtenção da solução de equações diferenciais parciais. Eles eram normalmente programados em linguagem FORTRAN ou em linguagem de montagem. Surgem os sistemas operacionais da época que eram o FMS e o IBSYS.

O IBM 7030 (figura 3), também conhecido por Strech, foi o primeiro supercomputador lançado na segunda geração, desenvolvido pela IBM. Seu tamanho era bem reduzido comparado com máquinas como o ENIAC, podendo ocupar somente uma sala comum. Ele era utilizado por grandes companhias, custando em torno de 13 milhões de dólares na época.

Figura 3 – IBM 7030.

1.4.3. A terceira geração (1965-1980): Circuitos integrados e multiprogramação

Os sistemas de terceira geração vieram a popularizar várias técnicas que não estavam implementadas nos sistemas de segunda geração, a mais importante essas técnicas é a Multiprogramação.

Sistemas operacionais de terceira geração agora tinha a capacidade de ler jobs (um programa ou um conjunto de programas) de cartão direto para disco. Desta forma, assim que um “job ativo” terminasse, o sistema operacional carregaria um novo “job” na partição livre da memória, proveniente do disco.

Um dos principais exemplos da terceira geração é o IBM 360/91, lançado em 1967, sendo um grande sucesso em vendas na época. Esta máquina já trabalhava com dispositivos de entrada e saída modernos, como discos e fitas de armazenamento, além da possibilidade de imprimir todos os resultados em papel. O IBM 360/91 (figura 4) foi um dos primeiros a permitir programação da CPU por microcódigo, ou seja, as operações usadas por um processador qualquer poderiam ser gravadas através de softwares, sem a necessidade do projetar todo o circuito de forma manual.

Figura 4 – Painel de controle do IBM 360.

1.4.4. A quarta geração (1981-1990): Computadores pessoais

A grande disponibilidade de poder computacional, levou ao crescimento de uma indústria voltada para a produção de software s para os computadores pessoais. A maioria destes softwares é “amena ao usuário” (*user-friendly*), significando que eles são voltados para pessoas que não têm nenhum conhecimento de computadores, e mais que isto, não têm nenhuma vontade de aprender nada sobre esse assunto. Certamente esta foi uma mudança grande na filosofia de desenvolvimento dos sistemas operacionais.

E outro desenvolvimento importante que começou a tomar corpo em meados dos anos 80 foi o dos sistemas operacionais para redes e o dos sistemas operacionais distribuídos. Em uma rede de computadores, os usuários estão conscientes da existência de um conjunto de máquinas conectadas à rede, podendo, portanto, ligar-se a máquinas remotas e solicitar serviços destas. Cada uma destas máquinas roda seu próprio sistema operacional e tem seu próprio usuário ou usuários.

Em contraste, um sistema distribuído faz com que um conjunto de máquinas interligadas apareça para seus usuários como se fosse uma única máquina com um só processador. Em tais sistemas, os usuários não tomam conhecimento de onde seus programas estão sendo processados ou mesmo onde seus arquivos estão sendo armazenados, pois tudo isso é manipulado automática e eficientemente pelo sistema operacional.

Figura 5 – Apple 1, o primeiro computador pessoal.

1.4.5. A quinta geração (1990-hoje): Computação distribuída

Os computadores da quinta geração usam processadores com milhões de transistores. Nesta geração surgiram as arquiteturas de 64 bits, os processadores que utilizam tecnologias RISC (acrônimo de *Reduced Instruction Set Computer*; em português, "Computador com um conjunto reduzido de instruções") e CISC (sigla para *Complex Instruction Set Computer*, ou, em uma tradução literal, "Computador com um Conjunto Complexo de Instruções"), discos rígidos com capacidade superior a 600 Gb, pendrives com mais de 100GB de memória e utilização de disco ótico com mais de 1 Tb de armazenamento.

A quinta geração está sendo marcada pela inteligência artificial e por sua conectividade. A inteligência artificial pode ser verificada em jogos e robores ao conseguir desafiar a inteligência humana. A conectividade é cada vez mais um requisito das indústrias de computadores. Hoje em dia, queremos que nossos computadores se conectem ao celular, a televisão e a muitos outros dispositivos como geladeira e câmeras de segurança.

Figura 6 – Computação distribuída

1.5. A importância da segurança da informação

A auditoria de segurança da informação só tem sentido por permitir melhoria do tratamento da informação na organização. Ela cumpre basicamente as mesmas funções de uma auditoria de sistemas de informação, tais como descritos por Imoniana (2004) e por Schmidt, dos Santos e Arima (2005). A informação é produzida, identificada, armazenada, distribuída, usada e processada em todos os níveis da organização, visando o alcance dos objetivos de negócio, sejam eles públicos ou privados. Essas atividades constituem a

gestão da informação, que tem suas práticas definidas pelos sistemas de informação que apoiam os processos de trabalho na organização, sejam eles manuais ou automáticos

A mensagem da necessidade de segurança da informação é usualmente estabelecida por uma política. A política de segurança da informação, tratada em detalhes no texto de Souza Neto (2010), deve tornar claro que cada participante ou colaborador na organização (agentes em geral) é um ator relevante quando se trata de proteger ativos de informação, principalmente aqueles considerados estratégicos ou críticos. Além disso, responsabilidades claras devem ser atribuídas aos agentes, de modo que se possam distribuir tarefas específicas ou gerais para que se esteja sempre aperfeiçoando os mecanismos de segurança da informação implantados. De forma mais prática, a política de segurança da informação é o principal controle de segurança numa organização, e a ele se articulam (e na maioria dos casos se subordinam) todos os demais controles

1.6. A importância da auditoria de segurança da informação

O objetivo é, basicamente, atestar que os controles de segurança em prática são eficientes e eficazes. Tal evita exposições da organização a riscos que podem provocar danos, se concretizados. Mair (1998) indica que a introdução de controles evita:

I. Manter registros de informação que estão errados;
II. Contabilizar informações que não são aceitáveis;
III. Interromper o negócio;
IV. Decidir erroneamente sobre gerenciamento; e dentre outras razões;
V. Evitar fraudes.

No ambiente desregulado dos sistemas de informação expostos à Internet, é também importante destacar que os controles evitam que a organização esteja sujeita a ataques de hackers. O que se busca, efetivamente, é a preservação dos princípios que norteiam o universo da tecnologia da informação: a disponibilidade, a integridade e o caráter confidencial da informação. Uma auditoria busca identificar fragilidades que podem ser exploradas por ameaças internas e externas à uma organização, assim considerando:

i. O comprometimento do sistema de informações, por problemas de segurança, pode causar grandes prejuízos à organização. Diversos tipos de incidentes podem ocorrer a qualquer momento, podendo atingir a informação confidencial, a integridade e disponibilidade;

ii. Problemas de quebra de confidencialidade, por vazamento ou roubo de informações sigilosas, podem expor para o mercado ou concorrência as estratégias ou tecnologias da organização, eliminando um diferencial competitivo, comprometendo a sua eficácia, podendo perder mercado e até mesmo ir à falência;

iii. Problemas de disponibilidade que podem ter um impacto direto sobre o faturamento, pois deixar uma organização sem matéria-prima ou sem suprimentos importantes ou mesmo, o impedimento de honrar compromissos com clientes, prejudicam sua imagem perante os clientes, gerando problemas com custos e levando a margem de lucro a ficar bem comprometida;

iv. Problemas de integridade, causados por invasão ou fatores técnicos em dados sensíveis, sem uma imediata percepção, irão impactar sobre as tomadas de decisões. Decisões erradas fatalmente reduzirão o faturamento ou aumentarão os custos, afetando novamente a margem de lucros;

v. A invasão da página de Internet de uma empresa, com modificação de conteúdo, ou até mesmo a indisponibilidade de serviços on-line, revela a negligência com a segurança da informação e causa perdas financeiras a quem sofreu algum tipo de ataque.

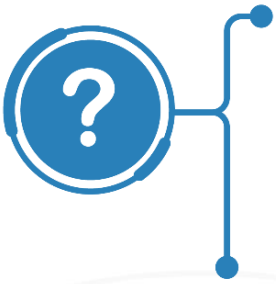
Saiba mais

Os *hackers* são pessoas com um conhecimento profundo de tecnologia e computação que trabalham desenvolvendo e modificando softwares e hardwares de computadores, não necessariamente para cometer algum crime. Eles também desenvolvem novas funcionalidades no que diz respeito a sistemas de informação. Portanto, qualquer pessoa que tenha conhecimento profundo em alguma específica da computação, descobrindo utilidades além das previstas nas especificações originais, pode ser chamada de hacker.

2. CONCEITOS BÁSICOS DA AUDITORIA

Alguns conceitos básicos relacionados com a auditoria são: campo, âmbito e área de verificação.

a) O **campo** compõe-se de aspectos como: objeto, período e natureza da auditoria.
b) O **objeto** é definido como o "alvo" da auditoria, pode ser uma entidade completa (corporações públicas ou privadas, por exemplo).
c) **Período** a ser fiscalizado pode ser um mês, um ano ou, em alguns casos, poderá corresponder ao período de gestão do administrador da instituição.
d) A **natureza** da auditoria poderá ser operacional, financeira ou de legalidade, por exemplo.
e) O **âmbito da auditoria** pode ser definido como a amplitude e exaustão dos processos de auditoria, ou seja, define o limite de aprofundamento dos trabalhos e o seu grau de abrangência.
f) A **área de verificação** pode ser conceituada como sendo o conjunto formado pelo campo e âmbito da auditoria.



Saiba mais

A auditoria é uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o objetivo de verificar sua conformidade com certos objetivos e políticas institucionais, orçamentos, regras, normas ou padrões.

Os procedimentos de auditoria formam um conjunto de verificações e averiguações que permite obter e analisar as informações necessárias à formulação da opinião do auditor. O processo de auditoria é baseado em **controles**, que representam a fiscalização exercida sobre as atividades de pessoas, órgãos, departamentos ou sobre produtos, para que estes não se desviem das normas ou objetivos previamente estabelecidos. Existem 3 (três) tipos de controles (quadro 01):

Controle	Descrição
Preventivos	usados para prevenir fraudes, erros ou vulnerabilidades. (senhas de acesso a algum sistema informatizado, por exemplo.

Detectivos	usados para detectar fraudes, erros, vulnerabilidades (por exemplo: Log de eventos de tentativas de acesso a um determinado recurso informatizado).
Corretivos	usados para corrigir erros ou reduzir impactos causados por algum sinistro (planos de contingência, por exemplo).

Quadro 01: Tipos de controle alvo de uma auditoria de sistemas.

Um dos objetivos desses controles é, primeiramente, a manutenção do investimento feito pela corporação em sistemas informatizados, tendo em vista que os sistemas de informação interconectados de hoje desempenham um papel vital no sucesso empresarial de um empreendimento. Esses controles também têm como objetivo evitar que algum sinistro venha a ocorrer; não conseguindo evitar, tentar fazer com que o impacto seja pequeno e, se mesmo assim, o impacto for grande, ter em mãos processos que auxiliem a reconstrução do ambiente.

Importante

Em geral, é um checklist que contempla os itens a serem verificados durante a auditoria. A concepção desses procedimentos antes do início dos processos de auditoria é de suma importância porque garantirá um aumento da produtividade e da qualidade do trabalho. Como exemplo, pode-se citar que, para o bom andamento de uma partida de futebol, não é aconselhável mudar as regras do jogo enquanto este estiver acontecendo; faz-se isto antes de começar a partida.

O resultado da análise dos controles durante o processo de auditoria se materializa através dos chamados “achados” de auditoria que são fatos importantes observados pelo auditor durante a execução dos trabalhos. Apesar de que geralmente são associados a falhas ou vulnerabilidades, os “achados” podem indicar pontos fortes da corporação auditada. Para que eles façam parte do relatório final de auditoria, estes devem ser relevantes e baseados em fatos e evidências incontestáveis.

Esses registros podem estar em forma de documentos, tabelas, listas de verificações, planilhas, arquivos, entre outros. Estes documentos são a base para o relatório de auditoria, pois contêm registro da metodologia utilizada, procedimentos, fontes de informação, enfim, todas as informações relacionadas ao trabalho de auditoria.

Elas são medidas corretivas possíveis, sugeridas pela pelo auditor em seu relatório, para corrigir as deficiências detectadas durante o trabalho de verificação de vulnerabilidades ou deficiências. Dependendo da competência ou posição hierárquica do órgão fiscalizador, essas recomendações podem se transformar em determinações a serem cumpridas (DIAS, 2000).

2.1. Classificação das auditorias

Vários autores fazem uma classificação ou denominação formal sobre a natureza ou sobre os diversos tipos de auditorias existentes. Os tipos mais comuns são classificados quanto: à forma de abordagem, ao órgão fiscalizador e à área envolvida. Acompanhe, a seguir, quais são elas:

Quanto à forma de abordagem:

Controle	Descrição
Auditoria horizontal	auditoria com tema específico, realizada em várias entidades ou serviços paralelamente.
Auditoria orientada	focaliza uma atividade específica qualquer ou atividades com fortes indícios de fraudes ou erros.

Quanto ao órgão fiscalizador:

Controle	Descrição
Auditoria interna	auditoria realizada por um departamento interno, responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um de seus objetivos é reduzir a probabilidade de fraudes, erros, práticas ineficientes ou ineficazes. Este serviço deve ser independente e prestar contas diretamente à classe executiva da corporação.
Auditoria externa	auditoria realizada por uma empresa externa e independente da entidade que está sendo fiscalizada, com o objetivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e regularidade de suas operações.
Auditoria articulada	trabalho conjunto de auditorias internas e externas, devido à superposição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

Quanto à área envolvida:

Controle	Descrição
Auditoria de programas de governo	Acompanhamento, exame e avaliação da execução de programas e projetos governamentais. Auditoria do planejamento estratégico – verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias são respeitadas.
Auditoria administrativa	engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão.
Auditoria contábil	é relativa à fidedignidade das contas da instituição. Esta auditoria, consequentemente, tem como finalidade fornecer alguma garantia de que as operações e o acesso aos ativos se efetuem de acordo com as devidas autorizações.
Auditoria financeira	conhecida também como auditoria das contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas. Auditoria de legalidade – conhecida como auditoria de conformidade. Consiste na análise da legalidade e regularidade das atividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.
Auditoria operacional	incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob a ótica da economia, eficiência e eficácia. Analisa também a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.
Auditoria de sistemas informatizados	tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informação, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências.

Dependendo da área de verificação escolhida, este tipo de auditoria pode abranger: todo o ambiente de tecnologia ou a organização do departamento de tecnologia. Além disso, pode ainda contemplar: os controles sobre banco de dados, redes de comunicação e de computadores e controles sobre os aplicativos.

Deste modo, sob o ponto de vista dos tipos de controles citados, a auditoria pode ser separada em duas grandes áreas:

a) **Auditoria de segurança de informações** - este tipo de auditoria em ambientes informatizados determina a postura ou situação da corporação em relação à segurança. Avalia a política de segurança e os controles relacionados com aspectos de segurança, enfim, controles que influenciam o bom funcionamento dos sistemas de toda a organização. São estes:

i. Avaliação da política de segurança;
ii. Controles de acesso lógico;
iii. Controles de acesso físico;
iv. Controles ambientais;
v. Plano de contingência e continuidade de serviços;
vi. Controles organizacionais;
vii. Controles de mudanças;
viii. De operação dos sistemas;
ix. Controles sobre o banco de dados;
x. Controles sobre computadores;
xi. Controles sobre ambiente cliente-servidor.

b) **Auditoria de aplicativos** - este tipo de auditoria está voltado para a segurança e o controle de aplicativos específicos, incluindo aspectos que fazem parte da área que o aplicativo atende, como: orçamento, contabilidade, estoque, marketing, RH etc. A auditoria de aplicativos compreende:

i. Controles sobre o desenvolvimento de sistemas aplicativos;
ii. Controles de entrada, processamento e saída de dados;
iii. Controles sobre o conteúdo e funcionamento do aplicativo com relação à área por ele atendida.

2.2. Motivação das auditorias

Um ditado popular diz "*que nenhuma corrente é mais forte que seu elo mais fraco*"; da mesma forma, "*nenhuma parede é mais forte que a sua porta ou janela mais fraca, de modo que você precisa colocar as trancas mais resistentes possíveis nas portas e janelas*". De forma similar é o que acontece quando você implementa segurança em um ambiente de informações. Na realidade, o que se procura fazer é eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível para estes.

Acima de tudo, o bem mais valioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as informações relacionadas com este bem de consumo ou serviço. Ao longo da história, o ser humano sempre buscou o controle das informações que lhe eram importantes de alguma forma; isto é verdadeiro mesmo na mais remota antiguidade. O que mudou desde então foram as formas de registros e armazenamento das informações; se na pré-história e até mesmo nos primeiros milênios da idade antiga o principal meio de armazenamento e registro de informações era a memória humana, com o advento dos primeiros alfabetos isto começou a mudar. Mas foi somente nos últimos dois séculos que as informações passaram a ter importância crucial para as organizações humanas.

Atualmente, não há organização humana que não seja altamente dependente da tecnologia de informações, em maior ou menor grau. E o grau de dependência agravou-se muito em função da tecnologia da informação, que permitiu acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, meio de acesso e meio de divulgação. Independente do setor da economia em que a empresa atue, as informações estão relacionadas com seu processo de produção e de negócios, políticas estratégicas, de marketing, cadastro de clientes etc. Não importa o meio físico em que as informações estão armazenadas, elas são de valor inestimável não só para a empresa que as gerou, como também para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria das vezes elas estão relacionadas com atividades diárias da empresa que, sem elas, poderia ter dificuldades.

Tradicionalmente, as empresas dedicam grande atenção de seus ativos físicos e financeiros, mas pouca ou até mesmo nenhuma atenção aos ativos de informação que possuem; esta proteção tradicional pode nem mesmo visar um bem valioso. Da mesma forma que seus ativos tangíveis, as informações envolvem 3 (três) fatores de produção tradicionais: capital, mão-de-obra e processos. Assim, ainda que as informações não sejam passíveis do mesmo tratamento fisco-contábil que os outros ativos, do ponto de vista do negócio, elas são um ativo da empresa e, portanto, devem ser protegidas. Isto vale tanto para as informações como para seus meios de suporte, ou seja, para todo o ambiente de informações (O`BRIEN, 2002).

Numa instituição financeira, o ambiente de informações não está apenas restrito à área de tecnologia, ele chega a mais longínqua localização geográfica onde haja uma agência ou representação de qualquer tipo. Enquanto na área de tecnologia os ativos de informação estão armazenados, em sua maior parte, em meios magnéticos, nas áreas fora deste ambiente eles ainda estão representados em grande parte por papéis, sendo muito tangíveis e de entendimento mais fácil por parte de seres humanos.

E, dada a característica de tais empreendimentos que, no caso de bancos é essencialmente uma relação de confiança, é fácil prever que isto acarretaria completo descontrole sobre os negócios e até uma corrida ao caixa. A atual dependência das instituições financeiras em relação à tecnologia está se estendendo por toda a economia, tornando aos poucos todas as empresas altamente dependentes dos computadores e, consequentemente, cada vez mais sensíveis aos riscos representados pelo eventual colapso do fluxo de informações de controle gerencial.

Os riscos são agravados em progressão geométrica à medida que informações essenciais ao gerenciamento dos negócios são centralizadas e, principalmente, com o aumento do grau de centralização. Ainda que estes riscos sejam sérios, as vantagens dessa centralização são maiores, tanto sob aspectos econômicos, quanto sob aspectos de agilização de processos de tomada de decisão em todos os níveis. Esta agilização é tanto mais necessária, quanto maior for o uso de facilidades de processamento de informação pelos concorrentes.

É preciso, antes de qualquer coisa, cercar o ambiente de informações com medidas que garantam sua segurança efetiva a um custo aceitável, pois é impossível obter-se segurança total já que, a partir de um determinado nível, os custos envolvidos tornam-se cada vez mais onerosos e superam os benefícios obtidos. Estas medidas devem estar claramente descritas na política global de segurança da organização, delineando as responsabilidades de cada grau da hierarquia e o grau de delegação de autoridade e, muito importante, estarem claramente sustentadas pela alta direção.

A segurança, mais que estrutura hierárquica, os homens e os equipamentos envolvem uma postura gerencial, que ultrapassa a tradicional abordagem da maioria das empresas.

3. CONCEITOS FUNDAMENTAIS DAS AUDITORIAS

O processo de auditoria é baseado em um conjunto de conceitos fundamentais, dentre os quais, há de se destacar:

a) **Ativo**: qualquer coisa que tenha valor e relevância para organização, envolvendo: documentos, sistemas informatizados, ativos de processamento de informação (equipamentos), manuais etc.;

b) **Incidente**: um simples ou uma série de eventos de segurança indesejados ou inesperados que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança (exemplo: vírus de computador, instalação de softwares ilegal, acessos não autorizados etc.;

c) **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

As vulnerabilidades por si só não provocam incidentes de segurança, porque são elementos passivos. Porém, quando possuem um agente causador, como ameaças, esta condição favorável causa danos ao ambiente. As vulnerabilidades podem ser:

Controle	Descrição
Físicas	• instalações prediais fora do padrão; • salas de datacenter mal planejadas; • falta de extintores, detectores de fumaça e outros para combate a incêndio em sala com armários • fichários estratégicos; • risco de explosões, vazamentos ou incêndio.
Naturais	• os computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e • outros, como falta de energia, o acúmulo de poeira, o aumento de umidade e de temperatura etc.
Hardware	• falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.
Software	• erros na aquisição de softwares sem proteção ou na configuração podem ter como consequência, uma maior quantidade de acessos indevidos, vazamentos de informações, perda de dados ou indisponibilidade do recurso quando necessário.

Mídias	• discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
Comunicação	• acessos de intrusos ou perda de comunicação.
Humanas	• rotatividade de pessoal, • falta de treinamento, • compartilhamento de informações confidenciais na execução de rotinas de segurança, erros ou omissões; • ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismos, roubos, destruição da propriedade ou dados, invasões ou guerras.

d) **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

O termo genérico para identificar quem realiza ataques em um sistema de computadores é hacker. Porém, tal generalização possui diversas ramificações, pois cada ataque apresenta um objetivo diferente. Por definição, hacker são aqueles que utilizam seus conhecimentos para invadir sistemas, sem a intenção de causar danos às vítimas, mas como um desafio às suas habilidades.

As mais famosas técnicas de ataques às redes corporativas são:

i. **Quebra de Senha** – O quebrador de senha, ou cracker, é um programa usado pelo hacker para descobrir uma senha do sistema. Uma das formas de quebra são os testes de exaustão de palavras, a decodificação criptográfica etc.;

ii. **Denial of Service** – Também conhecido como DoS, estes ataques de negação de serviço são aborrecimentos semelhantes aos mails bomba, porém muito mais ameaçadores porque eles podem incapacitar temporariamente uma rede corporativa ou um provedor de acesso. É um ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Sua finalidade não é o roubo de dados, mas a indisponibilidade de serviço. Existem variantes deste ataque, como o DoS distribuído, chamado DDoS, ou seja, a tentativa de sobrecarregar o I/O de algum serviço é feita de vários locais ao mesmo tempo;

iii. **Cavalo de troia** – É um programa disfarçado que executa alguma tarefa maligna. Um exemplo, o usuário roda um jogo qualquer que foi pego na internet. O jogo instala o cavalo-de-troia, que abre uma porta TCP (*Transmission Control Protocol*) no micro para a invasão. Este software não propaga a si mesmo de um computador para outro. Há também o cavalo-de-troia dedicado a roubar senhas e outros dados.

e) **Risco**: probabilidade de uma ameaça explorar uma vulnerabilidade e o impacto desta ocorrência. Categorias: Baixo, médio ou Elevado. O risco pode ser interpretado como a probabilidade de uma ameaça explorar uma vulnerabilidade, multiplicado pelo impacto que será gerado.

Durante o processo de auditoria, é importante a verificação do nível de maturidade do processo de gerenciamento de riscos, que envolve um conjunto de práticas e atividades que incluem a identificação, análise, priorização e monitoramento de eventos que podem ter efeitos positivos ou negativos sobre as metas e objetivos estabelecidos pela organização, seja no nível estratégico, tático ou operacional.

O gerenciamento de riscos envolve:

i. Aumento da probabilidade de atingimento dos objetivos.
ii. Enfrentamento de fatores externos e internos que tornam incertos os objetivos serão alcançados.
iii. Auxílio das organizações no estabelecimento de estratégias e na tomada de decisões fundamentadas.

O gerenciamento de riscos envolve benefícios:

i. Aumenta a probabilidade de atingimento dos objetivos;
ii. Promove a tomada de decisões gerenciais mais assertiva;
iii. Melhora o conhecimento organizacional, a aprendizagem e a comunicação interna e externa;
iv. Aumenta a competitividade no mercado;
v. Aumenta a confiança das partes interessadas;
vi. Encoraja uma cultura de gestão proativa e a mentalidade de riscos;
vii. Promove a gestão de mudanças eficaz;
viii. Otimizar os recursos com foco em riscos críticos;

ix. Fornece base confiável para relatórios confidenciais;
x. Protege as operações de ameaças e incertezas;
xi. Antecipa o conhecimento de potenciais eventos, antes desconhecidos;
xii. Busca a redução de multas, penalidades, e infrações das operações;
xiii. Aumenta o desempenho e a confiabilidade dos processos;
xiv. Minimiza perdas operacionais, financeiras e de qualidade.

O processo de gerenciamento de riscos pode ser observado na figura 07 abaixo:

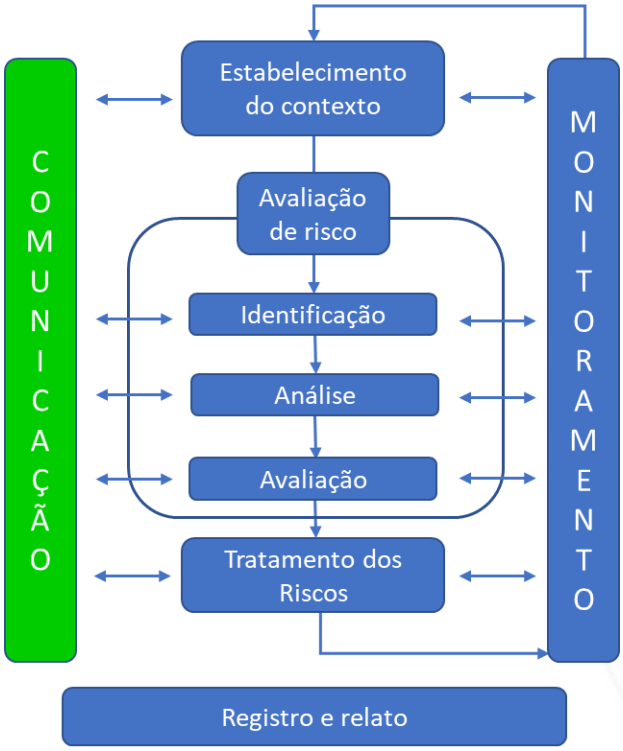


Figura 07: Modelo de gerenciamento de riscos baseado na norma ISO 31000.

4. PLANEJAMENTO DA AUDITORIA

Uma atividade de auditoria pode ser dividida em três fases: planejamento, execução (supervisão) e relatório.

Uma fase vital para qualquer contrato de auditoria é o seu **planejamento**. Ele desempenha o mesmo papel que em outras áreas, na vida pessoal, no desenvolvimento de um novo produto, entre outros. Dele resulta um arranjo ordenado dos passos necessários à condução de determinado objetivo. Tudo que é feito de forma organizada está fadado ao sucesso. O planejamento da auditoria envolve vários passos importantes.

Obtenção de conhecimento do negócio e da organização representa a etapa crítica neste processo, pois estabelece a base para a realização de muitos outros procedimentos de auditoria. Ao planejar o seu trabalho, o auditor toma importantes decisões sobre a relevância e risco de auditoria. Um produto importante do planejamento envolve a tomada de decisões preliminares sobre a estratégia a ser seguida.

Após a etapa do planejamento, vem a **supervisão**. Esta envolve o direcionamento dos trabalhos dos assistentes para atingir os objetivos de auditoria e verificar se os objetivos foram de fato atingidos. A extensão da supervisão necessária em um contrato depende da qualificação das pessoas que realizam os trabalhos, entre outros fatores. Com isto, ao planejar uma auditoria e sua supervisão, também deve ser previsto quantos membros da equipe são inexperientes e quantos são experientes.

A auditoria envolve alguns importantes atores:

a) **Auditor**: Profissional preparado para auditar. Tem formação, capacitação, certificação profissional, minimamente preparado para fazer uma validação, uma análise de conformidade nos trabalhos de campo;
b) **Auditado**: Aquele que é avaliado. Aquele cujos controles estão sobre sua responsabilidade e que serão verificados e validados. Aquele colaborador de certo departamento alvo da auditoria;
c) **Cliente**: Aquele que solicita ou contrata o trabalho de auditoria. Aquele que apoia, patrocina, defende e aprova a contratação. Ex.: Auditoria de SI em uma empresa X. O cliente é o(a) diretor(a) da empresa, visto que foi ele(a) que fez e estabeleceu a contratação, o escopo etc.;

d) **Especialista**: Alguém que tem especificação em certa área para avaliar e transmitir para a equipe de auditoria. Ele detém conhecimentos técnicos sobre determinada ferramenta em um ambiente computacional, por exemplo. Ele não é auditor, não tem formação de auditoria, mas possui um alto conhecimento em certo ambiente e vai auxiliar durante o processo de auditoria, fazendo uma análise e reportando ao auditor as condições;

e) **Guia**: Facilitador. Colaborador da empresa que conhece as áreas, os departamentos, os processos e vai facilitar a vida do auditor. Ele tende a contribuir com o trabalho e desempenho do serviço de auditoria, visto ele conhece a empresa;

f) **Observador**: pode ser alguém da administração pública, autarquia ou órgão regulador que acompanha o serviço de auditoria em execução, bem como um prestador de serviço, um fornecedor de sistema informatizado etc.

Uma auditoria pode ser conduzida através de ciclos, cada qual baseado na execução de fases específica (figura 08).

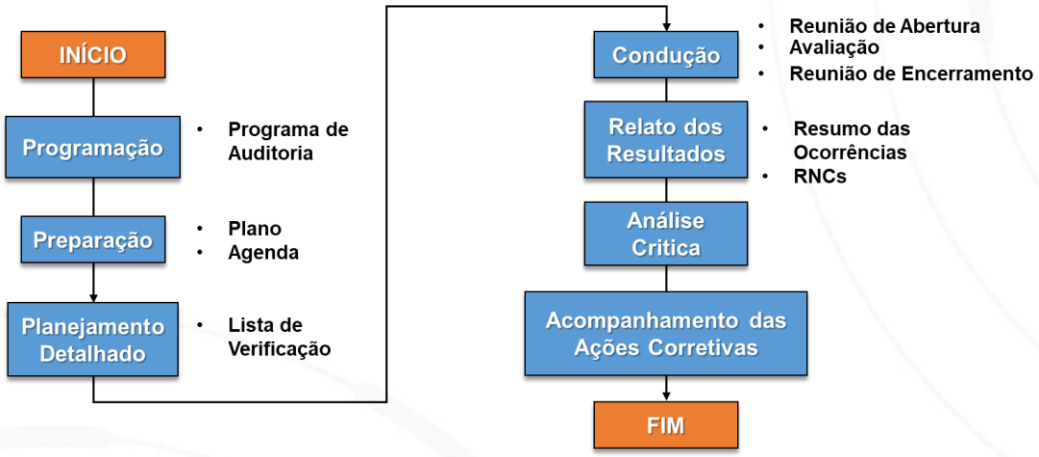


Figura 08: Fases de uma auditoria de conformidade.

As fases da auditoria envolvem um conjunto definido de atividades, assim distribuídas:

i. **Coleta das informações**: envolve contato inicial com o auditado e verificação da amplitude do trabalho no sentido de compreender o tamanho da organização a ser auditada; a complexidade do trabalho a ser realizado; a abrangência das atividades estarão envolvidas e as regras de segurança;

ii. **Preparação**: seleção da equipe de acordo com competências e habilidades; definição da duração estimada dos trabalhos; análise de aspectos e requisitos contratuais; verificação do idioma que será empregado na comunicação com a equipe do auditado; reunião com a equipe; elaboração/adequação das listas de verificação (checklist);

iii. **Escolha das datas**: com atenção especial para férias coletivas, férias de pessoas chave dos processos a serem auditados, feriados nacionais e locais, greves, acontecimentos marcantes (congressos, feiras etc.) regionais;

iv. **Notificações e programa de auditoria**: definição dos processos e controles que serão auditados, requisitos de normais legais e de referência (ISO), expor critérios e programa de auditoria, escopo, unidades e processos, datas e lugares, aspectos logísticos e de confidencialidade;

v. **Reunião de abertura dos trabalhos de auditoria**: organizada e conduzida pelo auditor líder, que pode estar sozinho ou com parte da equipe e representantes da empresa a ser auditada, oportunidade em que se confirma o programa da auditoria, canais de comunicação, esclarece dúvidas, confirma normas aplicáveis ao trabalho, esclarece os conceitos de conformidade e não conformidade, e define reuniões regulares;

vi. **Auditoria de campo**: realização do trabalho de validação pela equipe de auditores e especialistas com o objetivo de garantir a abrangência prevista no contrato. Deve haver clareza no apontamento de fatos, situações, não conformidades etc., entrevistas com a equipe do auditado, registros de inspeções, atas e medições;

vii. **Reunião de encerramento do trabalho de campo**: agradecimentos aos participantes, breve resumo dos trabalhos realizados, exposição das não conformidades e oportunidades de melhoria, esclarecimento de dúvidas, discussão de pontos específicos, definição de prazos de saneamento e adequação de não conformidades e medidas de supervisão, se necessário;

viii. **Relatório final**: que deve conter, minimamente - dados da organização, objetivos e escopo da auditoria, grupos e áreas auditadas, metodologia empregada, normas legais e de referência aplicadas, resultados das validações e conclusões;

ix. **Ações corretivas**: fase em que ocorre a investigação, pelo auditado, das não conformidades apontadas no relatório de auditoria, com documentação das

ações saneadoras, implementação do plano de ação e medição da efetividade deste;

x. **Acompanhamento pelos auditores**: atividade cuja realização depende do escopo da contratação. Nesta fase, a auditoria obtém respostas para as não conformidades, cumprimento dos prazos, e confirmação da efetividade das ações realizadas.

4.1. Conclusão do trabalho de campo

Na fase de conclusão da auditoria, o auditor frequentemente irá trabalhar sob rígidas condições de prazo, pois os clientes querem obter o parecer o mais cedo possível. Nada mais justo, porém é importante lembrar que não se pode sucumbir às pressões decorrentes do trabalho sob pena de emitir um relatório simples demais, de pouca qualidade ou até mesmo com poucos detalhes.

Na conclusão do trabalho de campo, o auditor deve ter certeza de que já fez todas as entrevistas necessárias, coletou todos os dados necessários para analisar as evidências e tecer um parecer correto, que auxilie o cliente a melhorar o seu ambiente de TI aumentando a sua disponibilidade, o seu caráter confidencial e a sua integridade de dados. Uma boa estratégia é revisar as entrevistas com as pessoas envolvidas na administração da tecnologia, relendo-as e confirmando os dados para garantir a integridade de tais informações. Também é importante revisar atas de possíveis reuniões passadas, a fim de se fazer a mesma confirmação.

As normas de auditorias geralmente aceitas não exigem que vulnerabilidades relevantes sejam identificadas separadamente, porém é muito interessante, para um maior entendimento e até programação de investimentos por parte do cliente, que as vulnerabilidades sejam divididas em níveis de severidade, acusando suas consequências caso não sejam remediadas e a medida do risco destas, para se prever em que momento tal fraqueza pode ser explorada por uma ameaça.

Ao avaliar o que foi verificado na auditoria, o auditor tem por objetivo determinar o tipo de parecer a ser emitido e determinar se a auditoria seguiu as normas geralmente aceitas. Para formar opinião sobre as demonstrações contábeis, por exemplo, o auditor deve assimilar todas as evidências que constatou durante a auditoria, da mesma forma que o auditor de sistemas informatizados deve reunir todo tipo de informação coletada do

ambiente de TI do cliente. O primeiro passo é identificar as distorções que foram encontradas e não foram corrigidas pelo administrador de TI. Em casos de pouca severidade, o auditor pode ressaltar o fato de que a alteração pode ser feita mais tarde, porém, em casos graves, ele também pode pedir que a alteração seja feita imediatamente.

Na conclusão da auditoria, é necessário que todas as constatações sejam resumidas e avaliadas. Aqui também é constatada a não conformidade com a norma aceita pelo cliente como sendo padrão de segurança de informação.

Importante

É importante ter cuidado na hora de comunicar toda e qualquer dificuldade em obter informações, ou barreiras encontradas para se chegar ao relatório de conclusão da auditoria.

5. AUDITORIA EM SISTEMAS DE INFORMAÇÃO

Uma auditoria de sistemas de informação pode abranger desde o exame de dados registrados em sistemas informatizados, até a avaliação do próprio sistema informático – aplicativos, sistemas operacionais etc.; a avaliação do ambiente de desenvolvimento, do ambiente de operação, do ambiente de gerenciamento da rede e todos os demais elementos associados a um ou mais sistemas de informação corporativos.

5.1. Técnicas de auditoria de Sistemas de Informação

Existem inúmeras técnicas de auditoria de sistemas de informação. É durante a fase de planejamento da auditoria, dependendo dos objetivos, do escopo e das limitações inerentes ao trabalho, que a equipe de auditoria seleciona as técnicas de auditoria mais adequadas para se chegar às conclusões esperadas do trabalho.

Algumas técnicas usadas em auditorias de sistemas são comuns a outros tipos de auditoria, como:

- entrevista (reunião realizada com os envolvidos com o ponto auditado, que deve ser documentada);
- questionário (conjunto de perguntas que podem ser aplicadas a muitas pessoas simultaneamente, sem a presença do auditor);
- verificação in loco (observação direta de instalações, atividades ou produtos auditados).

Outras técnicas são específicas para a avaliação de operações, transações, rotinas e sistemas em operação ou desenvolvimento. A seguir, acompanhe quais são elas:

Método	Características
Test-deck	consiste na aplicação do conceito de “massa de teste” para sistemas em operação, envolvendo testes normais e corretos, com campos inválidos, com valores incompatíveis, com dados incompletos etc.
Simulação paralela	consiste na elaboração de programas de computador para simular as funções da rotina do

	sistema em operação que está sendo auditado. Utiliza-se os mesmos dados da rotina em produção como input do programa de simulação.
Teste de recuperação	avaliação de um sistema em operação quanto aos procedimentos manuais e/ou automáticos para a recuperação e retomada do processamento em situações de falhas. Um exemplo típico é testar para ver se o backup funciona.
Teste de desempenho	Verificação de um sistema em operação quanto ao consumo de recursos computacionais e ao tempo de resposta de suas operações (exige instrumentos de monitoração para hardware e software).
Teste de estresse	Avaliação do comportamento de um sistema em operação quando submetido a condições de funcionamento envolvendo quantidades, volumes e frequências acima do normal.
Teste de segurança	Avaliação dos mecanismos de segurança preventivos, detectáveis e corretivos presentes no sistema.
Teste de caixa preta	Método que se concentra nos requisitos funcionais dos programas em operação. Os casos de testes, normalmente derivados de diferentes condições de entrada, avaliam funções, interfaces, acessos a bancos de dados, inicialização e término do processamento.
Mapping, tracing e snapshot	Métodos que preveem a inserção de rotinas especiais nos programas em operação, usadas para depurá-los (debug) após serem executados. São estes: Mapping: lista as instruções não utilizadas que determina a frequência daquelas executadas.

	Tracing: possibilita seguir o caminho do processamento dentro de um programa, isto é, visualizar quais instruções de uma transação foram executadas e em que ordem. Snapshot: fornece o conteúdo de determinadas variáveis do programa durante sua execução, de acordo com condições preestabelecidas.
Teste de caixa branca	Concentra-se nas estruturas internas de programas em desenvolvimento. Os casos de testes avaliam decisões lógicas, loops, estruturas internas de dados e caminhos dentro dos módulos.

5.2. Controles gerais

Os controles gerais consistem na estrutura, políticas e procedimentos que se aplicam às operações do sistema computacional de uma organização como um todo. Eles criam o ambiente em que os sistemas aplicativos e os controles irão operar.

Durante uma auditoria em que seja necessário avaliar algum sistema informatizado, seja ele financeiro, contábil, de pagamento de pessoal etc., é preciso inicialmente avaliar os controles gerais que atuam sobre o sistema computacional da organização.

Controles gerais deficientes acarretam uma diminuição da confiabilidade a ser atribuída aos controles das aplicações individuais. Por esta razão, os controles gerais são normalmente avaliados separadamente e antes da avaliação dos controles dos aplicativos que venham a ser examinados em uma auditoria de sistemas informatizados.

São identificadas 5 (cinco) categorias de controles gerais que podem ser consideradas em auditoria:

a) Controles organizacionais - políticas, procedimentos e estrutura organizacional estabelecidos para organizar as responsabilidades de todos os envolvidos nas atividades relacionadas à área da tecnologia;

b) Programa geral de segurança - oferece estrutura para: (1) gerência do risco, (2) desenvolvimento de políticas de segurança, (3) atribuição das responsabilidades de segurança, e (3) supervisão da adequação dos controles gerais da entidade;

c) Plano de continuidade do negócio - controles que garantam que, na ocorrência de eventos inesperados, as operações críticas não serão interrompidas., Elas devem ser imediatamente retomadas e os dados críticos protegidos;

d) Controle de software de sistema - limita e supervisiona o acesso aos programas e arquivos críticos para o sistema que controla o hardware e protege as aplicações presentes. O controle sobre o acesso e a alteração do software de sistema é essencial para oferecer uma garantia razoável de que os controles de segurança baseados no sistema operacional não estão comprometidos, prejudicando o bom funcionamento do sistema computacional como um todo;

e) Controles de acesso - limitam ou detectam o acesso a recursos computacionais (dados, programas, equipamentos e instalações), protegendo estes recursos contra modificação não-autorizada, perda e divulgação de informações confidenciais. Os controles de acesso têm o propósito de oferecer uma garantia razoável de que os recursos computacionais (arquivos de dados, programas aplicativos, instalações e equipamentos relacionados aos computadores) estão protegidos contra modificação ou divulgação não-autorizada, perda ou danos. Eles incluem controles físicos, tais como manutenção dos computadores em salas trancadas para limitar o acesso físico, e controles lógicos (softwares de segurança projetados para prevenir ou detectar acesso não autorizado a arquivos críticos).

5.3. Tipos de auditoría de Sistemas de Informação

Dentre as auditorias de sistemas de informação, destacam-se: auditoria de software aplicativo, auditoria do desenvolvimento de sistemas, auditoria de banco de dados, e auditoria de redes e de equipamentos.

5.3.1. Auditoria de software aplicativo

Os softwares aplicativos são aqueles projetados para executar determinado tipo de operação, a exemplo do cálculo da folha de pagamento ou de controle de estoque. São exemplos de controles que podem ser auditados: controles de aplicativos; controles de entrada de dados; a autorização para entrada de dados; controles do processamento de dados e controles da saída de dados.

5.3.2. Auditoria de desenvolvimento de sistemas

A auditoria do desenvolvimento de sistemas objetiva avaliar a adequação das metodologias e procedimentos de projeto, desenvolvimento, implantação e revisão pós-implantação dos sistemas produzidos dentro da organização auditada.

Esta avaliação pode abranger apenas o ambiente de desenvolvimento da organização ou prever também a análise do processo de desenvolvimento de um sistema específico, ainda na fase de planejamento, já em andamento ou após sua conclusão.

Todos os projetos de desenvolvimento de sistemas precisam ter sido avaliados em profundidade, devendo ser precedidos de análises de custo/benefício, capacidade de satisfação dos usuários e de atendimento aos objetivos da organização, custos de desenvolvimento, medidas de desempenho, planos de implementação, previsão de recursos humanos etc. São necessários, também, mecanismos gerenciais que auxiliem a definição de prioridade dos projetos e permitam sua avaliação e controle durante todo o processo de desenvolvimento.

5.3.3. Auditoria de banco de dados

Tradicionalmente, o termo banco de dados foi usado para descrever um arquivo contendo dados acessíveis por um ou mais programas ou usuários. Os arquivos de dados eram designados para aplicações específicas e o programa era projetado para acessá-los de uma forma predeterminada.

5.3.4. Auditoria de redes de computadores

Atualmente, é bastante comum que os usuários de um sistema estejam em um local diferente de onde se encontram os recursos computacionais da organização. Isto torna necessário o uso de mecanismos de transporte de informações entre diferentes computadores e entre computadores e seus periféricos. Para o bom funcionamento da comunicação de dados são usados:

a) Arquivo log de comunicações, onde ficam registrados todos os blocos transmitidos correta e incorretamente para efeito estatístico e para tentativas de recuperação de dados transmitidos;
b) Software de comunicação de dados para verificação de protocolo de transmissão, gravação do arquivo log de transações e para codificação de sinais de comunicação;

c) Protocolo de transmissão que garante a recepção correta do bloco de informações transmitidas;
d) Software ou hardware para a realização de codificação e decodifcação das informações transmitidas.

O principal risco oferecido pelas redes é o de acesso não autorizado a dados e programas da organização, que pode resultar em danos ou prejuízos intencionais ou acidentais.

5.3.5. Auditoria de equipamentos

Normalmente são chamados microcomputadores os computadores de mesa que compreendem um processador, disco rígido e flexível, monitor e teclado. Os microcomputadores podem ser utilizados isoladamente ou estar conectados a uma rede, com o propósito de compartilhar dados ou periféricos.

Para que possa proteger-se contra diversos tipos de riscos, a organização precisa adotar políticas e procedimentos específicos quanto ao uso de microcomputadores pelos seus funcionários, compreendendo padrões de hardware, software, aquisição, treinamento e suporte, além dos controles gerais e de aplicativos.

Os microcomputadores precisam de controles específicos destinados a protegê-los de furto ou acidente, que podem ocasionar a perda de dados e programas. Isto pode ser evitado através de restrições físicas de acesso às máquinas, controles de software, tais como: senhas de acesso e realização periódica de cópias de segurança. O furto de equipamentos pode ser evitado por meio de mecanismos adequados de segurança no local de trabalho.

6. O PAPEL DO AUDITOR

Coletar evidências sobre a segurança em um sistema informatizado é muito mais complexo do que em um sistema manual, sem automação, justamente devido à diversidade e complexidade da tecnologia de controle interno. Os auditores devem entender estes controles e ter know-how para coletar evidências corretamente. Tecnologias como hardware ou software evoluem muito rapidamente, o que torna o entendimento sobre o controle muito complicado e difícil, pois existem intervalos de surgimento de tecnologias e entendimento destas.

Em alguns casos, não é possível detectar evidências de forma manual. Nesse caso, o auditor terá que recorrer outros recursos como, por exemplo, sistemas informatizados que possibilitem a coleta das evidências necessárias. Novas ferramentas de auditoria podem ser requeridas devido à evolução da tecnologia.

6.1. Necessidades para seu um auditor

Auditores necessitam de grande capacidade de comunicação, pois o serviço pede que ao levantar-se questões relacionadas com o objeto auditado, a discussão seja levada para a camada executiva da empresa e os resultados deste trabalho também. Como a tecnologia influência diretamente a forma como os auditores se comunicam, deve-se recorrer a modelos padronizados que possam passar a extensão, conclusão e observações do trabalho realizado. A capacidade de pensar crítica e estrategicamente é essencial ao auditor.

Saiba mais

Por exemplo, o auditor deve ser capaz de analisar e avaliar o P.D.T. (Plano Diretor de Tecnologia) de um cliente e avaliar se os recursos de TI que existem na corporação manipulam as informações de forma concisa e coerente e atendem aos objetivos previamente definidos para estes sistemas.

Os principais serviços prestados por auditores são:

a) **Assurance**: Assim, os serviços de *assurance* são as traduções de informações provindas dos recursos encontrados no objeto auditado, melhorando o contexto e a qualidade para que a camada executiva possa tomar suas decisões;

b) **Consultoria gerencial**: Os serviços de consultoria gerencial abrangem as recomendações sobre como utilizar os sistemas de informação do cliente de uma forma mais proveitosa e que atenda aos objetivos de negócio da empresa auditada;

c) **Certificação de normas**: Os serviços de certificação de normas são aqueles em que o auditor irá prover uma lista de verificação (checklist) apontando conformidades e não-conformidades segundo determinada norma e irá emitir um parecer sobre a emissão ou não para uma empresa daquele certificado. (CARUSO, 1999).

6.2. Responsabilidades do auditor

Um auditor tem uma relação contratual direta com seus clientes. Quando concorda em prestar serviços, algumas coisas devem ser lembradas pela empresa contratante para que o processo de auditoria, já aprovado pela camada executiva, siga de acordo com os objetivos esperados.

Assim, alguns cuidados são importantes no processo de fechamento do contrato:

- Antes da assinatura do contrato, uma proposta comercial deve ser apresentada à empresa contratante, a fim de se conhecer o escopo de trabalho, ou seja, todas as responsabilidades da empresa contratada e da contratante. Isto é favorável para que, no final dos serviços, possas e fazer um processo de *Quality Assurance* (garantia da qualidade) da auditoria em si, isto é, uma medição do que foi proposto e do que foi realizado.
- A empresa que contratar os serviços de auditoria de terceiros deve ter o cuidado de escolher a empresa contratada seguindo algumas características como: tempo que a empresa está no mercado, se a empresa possui um plano de atualização permanente dos auditores, se a empresa não possui muitas queixas ou processos de clientes, verificar a carteira de clientes da empresa, entre outras características.
- Na hora da assinatura do contrato, é importante observar a parte sobre o sigilo de contrato, que é imprescindível para um contrato de serviços de auditoria. Se a empresa contratada não for de boa índole, pode acontecer de o auditor

repassar informações para concorrentes, já que ele também presta serviço para outras empresas.

Há três situações típicas onde o auditor pode ser responsabilizado por quebra de contrato, a considerar:

i. Na emissão de um parecer-padrão de auditoria sem ter aplicado as normas de auditoria geralmente aceitas;
ii. Na entrega do relatório fora do prazo estipulado;
iii. Na violação da relação confidencial acordada no contrato.

6.3. Competências do auditor

Segurança e confiança no processo de auditoria dependem da competência daqueles que conduzem a auditoria. Esta competência está baseada na demonstração de:

a) Atributos pessoais;
b) Capacidade para aplicar conhecimento e habilidades;
c) Educação, experiência profissional e treinamento em auditoria.

Os auditores devem desenvolver, manter e aperfeiçoar a sua competência através do contínuo desenvolvimento profissional e participação regular em auditorias. Devem ainda possuir atributos pessoais, de forma a permiti-los atuar de acordo com os princípios de auditoria. O Auditor deve ser:

a) Ético: justo, verdadeiro, sincero, honesto e discreto;
b) Mente aberta: disposto a considerar ideias ou pontos de vista alternativos;
c) Diplomático: com tato para lidar com pessoas (em diferentes níveis hierárquicos);
d) Observador: ativamente atento à circunvizinhança e às atividades físicas;
e) Perceptivo: instintivamente atento e capaz de entender situações;
f) Versátil: se ajuste prontamente a diferentes situações;
g) Tenaz: persistente, focado em alcançar objetivos;
h) Decisivo: chegue a conclusões oportunas baseadas em razões lógicas e análises;
i) Autoconfiante: atue e funcione independentemente, enquanto interage de forma eficaz com outros;
j) Bom juiz: julgar as constatações e fazer conclusões acertadas;
k) Paciente: ouvir atentamente o auditado para a coleta de constatações;
l) Imparcial: decidir baseados nas constatações.

Por outro lado, o auditor não deve ser:

i. Ingênuo
ii. Indisciplinado
iii. Teimoso
iv. Frágil
v. Chato
vi. Ansioso para agradar
vii. Inclinado a discussões
viii. Gerador de conflitos
ix. Dono da verdade

Importante

O auditor deve procurar fazer com que suas competências não somente sejam ditadas por normas, mas decorram de foco no cliente e no mercado.

7. MODELOS PARA SEGURANÇA DA INFORMAÇÃO

7.1. Introdução aos modelos de segurança da informação

A crescente utilização de soluções informatizadas nas diversas áreas de serviços exige níveis de segurança adequados e maior exposição dos valores e informações. A evolução da tecnologia de informação, migrando de um ambiente centralizado para um ambiente distribuído, interligando redes internas e externas, somada à revolução da Internet, mudou a forma de se fazer negócios.

Isto fez com que as empresas se preocupassem mais com o controle de acesso às suas informações bem como a proteção dos ataques, tanto internos quanto externos. Paralelamente, os sistemas de informação também adquiriram grande importância para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

7.1.1. Normas ISO

Uma vez que a segurança da informação busca garantir a confidencialidade, a integridade e a disponibilidade das informações, o emprego de um conjunto de boas práticas torna-se fundamental neste desafio. Neste sentido, as normas da família ISO/IEC 27000 convergem para o Sistema de Gestão de Segurança da Informação, tendo como as normas mais conhecidas as ISO 27001 e ISO 27002. São relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. Mas estas não são as únicas relacionadas à segurança da informação e cibersegurança.

7.2. Estrutura do modelo ISO/IEC 27001

A norma ABNT NBR ISO/IEC 27001:2013 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A adoção de um SGSI é uma decisão estratégica para uma organização. O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização. É esperado que todos estes fatores de influência mudem ao longo do tempo.

Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização, incluindo, ainda, requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

A ABNT NBR ISO/IEC 27001 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).

Esta norma recomenda a análise crítica e entendimento do contexto da empresa, envolvendo as questões internas e externas que são relevantes para seu propósito; a compreensão das necessidades e expectativas das partes interessadas; e o escopo do sistema de gestão de segurança da informação.

No aspecto de liderança, é fundamental que a Alta Direção demonstre sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação por vários meios, que estabeleça uma política de segurança da informação (PSI) e que assegure que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados.

As ações para contemplar riscos e oportunidades devem ser estabelecidas pela organização com foco na avaliação e tratamento de riscos de segurança da informação. Complementarmente, a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação a partir da definição de competências, adoção de programas de conscientização, comunicação e documentação das ações.

Na implementação do SGSI é recomendável a adoção do ciclo PDCA (método interativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos). As 4 (quatro) etapas do respectivo ciclo envolvem: *Plan* (planejar),

Do (executar), *Check* (verificar) e *Act* (agir). Este ciclo considera, no contexto do SGSI, um conjunto de atividades conforme pode ser verificado na figura 7.

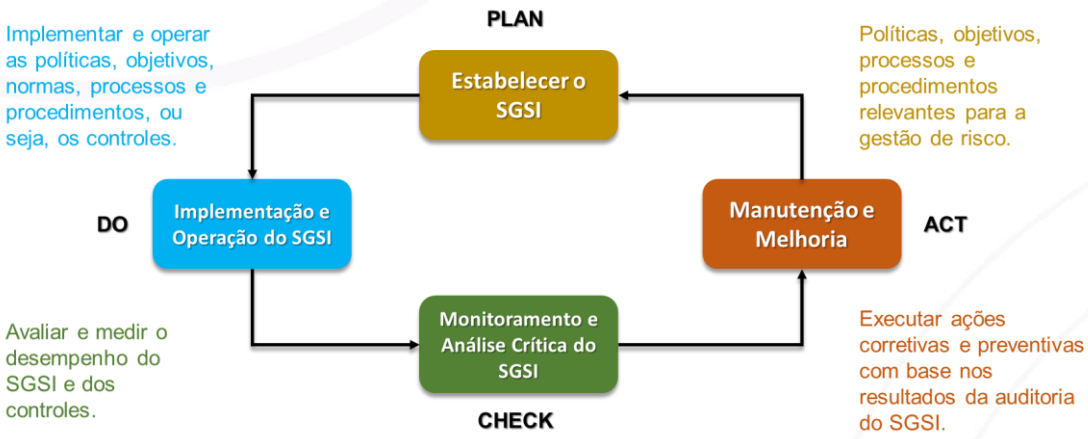


Figura 09: Ciclo PDCA na implementação e melhoria contínua do SGSI.

7.3. Estrutura do modelo ISO/IEC 27002

Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização. Esta Norma é projetada para ser usada por organizações que pretendam:

a) Selecionar controles dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001;
b) Implementar controles de segurança da informação comumente aceitos;
c) Desenvolver seus próprios princípios de gestão da segurança da informação.

Esta Norma contém 14 seções de controles de segurança da informação de um total de 35 objetivos de controles (declarações do que se espera que seja alcançado) e 114 controles (declarações específicas do controle, para atender ao objetivo de controle).

As 14 seções de controles de segurança da informação estão distribuídas da seguinte forma:

7.3.1. *Políticas de Segurança da Informação*

O objetivo de controle prevê uma orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Envolve a elaboração de e análise crítica das políticas para segurança da informação.

7.3.2. *Organização da Segurança da Informação*

Estabelecimento de uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização. Os controles envolvem a definição de responsabilidades e papéis pela segurança da informação, segregação de funções, contato com autoridades, contato com grupos especiais, segurança da informação no gerenciamento de projetos, política para o uso de dispositivo móvel e trabalho remoto.

7.3.3. *Segurança em Recursos Humanos*

O objetivo é assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados. A segurança em recursos humanos ocorre antes, durante e após o encerramento da contratação.

7.3.4. *Gestão de Ativos*

Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos. A gestão de ativos envolve: responsabilidade pelos ativos, inventário de ativos, Proprietário dos ativos, uso aceitável dos ativos, devolução de ativos, classificação da informação, rótulos e tratamento da informação, tratamento dos ativos, gerenciamento de mídias removíveis , descarte de mídias e transferência física de mídias.

7.3.5. *Controle de Acesso*

Limitar o acesso à informação e aos recursos de processamento da informação. Os controles envolvem: política de controle de acesso, acesso às redes e aos serviços de rede, registro e cancelamento de usuário, provisionamento para acesso de usuário, gerenciamento de direitos de acesso privilegiados, gerenciamento da informação de autenticação secreta de usuários, análise crítica dos direitos de acesso de usuário, retirada ou ajuste dos direitos de acesso, uso da informação de autenticação secreta, restrição de acesso à informação, procedimentos seguros de entrada no sistema (*log-on*), sistema de

gerenciamento de senha, uso de programas utilitários privilegiados e controle de acesso ao código-fonte de programas.

7.3.6. Criptografia

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação. Os controles envolvem a política para o uso de controles criptográficos e o gerenciamento de chave.

7.3.7. Segurança Física e do Ambiente

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização. Os controles envolvem: perímetro de segurança física, controles de entrada física, segurança em escritórios, salas e instalações, proteção contra ameaças externas e do meio , trabalho em áreas seguras, segurança em áreas de entrega e de carregamento, localização e proteção do equipamento, utilidades, segurança do cabeamento, manutenção dos equipamentos, remoção de ativos, segurança de equipamentos e ativos fora das dependências da organização, reutilização ou descarte seguro de equipamentos, equipamento de usuário sem monitoração e política de mesa limpa e tela limpa.

7.3.8. Segurança nas Operações

Garantir a operação segura e correta dos recursos de processamento da informação. A segurança das operações envolve a definição de responsabilidades e procedimentos operacionais, documentação dos procedimentos de operação, gestão de mudanças, gestão de capacidade, separação dos ambientes de desenvolvimento, teste e produção, controles contra *malware*, cópias de segurança das informações, registros de eventos, proteção das informações dos registros de eventos (logs), registros de eventos (log) de administrador e operador, sincronização dos relógios, instalação de software nos sistemas operacionais, gestão de vulnerabilidades técnicas, restrições quanto à instalação de software e controles de auditoria de sistemas de informação.

7.3.9. Segurança nas Comunicações

Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. A segurança das comunicações envolve os controles de redes, segurança dos serviços de rede, segregação de redes, políticas e procedimentos

para transferência de informações, acordos para transferência de informações, mensagens eletrônicas, assim como acordos de confidencialidade e não divulgação.

7.3.10. Aquisição, Desenvolvimento e Manutenção de Sistemas

Garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas. Nesta seção são consideradas: análise e especificação dos requisitos de segurança da informação, serviços de aplicação seguros em redes públicas, proteção das transações nos aplicativos de serviços, política de desenvolvimento seguro, procedimentos para controle de mudanças de sistemas, análise crítica técnica das aplicações após mudanças nas plataformas Operacionais, restrições sobre mudanças em pacotes de software, princípios para projetar sistemas seguros, ambiente seguro para desenvolvimento, desenvolvimento terceirizado, teste de segurança do sistema, teste de aceitação de sistemas e proteção dos dados para.

7.3.11. Relacionamento na Cadeia de Suprimentos

Garantir a proteção dos ativos da organização que que são acessados pelos fornecedores. A fim de que isto seja alcançado, são consideradas: política de segurança da informação no relacionamento com os fornecedores, identificação de segurança da informação nos acordos com fornecedores. cadeia de suprimento na tecnologia da informação e comunicação, monitoramento e análise crítica de serviços com fornecedores e gerenciamento de mudanças para serviços com fornecedores.

7.3.12. Gestão de Incidentes de Segurança da Informação

Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. São considerados: responsabilidades e procedimentos, notificação de eventos de segurança da informação, notificação de fragilidades de segurança da informação, avaliação e decisão dos eventos de segurança da informação, resposta aos incidentes de segurança da informação, aprendizado com os incidentes de segurança da informação e coleta de evidências.

7.3.13. Aspectos de SI na Gestão da Continuidade de Negócios

A continuidade da segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização. Esta continuidade envolve: planejamento da continuidade da segurança da informação, implementação da continuidade da segurança da informação, verificação, análise crítica e avaliação da continuidade da segurança da informação e disponibilização dos recursos de processamento da informação.

7.3.14. Conformidades

Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança. O aspecto que envolve a conformidade trata dos seguintes aspectos: identificação da legislação aplicável e de requisitos contratuais, direitos de propriedade intelectual, proteção de registros, proteção e privacidade de informações de identificação pessoal, regulamentação de controles de criptografia, análise crítica independente da segurança da informação, conformidade com as políticas e procedimentos de segurança da informação e análise crítica da conformidade técnica.

8. CERTIFICAÇÕES EM SEGURANÇA DA INFORMAÇÃO

8.1. Introdução às certificações em segurança da informação

A crescente utilização de soluções informatizadas nas diversas áreas de serviços exige níveis de segurança adequados e maior exposição dos valores e informações. A evolução da tecnologia de informação, migrando de um ambiente centralizado para um ambiente distribuído, interligando redes internas e externas, somada à revolução da Internet, mudou a forma de se fazer negócios.

8.2. Certificações relacionadas

Na área de Segurança da Informação é uma prática internacional comum exigir certificações alinhadas com as atribuições do cargo que um dado profissional ocupa ou pretende ocupar. Tais certificações valorizam o currículo do profissional, atestando que ele possui conhecimento ou experiência nos assuntos contemplados pelo conteúdo programático da certificação obtida. Segue abaixo um conjunto de certificações de segurança da informação que podem ser obtidas pelos profissionais que atual nesta área.

8.2.1. Auditor Líder em Segurança da Informação

Certificação do profissional na preparação de auditorias, distribuição de tarefas aos auditores de sua equipe, elaboração e apresentação de relatórios de auditoria, em conformidade com a Norma ISO 27001.

8.2.2. CISA - Certified Information Systems Auditor (ISACA)

A Certificação Profissional em CISA é reconhecida mundialmente como um padrão para aqueles que exercem a função de auditoria, controle, monitoramento e avaliação dos sistemas de informação de negócio nas organizações.

A designação CISA foi criada para profissionais com experiência de trabalho em auditoria de sistemas de informação, controle e segurança que incluem:

- Os processos de Auditoria em Sistemas de Informação;
- Governança e Gerenciamento de TI;
- Aquisição, Desenvolvimento e Implementação de Sistemas de Informação;
- Operação, Manutenção e Suporte em Sistemas de Informação;
- Proteção de Ativos de Informação.

ISACA é o acrônimo para *Information Systems Audit and Control Association* (Associação de Auditoria e Controle de Sistemas de Informação), uma associação internacional que suporta e patrocina o desenvolvimento de metodologias e certificações para o desempenho das atividades de auditoria e controle em sistemas de informação.

8.2.3. CISM - Certified Information Security Manager (ISACA)

A certificação CISM é para profissionais que são responsáveis por projetar, construir e gerenciar a segurança da informação nas organizações e que têm experiência nas seguintes áreas:

- Governança de Segurança da Informação;
- Gerenciamento de Riscos das Informações;
- Desenvolvimento de um Programa de Segurança da Informação;
- Gestão de Programas de Segurança da Informação;
- Gestão de Incidentes e Respostas em Segurança da Informação.

8.2.4. CRISC – Certified in Risk and Information Systems Control Certification (ISACA)

A designação de profissionais certificados em CRISC indica conhecimentos e experiência na identificação e avaliação de riscos e na concepção, execução, acompanhamento e manutenção de controles eficientes e eficazes de riscos.

A certificação CRISC é para os profissionais que estão envolvidos em nível operacional para mitigação de risco, e que possuem experiência nas seguintes áreas:

- Avaliação e Identificação de Riscos;
- Resposta a riscos
- Monitoramento de Riscos;
- Implementação e desenho de controles de Sistemas de Informação;
- Manutenção e Monitoramento de controles de Sistemas de Informação.

8.2.5. CGIT – Certified in the Governance of Enterprise IT (ISACA)

A certificação CGEIT é especialmente desenvolvida para profissionais com posição de gestão significativa no negócio, ou função com grande influência na Governança de TI para a organização. Devem ter ainda, grande experiência nas seguintes áreas:

- Frameworks de Governança de TI;
- Alinhamento Estratégico;

- Entrega de Valor de Ti ao negócio;
- Gerenciamento de Riscos;
- Gestão de Recursos;
- Medição de Performance.

8.2.6. *CISSP – Certified Information Security Systems Professional (ISC²)*

É uma certificação na área de Segurança da Informação que reconhece o nível de conhecimento do profissional em um conjunto de melhores práticas que foram condensadas em 10 domínios:

- Sistemas de controle de acesso;
- Segurança de telecomunicações e redes;
- Governança de Segurança da Informação e Gerenciamento de riscos
- Desenvolvimento seguro de software;
- Criptografia;
- Arquitetura de segurança e design;
- Segurança de operações;
- Plano de continuidade de negócios e recuperação de desastres;
- Leis, regulamentos, investigação e conformidade;
- Segurança física.

É um instituto focado no campo da Segurança da Informação, sem fins lucrativos, orientado a elaboração de certificações profissionais técnicas na área de segurança da informação.

8.2.7. *CSSLP – Certified Secure Software Lifecycle Professional (ISC²)*

Certificação do profissional em uma coleção de melhores práticas, políticas e procedimentos para garantir níveis de segurança adequados em todas as fases do ciclo de desenvolvimento de software, independentemente da tecnologia utilizada. Do conceito e planejamento a operações e manutenção e, finalmente, à eliminação, esta certificação estabelece padrões e práticas recomendadas do setor para a integração de segurança em cada fase.

9. PRIVACIDADE DE DADOS PESSOAIS

9.1. A importância da proteção de dados pessoais

Os dados pessoais têm sido alvo de muitas notícias recentemente, e violações de dados vêm acontecendo em empresas de arquivos de crédito, companhias aéreas e até mesmo naquelas que deveriam saber gerenciar melhor esses dados, como por exemplo um fornecedor de proteção de dados.

A tecnologia facilitou a violação de dados e sua transferência para as mãos erradas. A privacidade de dados é importante para as informações pessoais, e mais ainda para categorias especiais de dados pessoais, incluindo:

a) CPFs
b) Histórico médico
c) Origem étnico-racial
d) Crenças religiosas ou filosóficas
e) Opiniões políticas
f) Associação a sindicatos
g) Dados biométricos usados para identificar um indivíduo
h) Dados genéricos
i) Dados de saúde
j) Dados relacionados a preferências sexuais, vida sexual e/ou orientação sexual

Com dados pessoais sendo coletados em uma taxa cada vez maior, e com os saltos na tecnologia usado para alavancá-lo, não é de se estranhar que os estados, países e blocos comerciais procurem aumentar a regulamentação nessa área. Atualmente, há muito mais discussões sobre a Lei de Proteção de Dados Pessoais no Brasil.

9.2. Ciclo de vida do tratamento de dados pessoais

O tratamento de dados pessoais de pessoas naturais (físicas) é baseado em um ciclo de vida que se inicia com a coleta do dado e que determina a “vida” (existência) do dado pessoal durante um período, de acordo com certos critérios de eliminação.

Para orientar a prática do tratamento, o controlador divide o ciclo de vida do tratamento dos dados pessoais em 5 (cinco) fases: coleta, retenção, processamento, compartilhamento e eliminação.

9.2.1. Fases do ciclo de vida do tratamento de dados pessoais

O ciclo de vida do tratamento do dado pessoal tem início com a coleta deste e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento claramente definidas (figura 8).

a) A fase “coleta” refere-se à coleta, produção, recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.);

b) A “retenção” corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.);

c) O “processamento” é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador;

d) O “compartilhamento”, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhamento de dados pessoais;

e) A “eliminação” é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, bem como eliminação de documentos eletrônicos ou em papel em que constam dados pessoais. Esta fase também contempla o descarte dos ativos organizacionais (documentos, equipamentos etc.) nos casos necessários ao negócio da instituição.

Figura 10: Ciclo de vida do tratamento de dados pessoais

As fases do ciclo de vida do tratamento de dados pessoais encontram correlação com as operações de tratamento previstas na LGPD (tabela 2).

Fases do ciclo de tratamento	Operações de tratamento
Coleta	Coleta, produção, recepção, acesso.
Retenção	Arquivamento, armazenamento e acesso,

Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração, modificação e acesso.
Compartilhamento	Transmissão, distribuição, comunicação, transferência, difusão e acesso.
Eliminação	Acesso e eliminação.

Tabela 2: Relacionamento das fases do ciclo de vida x operações de tratamento de dados pessoais

9.3. A Lei Geral de Proteção de Dados (LGPD)

A Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios, prevalecendo, portanto, sobre quaisquer outras leis municipais ou estaduais.

A (LGPD), sancionada em 14/08/2018, entrou em vigor em 18/09/2020 após inúmeras discussões normativas nos Poderes Executivo e Legislativo. As infrações e sanções administrativas, de acordo com a Lei 14.010/2020, só passam a valer a partir de 01/08/2021. Esta Lei representa o primeiro regulamento geral sobre proteção de dados pessoais no Brasil, onde o tema era tratado apenas por leis específicas, como o Código Brasileiro de Defesa do Consumidor (Lei 8.078/1990) e a Lei Brasileira da Internet (Lei 12.965/2014).

A LGPD oferece aos indivíduos maior controle sobre seus dados pessoais, garantindo maior transparência sobre a utilização dos dados e exige maior segurança e controles de proteção de dados.

Diferentemente das leis de privacidade em algumas jurisdições, a LGPD é aplicável às organizações de todos os tamanhos e em todos os setores e foi inspirada no GDPR

(*General Data Protection Regulation*) ou Regulamento Geral de Proteção de Dados europeu, que é geralmente visto internacionalmente como um modelo em questões de privacidade, portanto, há de se esperar que as interpretações e desenvolvimentos no GDPR influenciem diretamente a obrigatoriedade da LGPD no decorrer do tempo.

A LGPD foi construída com base em determinadas premissas e tendo como fundamentos:

I. o respeito à privacidade (direito à reserva de informações pessoais);
II. a autodeterminação informativa (o cidadão é soberano sobre suas próprias informações pessoais e deve ser o protagonista de quaisquer temas relacionados ao tratamento de seus dados);
III. a liberdade de expressão, de informação, de comunicação e de opinião (previstos na CF 88);
IV. a inviolabilidade da intimidade, da honra e da imagem (preservação de direitos do cidadão);
V. o desenvolvimento econômico e tecnológico e a inovação (não prejudicam as atividades das empresas que realizam tratamento de dados);
VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por 2 (dois) "agentes de tratamento": o Controlador e o Operador:

- O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da organização, o controlador é representado pelo corpo diretivo da instituição, imbuído de adotar as decisões acerca do tratamento de tais dados.
- O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. No contexto da organização, os operadores são os colaboradores, ou mesmo, parceiros de negócio (fornecedores), pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Considera-se “tratamento de dados” pessoais, qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essas operações de tratamento são destacadas a seguir:

1. COLETA - recolhimento de dados com finalidade específica;
2. PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados;
3. RECEPÇÃO - ato de receber os dados ao final da transmissão;
4. CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;
5. UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados;
6. ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
7. REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo;
8. TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;
9. DISTRIBUIÇÃO - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
10. PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
11. ARQUIVAMENTO - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência;
12. ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;
13. ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório;
14. AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;
15. CONTROLE - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
16. MODIFICAÇÃO - ato ou efeito de alteração do dado;
17. COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;

18. TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
19. DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados;
20. EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava.

Há de se observar que as disposições da LGPD não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

I. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II. Realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os artigos 7º e 11 da LGPD);
III. Realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou;
IV. Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

A LGPD previu expressamente, 10 (dez) hipóteses de tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais. Estas hipóteses são:

I. Mediante o fornecimento de consentimento pelo titular;
II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD;
IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O tratamento de dados pessoais, pelo controlador, considerará as hipóteses de tratamento descritas acima, bem como observará a boa-fé e os demais princípios estabelecidos no ordenamento jurídico:

a) Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. O tratamento posterior somente será possível se for compatível com esses propósitos e finalidades. No caso da organização, a finalidade relaciona-se com a execução de suas atividades cotidianas vinculadas com a sua atividade fim, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória;

b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

g) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
i) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
j) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A LGPD traz regramento específico para o tratamento de dados pessoais sensíveis, que são definidos como "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*.".

São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida. O tratamento mediante consentimento exige que se registre a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento.

9.3.1. Relatório de Impacto a Proteção de Dados (RIPD)

A Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

A LGPD estabelece que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

O RIPD deverá conter, no mínimo: a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

9.3.2. Término do tratamento de dados

Conforme estabelece a LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses: (i) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade; (ii) fim do período de tratamento; (iii) revogação do consentimento ou a pedido do titular; (iv) determinação da autoridade nacional em face de violação de dispositivo legal.

9.3.3. Segurança da informação

Os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais. A proteção dos dados pessoais será alcançada por meio de medidas de segurança, técnicas e administrativas, que deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, algo previsto no conceito fundamental para a proteção da privacidade dos dados pessoais denominado Privacidade desde a Concepção (do inglês *Privacy by Design*).

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo.