AUDITORIA DE SISTEMAS

AULA 5

Prof. André Roberto Guerra

CONVERSA INICIAL

Como sensibilizar e capilarizar na organização questões de ética e práticas administrativas/financeiras/relacionamento politicamente corretas? Com a correta implantação de um programa de *compliance* e a seleção de um profissional preparado para ocupar a função de CO (*Compliance Officer* = Profissional de *Compliance*). Também é possível a contratação de parcerias que assumem a função remotamente e regularmente desenvolvam as ações de treinamento, monitoramento constante e investigações rápidas.

> Auditorias forçadas e exigência para implantação de Programa de *Compliance* são medidas comuns nos casos comprovados de corrupção, fraudes, formação de cartel e outros crimes corporativos. Antes aplicadas quase que exclusivamente nos EUA, a globalização dos crimes levou estas medidas para a Europa e Américas, bem como Oceania e nos principais países asiáticos.

A utilização de normas/controles para os sistemas de informação é facilitada pela existência de normas e padrões (*standards*) internacionais de SI que incorporam modelos estruturados (*frameworks*) e que são referenciais para a gestão e a auditoria de sistemas de informação.

TEMA 1 – COMPLIANCE

> Estar em Conformidade (*to Comply*, em inglês) interna e externamente traz uma série de benefícios imediatos para uma organização. Destaca a empresa nos ambientes comerciais e sociais como séria e responsável do chão de fábrica a mais alta esfera executiva, trazendo consumidores cada vez mais atentos. (Mercadológica, 2017)

Também oportuniza vantagens competitivas que se juntam à credibilidade, permitindo acessos a linhas de crédito antes restritas, valoriza o clima de confiança interno e certamente um melhor retorno de investimentos.

Implantar um programa de *compliance* é investimento.

1.1 Procedimentos para implantação de programa de *compliance*

- Fixação de padrões de conduta, código de ética e políticas internas e externas de relacionamentos críticos.

- Gestão de riscos, paralelamente aos procedimentos de auditoria e acompanhamento gerenciais, com transparência e respostas ágeis e efetivas em casos identificados de desvios dos padrões fixados.
- Melhoria contínua de processos, monitoria do programa e treinamentos frequentes.
- A integridade corporativa é essencial para a proteção dos investidores, colaboradores, parceiros comerciais e para a redução de danos causados por fraudes e corrupção.

1.2 ISO 37001 – Norma certificável de programas de *compliance*

Independentemente de tipo, tamanho e natureza da atividade, seja do setor público, privado ou sem fins lucrativos, os requisitos da ISO 37001 podem ser aplicáveis a qualquer organização. Seu principal objetivo é apoiar as organizações a combaterem o suborno por meio de uma cultura de integridade, transparência e conformidade com as leis e regulamentações aplicáveis, com os requisitos definidos pela ISO 37001 e pela própria organização por meio de políticas, procedimentos e controles adequados para gerenciar os riscos relativos ao suborno.

O que antes era um diferencial agora é requisito competitivo essencial para empresas sensíveis ou que operam com o sistema público por meio de licitações ou agências reguladoras.

TEMA 2 – NORMAS, GUIAS E PROCEDIMENTOS

As organizações podem exercer a Governança dos SI (*IT Governance*) por abordagem local (*ad-hoc*), com a criação dos seus próprios referenciais, baseados na experiência da organização, ou utilizar normas internacionais desenvolvidas e aperfeiçoadas, recorrendo à experiência acumulada de um grupo de organizações e de profissionais da vanguarda de SI.

A utilização dessas normas internacionais é apresentada e defendida por Spafford (2003) como a mais adequada, pois tem as seguintes características e benefícios:

> **Já existem** - Não há vantagens em investir tempo e esforço no desenvolvimento de um referencial próprio baseado na experiência e no conhecimento limitado de uma organização quando existem normas internacionais disponíveis.

> **São estruturados** - As normas internacionais de SI incorporam modelos estruturados que facilitam a compreensão e utilização das normas pelas organizações, permitindo assim que todas as partes interessadas nos SI (*stakeholders*) tenham uma referência em comum para saber o que podem esperar dos SI.
> **Incorporam as melhores práticas** - As normas estão em constante atualização, são construídas e melhoradas progressivamente ao longo dos anos, avaliadas por inúmeras organizações e profissionais de SI, validando esta experiência acumulada em melhores práticas.
> **Permitem o compartilhamento de conhecimento** - Adotando normas globalmente aceitas para os SI, as organizações se beneficiam do compartilhamento de conhecimento e de ideias (exemplos: grupos de usuários, websites, revistas, livros, etc.), o que não ocorre individualmente em uma organização.
> **São auditáveis** - A missão da Auditoria de SI é facilitada com a utilização de normas de Gestão de SI. Os Auditores de SI também devem utilizá-las em substituição das práticas *ad-hoc* de Auditoria. Os Sistemas de Informação da organização deverão ser auditados por comparação com pelo menos uma norma internacionalmente aceita, além das recomendações da norma adotada e de outras normas complementares. (Spafford, 2003)

Essas características e esses benefícios apresentados induzem ao questionamento: qual é o melhor referencial para a gestão e para a auditoria de SI?

O mesmo autor citado na descrição das características e benefícios (Spafford, 2003) argumenta que não existe uma resposta predeterminada para a questão.

Mais do que selecionar um referencial, as organizações devem analisar e comparar os diversos referenciais de SI existentes, para planejar a implementação de um modelo que combine/integre as melhores práticas, garantindo aderência e compatibilidade com as necessidades da organização. Portanto, não se deve apenas adotar normas/padrões, mas também adaptá-las e integrá-las em referencial útil para a organização. Compete aos profissionais de SI o modo correto de fazer a adaptação.

Para a correta adaptação das normas, deve-se garantir que elas incorporem, pelo menos, um conjunto mínimo de princípios de governança dos SI, que, segundo ITGI & OGC (2005), passam por:

> **Alinhamento Estratégico** - Alinhar as normas com foco no negócio e em soluções colaborativas.
> **Acréscimo de Valor** - Acrescentar valor à organização através de normas centradas na redução de custos e na valorização dos SI.
> **Gestão do Risco** - Gerir os riscos com impacto nos SI (em uso ou ainda em projeto), através de normas que contemplam a salvaguarda dos ativos de SI, bem como a recuperação de desastres e a continuidade de negócio.
> **Gestão dos Recursos** - Gerir os recursos de SI através de normas que promovam a otimização do conhecimento (recursos humanos) e da infraestrutura (recursos físicos).

> **Medição do Desempenho** - Medir o desempenho dos SI através de normas que permitam controlar os projetos de SI e monitorar a prestação dos serviços de SI. (ITGI & OGC, 2005)

Constatados por meio destes princípios resumidos por ITGI & OGC (2005), os referenciais de SI deverão garantir alinhamento com o negócio e com a Governança Corporativa (*Corporate Governance*), além dos requisitos técnicos considerados. A utilização de referenciais deverá permitir a definição das responsabilidades (*accountability*) e dos níveis de decisão (*decision rights*) para os SI.

Para ilustrar uma possível utilização dos referenciais, LeBlanc (2004) sugere a utilização dos conceitos do método *Six Sigma*. Este é um método estatístico de melhoria da qualidade dos processos, desenvolvido pelo grupo Motorola, baseado numa visão de serviço ao cliente. O método prevê 5 principais fases:

1. Definição (*Define*);
2. Medição (*Measure*);
3. Análise (*Analyse*);
4. Melhoria (*Improve*); e
5. Controle (*Control*).

Nesse contexto de melhoria contínua, LeBlanc (2004) propõe esquema que relaciona três dos referenciais metodológicos.

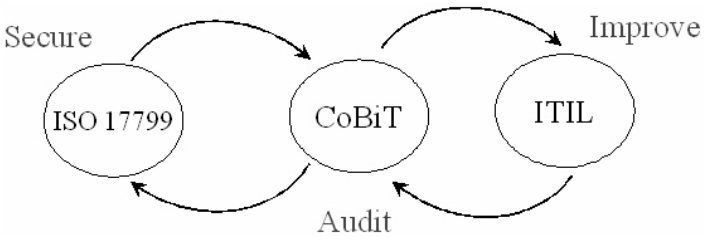
Inicialmente, na fase de Definição (*Define*), os SI devem ser seguros (*Secure*), condição-base para prestação de serviços de SI. Nas fases seguintes, na prestação dos serviços de SI aos clientes, deve ser executada a medição (*Measure*) e a análise (*Analyse*) dos dados relativos à qualidade dos serviços. Estas duas atividades devem ser efetuadas periodicamente no âmbito de uma auditoria (*Audit*) ou serem atividades já habituais no processo de prestação do serviço. Na fase seguinte, após a interpretação desses dados, devem ser identificadas medidas para melhoria (*Improve*) dos serviços.

O ciclo recomeça no sentido inverso, na fase de controle (*Control*), em que se deverá controlar utilizando da auditoria (*Audit*) as melhorias implementadas. Na sequência, efetuar a definição (*Define*) de novas medidas de segurança que melhorem a qualidade dos serviços de SI.

LeBlanc (2004) defende que “o referencial metodológico de SI mais adequado para as medidas de Segurança (*Secure*) é a ISO 17799, para a

Auditoria (*Audit*) é o CobiT e para a Melhoria (*Improve*) é o ITIL". Esses três referenciais metodológicos são apresentados/definidos individualmente nos temas seguintes.

Figura 1 – Três referenciais metodológicos integrados



Fonte: LeBlanc (2004).

Esses três referenciais selecionados (CobiT, ITIL e ISO 17799) são "os mais mencionados pela literatura que aborda a Auditoria de SI e são também os utilizados de forma mais comum pelos profissionais de SI a nível internacional".

Na tabela seguinte, são apresentados e comparados os três referenciais.

Tabela 1 – Comparativo entre CobiT, ITIL e ISO 17799

	CobiT	**ITIL**	**ISO 17799**
Nome	▪ *Control Objectives for Information and related Technology*	▪ *The Information Technology Infrastructure Library*	▪ *ISO 17799 Information Technology - Code of Practice for Information Security Management*
Entidade Responsável	▪ *IT Governance Institute / ISACA - Information Systems Audit and Control Association (USA)*	▪ *OGC – The Office of Government Commerce (UK)*	▪ *ISO - International Organizational for Standardization & IEC - International Electrotechnical Comission (Joint Technical Committee ISO/IEC JTC 1) (Switzerland)*
Primeira versão	▪ CobiT *1st Edition* (1996)	▪ ITIL v1 Library (1988)	▪ ISO/IEC 17799:2000
Última versão	▪ CobiT *4th Edition* (2005)	▪ ITIL v3 Library (2007)	▪ ISO/IEC 17799:2005
Versão analisada	▪ **CobiT *3rd Edition* (2000)**	▪ **ITIL *v2 Library* (1999)**	▪ **ISO/IEC 17799:2000**
Relacionados / Antecedentes / Subsequentes	▪ Em 1997 são lançados os *SISAS - Statements on Information Systems Auditing Standards* que definem o modo como os Auditores de SI devem executar as Auditorias de SI. ▪ Com o mesmo propósito, e substituindo todos os anteriores, em 2005 são lançados os *IS Standards, Guidelines and Procedures for Auditing and Control Professionals.*	▪ Com a contribuição do itSMF (*Information Technology Service Managment Forum*), a partir de 2000 o ITIL passou a ser considerado como a melhor prática para as organizações conseguirem a certificação na *British Standard for IT Service Management* (BS 15000): *- Part 1 : Specification for Service Management* *- Part 2 : Code of Practice for Service Management* ▪ Espera-se que a BS 15000 se transforme definitivamente no standard ISO/IEC 20000.	▪ Teve origem em 1993numa *British Standard* (BS 7799), da qual existiram duas partes: *- Part 1 : Information Technology – Code of Practice for Information Security Management* *- Part 2 : Information Security Management Systems – Specification with Guidance for Use* ▪ *Part* 1 transformou-se na ISO 17799 em 2000 e a *Part* 2 na ISO 27001 em 2005. ▪ Durante 2007 a ISO/IEC 17799:2005 (*Part* 1) passará a ISO/IEC 27002, inserida na nova série de standards ISO/IEC 2700x dedicada à Segurança.
Génese	▪ Auditar os processos de SI	▪ Organizar e estruturar as áreas dos SI	▪ Garantir a segurança da informação
Objectivo	▪ Governo dos SI	▪ Gestão de Serviços de SI	▪ Gestão da Segurança da Informação
Foco	▪ Alinhamento dos SI com o Negócio	▪ Qualidade dos Serviços de SI	▪ Segurança da Informação
Visão	▪ Visão de gestão dos processos de SI	▪ Visão operacional dos serviços de SI	▪ Visão sistémica da informação
Conveniência	▪ Orientador, integrador, controlador	▪ Auxiliador, estruturador, aperfeiçoador	▪ Basilar, protector

Fonte: Silva (2007).

TEMA 3 – COBIT

Pela análise dos três referenciais apresentados na Tabela 1, pode-se concluir que o CobiT, de modo geral e salvas as situações específicas, será aplicado (preferencialmente) na auditoria de SI. São apresentadas a seguir algumas razões que fundamentam essa conclusão.

- Desde a criação, o CobiT tem foco na criação de um referencial para auditar os processos de SI. O ITIL teve origem não tão abrangente (a organização e a estruturação das áreas de SI), enquanto a ISO 17799 nasceu especializado apenas na segurança da informação.
- A entidade responsável pela elaboração do CobiT é uma Associação de Auditores de SI (ISACA – *Information Systems Audit and Control Association*), o que não acontece com os outros dois referenciais.
- O CobiT possui uma visão de gestão dos processos de SI e privilegia o alinhamento destes com o negócio, fatores importantes para a auditoria de SI. O ITIL também considera o alinhamento com o negócio, contudo, focado na qualidade dos serviços de SI, e possui uma visão mais operacional, fatores que o tornam mais adequado para auditoria de SI quando os objetos da auditoria forem serviços, e não processos de SI abrangentes. O ISO 17799 será o referencial mais adequado nos casos de auditoria à informação e à sua segurança nos SI, uma vez que possui uma visão sistêmica da informação.
- O CobiT é útil para as organizações enquanto instrumento orientador e integrador de controles de SI em todos os níveis de governança dos SI e também será um referencial sobre o qual todos os tipos controles de SI poderão ser auditados. O ITIL poderá ser um referencial adequado para auditar os processos de gestão de serviços de SI e o ISO 17799 para auditar os procedimentos básicos de gestão da segurança da informação.
- Como consequência, os destinatários privilegiados do CobiT são os auditores de SI, sendo também utilizado pelos gestores de topo e gestores de SI. Nos casos do ITIL e do ISO 17799, a utilização pelos auditores de SI deve ser favorecida apenas nas situações anteriormente indicadas, uma vez que estes dois referenciais são mais adequados para utilização pelos gestores de serviços de SI e pelos gestores da segurança da informação, respectivamente.

A principal premissa do CobiT é a orientação para o negócio, ou seja, todos os processos de SI devem estar alinhados com a governança dos SI, que, por sua vez, deverá estar alinhada com os objetivos de negócio.

Este modelo estruturado considera 5 tipos de recursos de SI (as pessoas, os aplicativos, a tecnologia, as instalações e os dados), que, em conjunto, possibilitam a produção e o suporte da informação da empresa, considerando 7 princípios essenciais (eficácia, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade).

Para gerar as informações que o negócio necessita para atingir os seus objetivos, os recursos de SI são administrados por processos de SI. Cada um desses processos deverá possuir controles de SI subjacentes.

O referencial CobiT considera os controles de SI agrupados em 4 grandes domínios que trabalham em conjunto, de forma cíclica, para uma organização bem suportada em termos de SI, otimizada com base nas prioridades e nos recursos da organização. Os 4 domínios são:

- Planejar e Organizar (PO – *Plan and Organize*);
- Adquirir e Implementar (AI – *Acquire and Implement*);
- Produzir e Suportar (DS – *Deliver and Support*);
- Monitorar e Avaliar (M – *Monitor and Evaluate*).

Cada um desses 4 domínios é constituído por um conjunto de processos de SI (34 no total) que correspondem a objetivos de controle de alto nível. Por sua vez, esses processos são constituídos por atividades de SI (318 no total) que correspondem a objetivos de controle detalhados.

TEMA 4 – ITIL

ITIL® (*Information Technology Infrastructure Library*) "é o *framework* para gerenciamento de serviços de TI mais adotado mundialmente. A utilização das melhores práticas contidas na **ITIL V3** (versão atual) ajuda as organizações a atingirem seus objetivos de negócio utilizando apropriadamente os serviços TI".

A ITIL® foi desenvolvida no final dos anos 80 pelo governo britânico, primeiramente como CCTA (*Central Computer and Telecommunications Agency*) e posteriormente pela OGC (*Office of Government Commerce*), com base na necessidade do governo de ter seus processos organizados na área de TI. O resultado foi a junção dos melhores processos e práticas para ancorar a

gestão dos serviços de TI. Foram levadas em conta as experiências acumuladas por organizações públicas e privadas de diversos países.

Durante a década de 90, várias organizações europeias privadas passaram a adotar essas melhores práticas, o que acabou popularizando as publicações. Hoje, já na versão 3, a ITIL é uma marca mantida pela empresa Alexos, uma joint venture entre a UK Cabinet Office e a Capita, uma empresa especializada em gestão de processos de negócio.

O referencial ITIL toma como ponto de partida, não só a tecnologia existente, mas também as necessidades do negócio no nível de Serviços de SI. O ITIL centra-se fundamentalmente na Gestão dos Serviços de SI que tem como objetivos a produção (*delivery*) e o suporte (*support*) dos Serviços de SI que sejam adequados aos requisitos da organização.

O ITIL é considerado por grande parte dos Gestores de SI como sendo um conjunto coerente de melhores práticas (*guidelines*) para a Gestão de Serviços de SI e para a totalidade dos processos com eles relacionados (*end-to-end processes*). Privilegia as seguintes abordagens:

- promoção da qualidade dos Serviços de SI;
- visão holística da Gestão dos Serviços de SI;
- orientação para o negócio (cliente/usuário); e
- uso eficaz/eficiente dos SI.

Os 2 módulos centrais (*core*) do modelo estruturado e respectivos processos são:

- Suporte aos Serviços (Service Support)
  - ✓ Gestão de Incidentes (*Incident Management*);
  - ✓ Gestão de Problemas (*Problem Management*);
  - ✓ Gestão de Configurações (*Configuration Management*);
  - ✓ Gestão de Alterações (*Change Management*);
  - ✓ Gestão de Versões (*Release Management*);
  - ✓ Apoio aos Serviços (*Service Desk*).
- Produção dos Serviços (Service Delivery)
  - ✓ Gestão de Capacidade (Capacity Management);
  - ✓ Gestão de Disponibilidade (Availability Management);
  - ✓ Gestão de Níveis de Serviço (Service Level Management);
  - ✓ Gestão de Continuidade de Serviços (IT Service Continuity Management);
  - ✓ Gestão Financeira dos Serviços (Financial Management for IT Services).

Os 5 módulos complementares do ITIL são mais latos, pois para além da Gestão dos Serviços de SI, abordam aspectos relacionados com a definição e o desenvolvimento de processos eficazes de SI. Os temas tratados pelos seus respectivos processos são os seguintes:

- Gestão da Infraestrutura de TIC (ICT Infrastructure Management) - É muito abrangente em termos de processos de gestão das tecnologias (arquitetura e planejamento, produção, operação, suporte técnico, etc.).
- Gestão de Aplicações (Application Management) - Inclui processos de desenvolvimento de software usando uma perspectiva de ciclo de vida de desenvolvimento, com foco na rigorosa definição dos requisitos aplicacionais em função das necessidades do negócio.
- Gestão da Segurança (Security Management) - Aborda os processos de planeamento, de gestão e de resposta a incidentes relativos aos níveis de segurança da informação e das TIC.
- Planejamento da Implementação da Gestão dos Serviços (Planning to Implement Service Management) - Prevê os processos essenciais no planeamento e na implementação da Gestão de Serviços de SI.

- A Perspectiva de Negócio (The Business Perspective) - Aborda os processos de relacionamento e de comunicação da Gestão dos SI com o negócio, incluindo a restante organização e entidades externas. (Mundoitil, 2017)

TEMA 5 – NORMA ISO 17799

Norma é aquilo que “se estabelece como medida para a realização de uma atividade. Uma norma tem como propósito definir regras e instrumentos de controle para assegurar a conformidade de um processo ou serviço” (Fagundes, 2013).

Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT, 2005), os objetivos da normalização são:

- **Comunicação**: proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente, melhorando a confiabilidade das relações comerciais e de serviços;
- **Segurança**: proteger a vida humana e a saúde;
- **Proteção do consumidor**: prover a sociedade de mecanismos eficazes para aferir qualidade dos produtos;
- **Eliminação de barreiras técnicas e comerciais**: evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando assim o intercâmbio comercial. (ABNT, 2005)

No ano de 2000 a ABNT aceitou a norma ISO como padrão brasileiro, surgindo em 2001 a NBR 17799:2001 – Código de Prática para a Gestão da Segurança da Informação. Porém, em 2005 surgiu a norma ISO 27001, que é a BS7799-2:2002 revisada, com melhorias e adaptações contemplando o ciclo PDCA de melhorias e a visão de processos que as normas de sistemas de gestão já incorporaram (Caubit, 2006).

No mesmo ano, foi também aprovada e publicada pela ISO a norma ISO 27002. No Brasil, a ABNT publicou a sua equivalente como norma brasileira NBR ISO IEC 17799:2005. A ISO/IEC 27001 é a norma usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002.

A norma brasileira NBR ISO/IEC 17799:2005 é um guia prático “que estabelece diretrizes e princípios gerais para **iniciar**, **implementar**, **manter** e **melhorar a gestão** de segurança da informação em uma organização”.

Nesse sentido, a norma se subdivide em 16 capítulos:

1. Introdução,
2. Objetivo,
3. Termos e Definições,
4. Estrutura da Norma,
5. Análise/avaliação e tratamento de Riscos,

6. Política de Segurança da Informação,
7. Organizando a Segurança da Informação,
8. Gestão de Ativos,
9. Segurança em Recursos Humanos,
10. Segurança Física e do Ambiente,
11. Gerenciamento das Operações e Comunicações,
12. Controle de Acessos,
13. Aquisição, desenvolvimento e manutenção de Sistemas de Informação,
14. Gestão de Incidentes de Segurança da Informação,
15. Gestão da Continuidade do Negócio e
16. Conformidade

5.1 Evolução da Norma ISO/IEC 27002:2005

Essa norma teve origem em 1989, a fim de implementar e normalizar a atuação das empresas na gestão da segurança da informação,

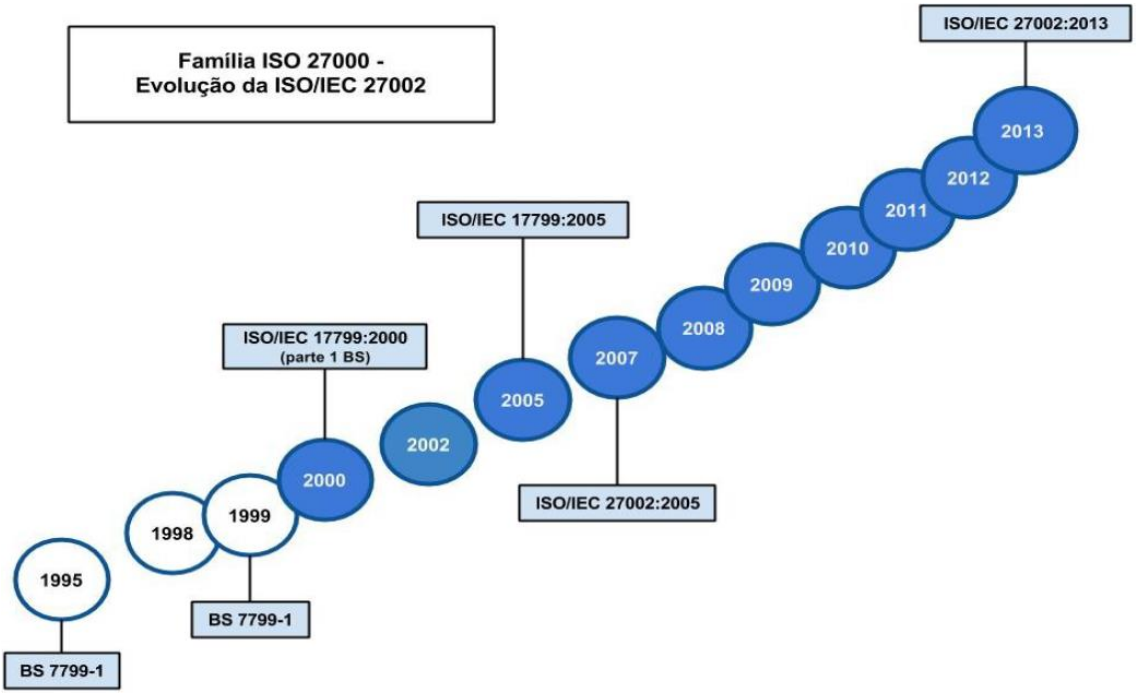
> O *Commercial Computer Security Center*, órgão ligado ao departamento de indústria e comércio do Reino Unido, publicou a primeira versão do Código para Gerenciamento de Segurança da Informação – PD0003. Seis anos depois, este código foi revisado e publicado como uma *British Standard*, denominado BS7799, que apresentava as melhores práticas em controles de segurança para auxiliar as organizações comerciais e de governo na implantação e crescimento da segurança da informação. (Oliva e Oliveira, 2003).

Devido ao interesse internacional em uma norma de segurança da informação, a BS 7799-1:1999 foi submetida à *International Organization for Standardization* (ISO), organização internacional que aglomera os grêmios de padronização/normalização de 148 países. Em dezembro de 2000, a BS 7799-1:1999 foi publicada como norma internacional ISO 17799:2000.

Em 2001, a Associação Brasileira de Normas Técnicas – ABNT publicou a versão brasileira da ISO 17799:2000, que ficou “com a denominação de NBR/ISO 17799 – Código de Prática para a Gestão da Segurança da Informação. Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005”.

As séries de normas ISO 27000 foram especificamente reservadas pela ISO para as questões de segurança da informação. Pode-se observar pela Figura 2 essa evolução.

Figura 2 – Evolução da norma ISO 17799/27002



Fonte: Friedrich, 2014

> Em 2007, a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração ISO/IEC 27002 (ABNT, 2005). No dia 18 de novembro de 2013 foi lançada a nova versão ABNT NBR ISO/IEC 27002:2013 – Código de Prática para controles de Segurança da informação. A atualização da norma reflete a evolução de práticas de gestão e governança de segurança da informação nos últimos oito anos (RNP, 2013).

Salienta-se que,

> [...] para uma organização obter a certificação, que significa que um organismo de certificação independente confirmou que a segurança da informação está sendo implementada da melhor maneira possível na organização, depende da ISO 27001. A ISO 27002:2005 é uma norma "auxiliar" que fornece mais detalhes sobre como implementar os controles de segurança especificados na ISO 27001 (ABNT, 2005).

5.2 A Norma ABNT NBR ISO/IEC 27002

A norma ISO 27002:2005, nos primeiros capítulos, contêm objetivo, termos e definições, estrutura da norma e uma seção introdutória: “Essa seção introdutória trata da Análise, Avaliação e Tratamento de Riscos a fim de orientar na identificação, quantificação e priorização do gerenciamento do risco, e os critérios definidos para aceitar o risco ou não” (ABNT, 2005).

Nas demais seções da norma, contém 11 controles de segurança da informação, conforme a Tabela 2, e juntos totalizam 39 categorias principais de segurança.

Tabela 2 – Seções e suas respectivas quantidades de categorias

Capítulo	Título	Número subcapítulos
5	Política de segurança da Informação	1
6	Organizando a Segurança da Informação	2
7	Gestão de Ativos	2
8	Segurança em Recursos Humanos	3
9	Segurança Física e do Ambiente	2
10	Gestão de Operações e Comunicações	10
11	Controle de Acesso	7
12	Aquisição, Desenvolvimento e Manutenção de SI	6
13	Gestão de Incidentes de Segurança Informação Gestão	2
14	da Continuidade do Negócio	1
15	Conformidade	3

Os títulos de cada seção, com suas respectivas recomendações, são aqui descritos (ABNT, 2005):

- **Política de Segurança da Informação**: recomendações para a formalização de uma política. Contendo: diretrizes, princípios e regras que irão prover orientação e apoio para implantação e manutenção da segurança.
- **Organização da Segurança da Informação:** recomendações para o estabelecimento de uma estrutura de gestão para planejar e controlar a implementação da segurança da informação na organização.
- **Gestão de Ativos:** recomendações sobre a realização de inventário dos ativos informacionais e atribuição de responsabilidades pela manutenção dos controles necessários para protegê-los;
- **Segurança em Recursos Humanos:** recomendações para reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações;
- **Segurança Física e do Ambiente:** recomendações para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis ao negócio contra acesso não autorizado, dano ou interferência;
- **Gestão das Operações e Comunicações:** recomendações para garantir a operação correta e segura dos recursos de processamento de informações e proteger a integridade de serviços e informações;
- **Controle de Acesso:** recomendações para a monitoração e o controle do acesso a recursos computacionais, para protegê-los contra abusos internos e ataques externos;
- **Aquisição, Desenvolvimento e Manutenção de SI:** recomendações para o uso de controles de segurança em todas as etapas do ciclo de vida forçam que, com todos os esforços de TI, tudo seja implementado e mantido com a segurança em mente, usando controles de segurança em todas as etapas do processo;
- **Gestão de Incidentes da Segurança da Informação:** recomendações para notificação de fragilidades e eventos de segurança da informação, responsabilidades e procedimentos e coleta de evidências.
- **Gestão da Continuidade do Negócio:** recomendações para preparar a organização para neutralizar as interrupções às atividades comerciais e proteger os processos críticos em caso de ocorrência de falha ou desastre;

- **Conformidade:** recomendações para a preservação da conformidade com requisitos legais (tais como direitos autorais e direito à privacidade), com normas e diretrizes internas e com os requisitos técnicos de segurança. (ABNT, 2005)

5.3 Seções e controles da norma ABNT NBR ISO/IEC 27002:2005

A norma ABNT NBR ISO/IEC 27002 da versão 2005 encontra-se estruturada nas seguintes seções e seus respectivos controles. A Tabela 3 cita as seções de forma resumida, as categorias existentes e os controles principais que compõem essa estrutura.

Tabela 3 – Seções e controles da norma ABNT NBR ISO/IEC 27002:2005

5. Política de Segurança da Informação
5.1 Política de Segurança da Informação **Objetivo**: prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
6. Organização da Segurança da Informação
6.1 Infraestrutura da Segurança da Informação **Objetivo**: gerenciar a segurança de informação dentro da organização;
6.2 Partes Externas **Objetivo**: manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.
7. Gestão de Ativos
7.1 Responsabilidade pelos ativos **Objetivo**: alcançar e manter a proteção adequada dos ativos da organização.
7.2 Classificação da informação **Objetivo**: assegurar que a informação receba um nível adequado de proteção.
8. Segurança em Recursos Humanos
8.1 Antes da contratação **Objetivo**: assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordos com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos.
8.2 Durante a contratação **Objetivo**: assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, de suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.
8.3 Encerramento ou mudança da contratação **Objetivo**: assegurar que os funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.
9. Segurança Física e do Ambiente
9.1 Áreas seguras **Objetivo**: prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização.
9.2 Segurança de equipamentos **Objetivo**: impedir perdas, danos, furto ou comprometimento de ativos e interrupções das atividades da organização.
10. Gerenciamento das Operações e Comunicações
10.1 Procedimentos e responsabilidades operacionais **Objetivo**: garantir a operação segura e correta dos recursos de processamento da informação;
10.2 Gerenciamento de serviços terceirizados **Objetivo**: implementar e manter o nível apropriado de segurança da informação e entrega de serviços em consonância com acordos de entrega de serviços terceirizados.

10.3 Planejamento e aceitação dos sistemas **Objetivo**: minimizar o risco de falhas nos sistemas.
10.4 Proteção contra códigos maliciosos e códigos móveis **Objetivo**: proteger a integridade do software e da informação.
10.5 Cópias de segurança **Objetivo**: manter a integridade e disponibilidade da informação e dos recursos de processamento da informação.
10.6 Gerenciamento da segurança em redes **Objetivo**: garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.
10.7 Manuseio de mídias **Objetivo**: prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.
10.8 Troca de informações **Objetivo**: manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.
10.9 Serviços de comércio eletrônico **Objetivo**: garantir a segurança de serviços de comércio eletrônico e sua utilização segura.
10.10 Monitoramento **Objetivo**: detectar atividades não autorizadas de processamento da informação.
11. Controle de Acesso
11.1 Requisitos de negócio para controle de acesso **Objetivo**: controlar acesso à informação
11.2 Gerenciamento de acesso do usuário **Objetivo**: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação
11.3 Responsabilidade dos usuários **Objetivo**: prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação e dos recursos de processamento da informação.
11.4 Controle de acesso à rede **Objetivo**: prevenir acesso não autorizado aos serviços da rede.
11.5 Controle de acesso ao sistema operacional **Objetivo**: prevenir acesso não autorizado aos sistemas operacionais
11.6 Controle de acesso à aplicação e à informação **Objetivo**: prevenir acesso não autorizado à informação contida nos sistemas de aplicação.
11.7 Computação móvel e trabalho remoto **Objetivo**: garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.
12. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
12.1 Requisitos de segurança de sistemas de Informação **Objetivo**: garantir que segurança é parte integrante de sistemas de informação.
12.2 Processamento correto nas aplicações **Objetivo**: prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.
12.3 Controles criptográficos **Objetivo**: proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.
12.4 Segurança dos arquivos do sistema **Objetivo**: garantir a segurança de arquivos de sistema
12.5 Segurança em processos de desenvolvimento e de suporte **Objetivo**: manter a segurança de sistemas aplicativos e da informação.
12.6 Gestão de vulnerabilidades técnicas **Objetivo**: reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
13. Gestão de Incidentes de Segurança da Informação
13.1 Notificação de fragilidades e eventos de segurança da informação **Objetivo**: assegurar que um enfoque consistente e efetivo seja aplicado a gestão de incidentes da segurança da informação.
13.2 Gestão de incidentes de segurança da informação e melhorias

Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
14. Gestão da Continuidade do Negócio
14.1 Aspectos da gestão da continuidade do negócio, relativos à segurança da informação **Objetivo**: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
15. Conformidade
15.1 Conformidade com requisitos legais **Objetivo**: evita violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
15.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica **Objetivo**: garantir a conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.
15.3 Considerações quanto à auditoria de sistemas de informação **Objetivo**: maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.

FINALIZANDO

Conforme Caruso (1995), “a maioria das organizações direciona as atenções e investimentos em segurança apenas nos seus ativos tangíveis físicos e financeiros, mas dedicam pouca atenção e investimentos aos ativos de informação, considerados vitais na sociedade do conhecimento”.

Observa-se que, para implementar alguma norma, vários são os requisitos que a organização deve obedecer, como: comprometimento da equipe, investimentos de dirigentes e colaboradores de toda organização, desenvolvimento de projetos de segurança, mapeamento de ativos, estabelecimento de diretrizes e procedimentos, análise de riscos, análise de impactos, planos de continuidade, políticas de segurança, confecção de documentação e auditorias periódicas. Cada um desses requisitos demanda tempo, e cada organização deve estar ciente disso antes de iniciar um processo de implementação da norma.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

_____. **NBR ISO/IEC 27002:2013**. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 4 dez. 2017.

_____. NBR ISO 27005: **Tecnologia da Informação**: Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2006.

_____. NBR/ISO/IEC 17799. **Tecnologia da Informação:** código de prática para a gestão da segurança da informação**.** ABNT, 2005.

AICPA – AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS. Disponível em: <http:// www.aicpa.org>. Acesso em: 4 dez. 2017.

ATUALIZADAS as normas 27001 e 27002 – Técnicas de Segurança. **RNP – Rede Nacional de Pesquisas**. Disponível em: <http://esr.rnp.br/noticias/atualizadas-as-normas-27001-e-27002-tecnicas-de-seguranca>. Acesso em: 4 dez. 2017.

BRANDALISE. M. M. T. **Roteiro para elaboração de programas de auditoria em sistema**. 102 f. Trabalho de conclusão de curso (Bacharelado em Sistema de Informação) – Universidade de Caxias do Sul. Caxias do Sul, 2012. Disponível em: <https://repositorio.ucs.br/xmlui/bitstream/handle/11338/1228/TCC%20Mauricio%20Modesto%20Toscan%20Brandalise.pdf?sequence=1&isAllowed=y>. Acesso em: 22 jan. 2018.

CARUSO, C. A. **A segurança em microinformática e em redes locais**. São Paulo: LTC, 1995.

CAUBIT, R. O que é a ISO 27001, afinal? **Modulo Security Magazine**, 19 jan. 2006. Disponível em: <www.modulo.com.br>. Acesso em: 4 dez. 2017.

COSTA, J. C. B. **Controle Interno**: sugestão de implantação em uma empresa de corretagem de seguros. Disponível em: <http://brasilesco.la/m14692>. Acesso em: 4 dez. 2017.

FAGUNDES, L. L. de. **Aula 02 27k:** Normas para Gestão da Segurança da Informação. São Leopoldo: UNISINOS, Notas de aula. Disponível em: <professor.unisinos.br/llemes/Aula02/Aula02.pdf>. Acesso em: 4 dez. 2017.

FRIEDRICH, L. D. P. M. **Um sistema web para análise de gestão da segurança da informação segundo a Norma ABNT NBR ISO IEC 27002**. Trabalho de conclusão de curso; (Graduação em Redes de Computadores) – Universidade Federal de Santa Maria. Santa Maria, 2013.

GIL, A. L. **Auditoria de computadores**. São Paulo: Atlas, 1999.

IIA - The Institute of Internal Auditors. **GTAG – Global Technology Audit Guide:** Management of IT Auditing. The Institute of Internal Auditors, Florida, USA, 2006.

IMONIANA, J. O. **Auditoria de sistemas de informação**. 3. ed. São Paulo: Atlas, 2015.

ISACA – Information Systems Audit and Control Association. **COBIT 5**. Estados Unidos, 2015. Disponível em: <http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx>. Acesso em: 4 dez. 2017.

_____. **CISA Job Practice Areas**. Disponível em: <http://www.isaca.org>. Acesso em: 4 dez. 2017.

_____. **Glossary of Terms**. Disponível em: <http://www.isaca.org>. Acesso em: 4 dez. 2017.

IT SERVICE MANAGEMENT FORUM. **An Introductory Overview of ITIL**. Version 1.0.a itSMF: United Kingdom, 2004.

MICHAELIS. **Dicionário *online***. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 4 dez. 2017.

MUNDOITIL. Disponível em: <https://www.mundoitil.com.br >. Acesso em: 4 dez. 2017.

OLIVA, R. P.; OLIVEIRA, M. Elaboração, implantação e manutenção de política de segurança por empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799. **REUNA**, Belo Horizonte, v.16, n.4, p. 95-113, out.-dez. 2011. Disponível em: <http://revistas.una.br/index.php/reuna/article/view/405/454>. Acesso em: 22 jan. 2017.

PESQUISA Global de Segurança da Informação 2013. Disponível em: <http://www.pwc.com.br/pt_BR/br/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13.pdf >. Acesso em: 4 dez. 2017.

SILVA, P. M. G. **A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências**. 193 f. Dissertação (Mestrado em Tecnologias e Sistemas de Informação) – Universidade do Minho. Braga, 2007. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/8058/1/Pedro%20Gomes%20Silva_A%20Funcao%20Auditoria%20de%20SI.pdf>. Disponível em: 22 jan. 2018.

VERBETES: Compliance. **Mercadológica C. M.** Disponível em: <http://www.mercadologicacm.com.br/html/verbetes.html#compliance>. Acesso em: 4 dez. 2017.