Senado Federal
Instituto Legislativo Brasileiro - ILB

HELIO MARÇOLA JUNIOR

ESTRUTURAÇÃO DE ESCRITÓRIO SETORIAL DE SEGURANÇA E RISCOS DE INFORMAÇÃO EM TI COM O COBIT 5 FOR INFORMATION SECURITY

Brasília - 2014

HELIO MARÇOLA JUNIOR

ESTRUTURAÇÃO DE ESCRITÓRIO SETORIAL DE SEGURANÇA E RISCOS DE INFORMAÇÃO EM TI COM O "COBIT 5 FOR INFORMATION SECURITY"

Trabalho final apresentado para aprovação no Curso de Pós-Graduação *Lato Sensu* em Administração Legislativa, realizado pelo Instituto Legislativo Brasileiro (ILB) como requisito para obtenção do título de especialista em Administração Legislativa.

Área de Concentração: Administração Legislativa (Gestão de processos)

Orientadora: Flávia Santinoni Vera

Brasília – 2014

HELIO MARÇOLA JUNIOR

ESTRUTURAÇÃO DE ESCRITÓRIO SETORIAL DE SEGURANÇA E RISCOS DE INFORMAÇÃO EM TI COM O "COBIT 5 FOR INFORMATION SECURITY"

Trabalho final apresentado ao Instituto Legislativo Brasileiro (ILB) como pré-requisito para obtenção do Certificado de Conclusão do Curso de Pós-Graduação *Lato Sensu* em Administração Legislativa.

Data de Aprovação:

Brasília, 10 de dezembro de 2014.

Banca Examinadora

_____

Flávia Santinoni Vera

_____

Renato Jorge Brown Ribeiro

AGRADECIMENTOS

Agradecimentos a todos que, de maneira direta e indireta, apoiando e contrapondo, contribuíram na elaboração deste trabalho, declinando de textualizar nomes para tentar evitar equívocos e esquecimentos, que poderiam mais transtornar os eventuais omitidos que lisonjear os mencionados.

Dedico a realização deste trabalho à minha família.

“O estudo em geral, a busca da verdade e da beleza são domínios em que nos é consentido ficar crianças toda a vida.”

(Albert Einstein)

RESUMO

Informação é elemento essencial no processo decisório e na formulação de estratégias de qualquer organização, e o processo de Gestão Estratégica da Informação deve ser ágil e inteligente para se ajustar à realidade de mudanças exponenciais da era da informação, buscando aumento de produtividade, minimização de dificuldades e riscos, e almejando os objetivos organizacionais pretendidos. Neste sentido, o presente trabalho apresenta as vantagens do modelo de governança e gestão da TI corporativa COBIT 5 (Control Objectives for Information and related Technology - COBIT® 5), divulgado em 2011 pela associação internacional ISACA (Information Systems Audit and Control Association - ISACA®). Ao estudar boas práticas reconhecidas pelo COBIT 5 for Information Security, este trabalho busca estabelecer um modelo de Escritório Setorial de Segurança e Riscos de Informação a ser implementado em área responsável pela tecnologia da informação (TI) no Senado Federal, com vistas a se avançar no planejamento e na especificação da gestão de riscos e segurança em TI, o que inclui avaliar impactos, selecionar e priorizar processos, difundir conceitos e benefícios, bem como definir e homologar processos. A análise do material pesquisado indica este arcabouço, por meio dos seus princípios e facilitadores, como referência basilar para a implantação de práticas de segurança da informação no Senado Federal e propicia fonte motivacional e estruturante para a implantação de escritório setorial de segurança e riscos de informação em TI.

Palavras-chave: Segurança da Informação. Risco. Tecnologia da Informação. COBIT®. ISACA.

ABSTRACT

Information is essential in decision making processes and for the formulation of strategies of any organization. The process of Strategic Information Management must be quick and smart to fit the reality of exponential changes in the information age, to increase productivity, minimize difficulties and risks and seek desired organizational objectives. In this sense, this paper seeks to presents advantages of the governance and management model for enterprise IT COBIT 5 (Control Objectives for Information and related Technology - COBIT 5 for Information Security), released in 2011 by the International Association ISACA (Information Systems Audit and Control Association - ISACA®). By studying the best practices recognized by the COBIT 5 for Information Security, this study seeks to establish a model of a department for Security and Risk informational management to be implemented in the area responsible for information technology (IT) of the Federal Senate, seeking to progress in the planning and specification of risk management and IT security, which includes the assessment of impacts, the selection and the prioritizing of processes, the dissemination of concepts and benefits and the definition and approval of procedures. The Analysis of the present material indicates this framework, through its principles and facilitators, being a benchmark for the implementation of information security practices in the Federal Senate, providing the motivation and necessary structure for the implementation of a department for security and risk IT management.

Keywords: Information Security. Risk. Information Technology. COBIT. ISACA.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APO	Align, Plan and Organise
APS	Ato do 1ºSecretário
ATC	Ato da Comissão Diretora
BAI	Build, Acquire and Implement
BMIS	Business Model for Information Security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CGEIT®	Certified in the Governance of Enterprise IT®
CID	Confidencialidade, Integridade e Disponibilidade
CIO	Chief Information Officer
CISA®	Certified Information Systems Auditor®
CISM®	Certified Information Security Manager®
CISO	Chief Information Security Officer
CISSP	Certified Information System Security Professional
COBIT®	Control Objectives for Information and related Technology®
COO	Chief Operating Officer
CRISC	Certified in Risk and Information Systems Control
CRO	Chief Risk Officer
CTO	Chief Technology Officer
DSIC	Departamento de Segurança da Informação e Comunicações
DSS	Deliver, Service and Support
EDM	Evaluate, Direct and Monitor
ERM	Enterprise risk management
FISMA	Federal Information Security Management Act
GSI	Gabinete de Segurança Institucional
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IEC	International Electro technical Commission
IN	Instrução Normativa
ISACA®	Information Systems Audit and Control Association®
ISF	Information Security Forum
ISM	Information Security Manager

ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSC	Information Security Steering Committee
ITAF	IT Assurance Framework
ITIL	Information Technology Infrastructure Library
MEA	Monitor, Evaluate and Assess
MPOG	Ministério do Planejamento, Orçamento e Gestão
NIST	U.S. National Institute of Standards and Technology
OLA	Operating Level Agreement
PAM	Process Assessment Model
PBRM	planning, building, running and monitoring
PCI DSS	Payment Card Industry Data Security Standard
PR	Presidência da República
PSI	Política de Segurança da Informação
RACI	Responsible, Accountable, Consulted and Informed
RASF	Regulamento Administrativo do Senado Federal
RH	Recursos Humanos
SI	Sistemas de Informação
SLA	Service Level Agreement
SLTI	Secretaria de Logística e Tecnologia da Informação
TCU	Tribunal de Contas da União
TGF	Taking Governance Forward
TI	Tecnologia da Informação

SUMÁRIO

INTRODUÇÃO

Pode-se aceitar que organizações objetivam trazer retornos, os mais diversos, para partes interessadas (*stakeholders* em inglês), equilibrando benefícios, riscos e recursos.

Com efeito, riscos são inerentes ao “negócio”, independentemente da natureza do empreendimento. Assim, há riscos referentes ao potencial cumprimento da missão institucional, mesmo para o Senado Federal. Portanto, reduzir riscos organizacionais é permanente desafio, considerando a evolução contínua de ameaças.

Saliente-se ainda que informação, durante todo o seu ciclo de vida, seja fator crítico empresarial. Por conseguinte, tecnologia da informação (TI) tem função primordial nas corporações hodiernas.

Na verdade, qualidade e proteção das informações, objetivando suas confidencialidade, integridade e disponibilidade, têm papel significativo essencial para o dia-a-dia organizacional.

Portanto, prejuízo na segurança da informação pode causar impacto negativo na corporação trazendo perdas financeiras e / ou operacionais. Ademais, o empreendimento atingido potencializa exposição a choques externos de reputação e / ou legais, danificando relações com cliente ou funcionário, ou mesmo colocando em perigo a sobrevivência da organização.

Considera-se que estruturação do setor de segurança e risco de informações pode ajudar na constituição de outras iniciativas no domínio da proteção como prática generalizada nas ações empreendidas.

O Control Objectives for Information and related Technology (COBIT®) 5 é modelo de governança e gestão empresarial, lançado em 2011 pela Information Systems Audit and Control Association (ISACA®). O COBIT 5 for Information Security, divulgado em 2012, se baseia nos mesmos princípios do COBIT 5.

Esta pesquisa poderá confirmar se o uso das diretrizes indicadas pelo “COBIT 5 for Information Security” pode facilitar implementação da segurança da informação na prática diária do órgão, e estruturação de Escritório Setorial de Segurança e Riscos de Informação em TI.

Este trabalho está organizado em seis partes, conforme descrito a seguir.

O Capítulo 1 apresenta base conceitual, concisa e contextualizada, sobre escritório setorial de segurança e riscos de informação em TI, com a motivação de seu estabelecimento, justificando-se a importância do assunto, sendo ainda constituído o objetivo geral do trabalho.

O Capítulo 2 descreve brevemente a instituição ISACA, o arcabouço COBIT e, mais especificamente, os conceitos envolvidos no COBIT 5 for Information Security.

O Capítulo 3 aborda a aplicabilidade do COBIT 5 for Information Security na estruturação do escritório setorial de segurança e riscos de informação, envolvendo o cenário de área responsável pela TI corporativa.

O Capítulo 4 aborda o estágio atual da segurança da informação no Senado Federal.

O Capítulo 5 estuda o uso do COBIT 5 for Information Security como facilitador da instituição do escritório setorial de segurança e riscos de informação em TI.

Em Considerações Finais, há a conclusão desta pesquisa e a apresentação de sugestões de potenciais trabalhos futuros a serem realizados para dar-lhe continuidade.

1 O ESCRITÓRIO SETORIAL DE SEGURANÇA E RISCOS DE INFORMAÇÃO EM TI

1.1 A SEGURANÇA E OS RISCOS DE INFORMAÇÃO

É realmente certo que empreendimentos existem para criar valor para seus *stakeholders*, isto é, para manter equilíbrio entre a realização de benefícios, a melhor condição de risco e o uso de recursos.

Os *stakeholders* são indivíduos ou entidades relevantes com interesses pertinentes à organização, que podem afetar, serem afetados, ou perceberem-se a ser afetados por atividade do empreendimento, ou ainda, pessoas ou organizações que assumam risco, direto ou indireto, em face da companhia, como acionistas, funcionários, clientes, fornecedores, credores e governos.

É preciso considerar que o risco é evento futuro identificado, ao qual é possível associar probabilidade de ocorrência:

> Quando investidores compram ações, cirurgiões realizam operações, engenheiros projetam pontes, empresários abrem seus negócios e políticos concorrem a cargos eletivos, o risco é um parceiro inevitável. Contudo, suas ações revelam que o risco não precisa ser hoje tão temido: administrá-lo tornou-se sinônimo de desafio e oportunidade. (Bernstein, 1996, p. VII)

De sorte que o Senado Federal, assim como outras instituições, está sujeito a riscos que podem comprometer a realização de seus objetivos, o serviço público prestado e até a sua reputação e imagem.

Assim, a necessidade de mitigar riscos corporativos está constantemente se intensificando e inclui a proteção de ativos contra ameaças sempre em mudança.

A informação é recurso corporativo fundamental desde sua criação até o momento em que é destruída. O avanço da TI tornou-a onipresente e com papel significativo nos ambientes organizacionais, sejam públicos, sociais ou privados.

As organizações e seus executivos se esforçam para:

- Manter a qualidade da informação para apoiar decisões de negócios;
- Gerar valor para o negócio pelos investimentos feitos em TI, ou seja, alcançar objetivos estratégicos e obter benefícios de negócios por meio da utilização eficaz e inovadora de TI;
- Alcançar a excelência operacional por meio da aplicação confiável e eficiente da tecnologia;
- Manter em nível aceitável os riscos relacionados a TI;
- Aperfeiçoar o custo de serviços e de tecnologia de TI.

Neste momento em que o significado da informação e das tecnologias afins está crescente em todos os aspectos dos negócios e da vida pública, a necessidade de mitigar o risco de informação está constantemente se intensificando, incluindo proteção de informações e de ativos de TI relacionados contra ameaças sempre em mudança.

Com efeito, a segurança da informação é essencial para as operações cotidianas corporativas, que devem garantir a confidencialidade e a integridade de suas informações, proporcionando disponibilidade a quem tenha razões legítimas para usá-las. Ela é facilitadora de negócios estritamente ligada à confiança dos *stakeholders*, tanto por abordar o risco do negócio como pela criação de valor para a corporação, tais como vantagem competitiva.

A melhoria das circunstâncias de risco é considerada muito relevante para a segurança da informação.

Eventual violação da segurança da informação pode levar a substancial impacto para a organização causando, por exemplo, danos financeiros ou operacionais. Além disso, o empreendimento pode ficar exposto a impactos externos, tais como risco lega ou de reputação, que podem prejudicar as relações com cliente ou funcionário, ou mesmo colocar em perigo a sobrevivência da entidade.

A necessidade de abordagens mais fortes, melhores e mais sistemáticas para a segurança da informação é ilustrada com os seguintes exemplos:

- A infraestrutura nacional crítica depende de sistemas de informação, e invasão bem-sucedida pode resultar em significativo impacto para a economia ou a segurança humana;
- A informação financeira não pública pode ser utilizada para ganho econômico;
- A divulgação de informação confidencial pode gerar constrangimento para corporações, causar danos à reputação ou prejudicar relações mercantis;
- A intrusão em rede de computadores, por exemplo, para a obtenção de dados relacionados com pagamento, pode levar a danos substanciais à reputação e a dano financeiro devido a multas;
- A evasão de inteligência nacional ou militar pode resultar em danos às relações políticas;
- O vazamento de dados pessoais pode resultar em perdas financeiras e esforços desnecessários para reconstruir a reputação financeira individual;
- A importância de custo não planejado, financeiro e/ou operacional, relacionado à contenção, à investigação e à remediação de infração de segurança, pode afetar empreendimento que tenha sofrido violação.

A crescente regulamentação dentro do cenário de negócios contribui para a conscientização do conselho de administração sobre a importância da segurança da informação para informação e ativos de TI relacionados.

1.2 O ESCRITÓRIO DE SEGURANÇA E RISCOS DE INFORMAÇÃO

A estruturação de Escritório Setorial de Segurança e Riscos de Informação em TI pode contribuir na coordenação da execução das demais ações de segurança na área de TI, e constituir pressuposto para que a segurança da informação seja difundida e os seus sejam aspectos abordados nas atividades e processos realizados.

Estabelecer Escritório Setorial de Gestão de Riscos e Segurança em TI contribui para:

- coordenar ações de aprimoramento da gestão de riscos e segurança em TI, bem como aperfeiçoamento de processos de trabalho;
- promover a vigilância proativa da perspectiva de riscos a que a organização está submetida, por exemplo, pelo uso de redes sociais e/ou dispositivos pessoais no local de trabalho, computação em nuvem e ofertas de serviços de TI;
- viabilizar diretrizes estratégicas, responsabilidades, competências e o apoio na implantação do sistema de gestão de risco e segurança em TI;
- integrar iniciativas relacionadas à gestão de risco e segurança em TI;
- aprimorar ganho de produtividade e eficiência de processos e gestão de risco e segurança em TI;
- facilitar avaliação de riscos e segurança em TI pelas unidades administrativas.

O Escritório Corporativo de Gestão de Segurança e Risco do Estado da Carolina do Norte (EUA) define como sua missão a liderança no desenvolvimento, no fornecimento e na manutenção de programa de segurança da informação e a gestão de riscos que proteja ativos de informação e infraestrutura de suporte do estado contra uso não autorizado, divulgação, modificação, perda ou dano. Além

disso, suporta programa estadual abrangente, que engloba implementação de segurança da informação, monitoramento, gerenciamento de vulnerabilidades e ameaças, gerenciamento de incidentes cibernéticos e gestão de continuidade de negócios corporativos.

Ele trabalha com agências do Poder Executivo para ajudá-lo a cumprir requisitos legais, regulamentares e de arquitetura técnica, em todo o estado, políticas, melhores práticas da indústria e outros requisitos, colaborando com agências estatais, governos federais e locais, cidadãos e empresas do setor privado, e apoiando o gerenciamento de risco e serviços de tecnologia da informação seguros e sustentáveis, a fim de atender às necessidades de cidadãos.

São seus objetivos: proteger a confidencialidade, a integridade e a disponibilidade de dados dos cidadãos e do Estado; promover ambiente operacional de TI seguro; melhorar processos de segurança, incorporando metodologias do processo Information Technology Infrastructure Library (ITIL) para operações de segurança; coordenar e comunicar; e identificar e fornecer orientações sobre gerenciamento de riscos, planejamento de continuidade de negócios, auditoria e conformidade.

No Brasil, o Tribunal Regional do Trabalho da 11ª Região é órgão do Poder Judiciário, cuja jurisdição abrange os estados do Amazonas e de Roraima. Segundo consta no *site* do seu Escritório de Segurança de Informação, destacam-se, como suas atividades principais, a Gestão da Segurança da Informação, o Desenvolvimento da Política de Segurança da Informação, a Gestão de Riscos de Segurança da Informação, a Gestão da Continuidade dos Serviços de TI, a Gestão de Incidentes de Segurança da Informação e a Divulgação da cultura de Segurança da Informação.

Ainda entre as atividades básicas envolvidas com a estruturação de escritório de segurança da informação, há a definição dos papéis e das responsabilidades dos envolvidos, a sua formalização por meio de documentos que o descrevam, e a definição dos processos de suas atividades (MACÊDO, 2012).

Também o Conselho da Secretaria do Tesouro do Canadá possui em seu *site* orientação para desenvolvimento de plano de segurança departamental, na qual consta:

- Processo de desenvolvimento de plano de segurança departamental, de forma ilustrada, que incluiu comunicação e consulta, gestão de riscos de segurança e o seu preparo;
- Gestão integrada de riscos de segurança adaptada de NIST Special Publication 800-39, Integrated Enterprise-Wide Risk Management: Organization, Mission, e Information System View – ilustra abordagem integrada para gestão de riscos de segurança;
- Exemplo de matriz de risco simples para avaliar impacto e probabilidade ao longo de dois eixos.

O objetivo desse guia é ajudar no atendimento às exigências da política de segurança do Governo e à diretiva relativa à gestão da segurança para se desenvolver plano de segurança do departamento. Detalha decisões de gestão de riscos de segurança e delineia estratégias, metas, objetivos, prioridades e prazos para melhorar a segurança do departamento.

Ele descreve abordagem para desenvolvimento da política de segurança do Governo, baseado em processo de gestão de riscos de segurança, a fim de assegurar que decisões de gestão de riscos de segurança sejam comprovadas por meio de análises aprofundadas e apoiadas por processos rigorosos, repetíveis e documentados.

Essa abordagem tem como objetivo apoiar desenvolvimento de plano de segurança departamental que proporciona aos chefes-adjuntos e gerentes seniores visão integrada de requisitos de segurança do departamento alinhada com prioridades estratégicas, programas, planos, processos e outras práticas dentro de cada departamento.

O guia se baseia em princípios bem conhecidos e em melhores práticas relacionadas ao planejamento, à gestão de riscos e à medição de desempenho, montados a partir de instrumentos e diretrizes da política do Conselho do Tesouro, de relatórios de jurisdições, do setor privado e de outros países, juntamente com organismos de normalização, como ISO e NIST. A diretriz também inclui entrada de representantes de departamentos, os quais participaram de seu desenvolvimento.

1.2.1 O público

O guia é destinado a diretores departamentais de segurança, profissionais de segurança e gestores em todos os níveis. Seus papéis e responsabilidades específicas, relacionados com o planejamento do departamento de segurança e a gestão de riscos de segurança, são identificados na política de segurança do Governo e na diretiva relativa à gestão da segurança departamental.

A orientação também pode ser útil para gerentes de departamentos corporativos de risco, planejadores estratégicos, coordenadores de arcabouço de responsabilidade de gestão e outros especialistas no assunto, os quais desempenham papel importante para ajudar a integrar segurança corporativa de gestão de riscos, planejamento e práticas de medição de desempenho, e cujas perspectivas corporativas devem ser consideradas no desenvolvimento do plano de segurança do departamento.

1.2.2 A aplicação

Os chefes-adjuntos e diretores departamentais de segurança dos departamentos têm responsabilidades políticas relacionadas com planejamento de segurança e gestão de riscos de segurança. Cada departamento tem características únicas no que diz respeito a mandato, tamanho, programas, processos e práticas de gestão interna, juntamente com recursos destinados às operações de segurança. Dadas essas diferenças de cada departamento, incluindo-se pequenos departamentos e agências, deve-se determinar abordagem para desenvolvimento de seu plano de segurança do departamento que considere suas operações distintas, capacidade e ambiente de risco, adotando-se ou adaptando-se essa diretriz para melhor atender às suas necessidades de negócio.

1.2.3 A implementação

A diretiva relativa à gestão da segurança departamental forneceu período de transição de três anos para plena aplicação de requisitos relacionados com o plano de segurança do departamento que começou em 2009 e com previsão de término em 2012. A seguinte sequência de ações é sugerida para ajudar a

assegurar que cada passo no processo de gestão de riscos de segurança possa ser completado e que os resultados possam ser utilizados como base para desenvolvimento do plano de segurança do departamento:

- Analisar e definir o contexto; iniciar consultas;
- Conduta e/ou avaliações de risco completas:
    - Consolidar resultados da avaliação de riscos de segurança existentes e identificar lacunas na cobertura, ou seja, atividades do programa que não sejam cobertas por avaliações atuais de risco de segurança para lidar com informações, ativos ou outros recursos;
    - Identificar requisitos para controles adicionais ou indicadores de desempenho.
- Definir prioridades de segurança com base em resultados de avaliações de riscos de segurança e análise de opções de tratamento, desenvolver estratégia de implementação;
- Desenvolver plano de segurança do departamento e buscar aprovação de chefes-adjuntos;
- Iniciar implementação e monitorar desempenho;
- Conduta e/ou avaliações de risco completas conforme necessário para tratar lacunas identificadas;
- Relatório de Progresso de chefes-adjuntos e gerentes seniores;
- Atualizar plano de segurança do departamento como exigido;
- Continuar atividades de gerenciamento de riscos de segurança e implementação e monitoramento dos controles;
- Manter plano de segurança do departamento e informar a chefes-adjuntos e gerentes seniores.

1.2.4 A abordagem integrada para o planejamento

A gestão da segurança é mais eficaz quando é sistematicamente tecida nas corporações, nos programas de cultura e de departamento e no serviço público como um todo.

Os conceitos de planejamento integrado e gestão integrada de riscos não são novos, sendo importante serem vistos como prática necessária para alinhar metas, recursos e resultados, caracterizada como base para avaliação e compreensão de necessidades atuais e futuras dos departamentos e do serviço público em geral.

A gestão de risco, uma vez direcionada para a incerteza relacionada a eventos futuros e resultados, é componente integral de bom planejamento e tomada de decisões em todos os níveis. O quadro de gestão de risco reconhece que risco tem de ser gerido nos níveis e resultados agregados no âmbito corporativo para facilitar definição de prioridades e melhorar a tomada de decisões.

A integração consiste em reunir planos, atividades e processos para que eles funcionem em harmonia uns com os outros a fim de se alcançar objetivos comuns de negócios. O alinhamento consiste em ligar objetivos de curto e de longo prazo para resultados estratégicos e atividades do programa do departamento tal como definidos.

Desenvolver abordagem integrada para planejamento pode ajudar a revelar interdependências e ligações horizontais de atividades individuais, oportunidades de tornar processos de trabalho e operações mais rápidos, e potencial de economias de escala. Alinhar planos para objetivos do negócio do departamento pode ajudar a garantir que recursos possam ser efetivamente alocados para atingir resultados estratégicos.

No exame de melhores práticas de departamentos com programas de segurança maduros, tem sido observado que segurança está firmemente integrada às funções de gestão interna e alinhada com planejamento empresarial e atividades de gerenciamento de risco.

Políticas de segurança e processos de gestão de riscos de segurança e planos estão bem documentados, sob medida para atividades de negócios exclusivos do departamento, e incluem medição de desempenho como componente

integral do planejamento. Integração e alinhamento são ainda apoiados por meio de governança forte, que utiliza estrutura de elementos de prestação de contas de gestão no sentido de estabelecer expectativas de boas práticas de gestão interna e do programa de arquitetura de atividade departamental como quadro para alinhar práticas de gestão interna com resultados do programa de entrega.

Abordagem integrada para gestão e planejamento de riscos exige participação ativa da alta administração e partes interessadas internas de áreas corporativas e do programa. Ela é alcançada por meio de diálogo regular e recorrente, compreensão clara dos papéis e responsabilidades e compromisso de melhorar planejamento e práticas de gestão de risco em todos os níveis dentro do departamento.

1.2.5 A documentação

Documentar processos de segurança, políticas e planos é forma de estabelecer entendimento comum e quadro de referência para terminologia de segurança, apoiar comunicação interna e externa, definir papéis e responsabilidades, e construir maturidade de práticas de segurança e gestão de riscos de segurança. Documentar análise e conclusões da gestão de riscos de segurança ajuda a garantir que resultados sejam reprodutíveis e fornece provas de diligência para que pessoas, inclusive gerentes e auditores, possam entender o pensamento que levou a ação a ser tomada e traçar ações para decisões de gestão, planos e políticas.

A documentação deve ser preparada para processo de avaliação e tratamento de risco de segurança com vistas a capturar análise, resultados e ações resultantes e a fornecer base para análise, definição de prioridades, tomada de decisões e medição de desempenho, ajudando, assim, a demonstrar relação de controles selecionados voltados a resultados da avaliação de risco de segurança e a processos de tratamento de riscos de segurança.

Como a extensão e o formato da documentação são diferentes entre departamentos, dado o tamanho de cada um, a complexidade, as operações e as práticas de gestão interna, cada departamento deve tomar medidas para estabelecer e manter a evidência do processo de gestão de riscos de segurança e resultados

que sejam legíveis, prontamente identificáveis e recuperáveis. Essa documentação também deve permanecer disponível para aqueles que dela necessitem, respeitando qualquer política, requisitos legais ou regulamentares e obrigações contratuais para protegê-la e controlá-la.

1.2.6 O processo de desenvolvimento do plano de segurança departamental

A orientação no desenvolvimento de plano de segurança do departamento é estabelecida de acordo com o processo definido. O processo é híbrido, decorrente de diversos modelos de planejamento e gerenciamento de riscos que são descritos em documentos de referência utilizados para desenvolver essa orientação. Cada passo no processo gestão de riscos de segurança foi mapeado com requisitos obrigatórios relacionados ao plano de segurança do departamento, tal como descrito na política de segurança e na diretiva relativa à gestão da segurança departamental, a fim de ajudar a garantir que esses requisitos possam ser atendidos.

2 O COBIT 5 FOR INFORMATION SECURITY DA ISACA

2.1 A ISACA

A “Information Systems Audit And Control Association” (ISACA®) é provedora, com abrangência internacional, de conhecimento, orientações, certificações, comunidade, defesa e educação no crescente campo de controles de auditoria de sistemas computacionais, em sistemas de informação (SI), garantia e segurança, governança e gestão de TI corporativa, e risco e conformidade relativas à TI.

Fundada em 1969, essa organização, independente e sem fins lucrativos, conta com mais de 100 mil membros distribuídos em 180 países, envolvendo profissionais de governança de TI, bem como auditores externos e internos, consultores, educadores, profissionais de segurança, órgãos reguladores e diretores de informação.

Organiza conferências internacionais, publica o ISACA® Journal e desenvolve padrões internacionais de controle e de auditoria, auxiliando seus participantes a garantir confiança e valor a partir de sistemas de informação.

Essa instituição também promove e certifica habilidades e conhecimentos em TI por meio de titulações mundialmente respeitadas: Certified Information Systems Auditor® (CISA®) – Certificado de Auditor de Sistemas de Informação (em tradução livre); Certified Information Security Manager® (CISM®) – Certificado de Administrador de Segurança da Informação (em tradução livre); Certified in the Governance of Enterprise IT® (CGEIT®) – Certificado em Governança de TI Corporativa (em tradução livre); e Certified in Risk and Information Systems Control TM (CRISC TM) – Certificado em Risco e Controle de Sistemas de Informação (em tradução livre).

2.2 O COBIT

A ISACA atualiza e expande continuamente orientações práticas e uma família de produtos com base no arcabouço denominado Control Objectives for Information and related Technology (COBIT®). O COBIT auxilia profissionais de TI e

líderes empresariais no cumprimento de suas responsabilidades de governança e gestão de TI, particularmente nas áreas de garantia, segurança, risco e controle e entrega de valor ao negócio.

Ele permite o desenvolvimento de políticas claras e de boas práticas para o controle de TI nas organizações, enfatizando a conformidade regulamentar, auxiliando as organizações a aumentar o valor obtido a partir dela, permitindo o alinhamento e a aplicação simplificada do arcabouço COBIT.

O COBIT na versão 5, designado como COBIT 5, modelo de governança e gestão da TI corporativa, divulgado em 2011 pela ISACA, atualiza a geração de arcabouços da ISACA referente à abrangência estratégica, fornecendo quadro compreensivo que auxilia empresas na consecução de seus objetivos quanto à governança e à gestão de informações e ativos de tecnologia (TI) corporativos.

Ele é projetado para atender às necessidades de dirigentes de negócio e permanecer alinhado com governança e gestão técnica de TI corporativa. Simplificando, ajuda as empresas a criarem valor da TI por manter balanceamento ótimo entre desempenho, retorno e riscos associados.

O COBIT 5 permite governar e gerir a TI de forma holística para toda a organização, considerando o processo completo de negócio e áreas funcionais com responsabilidade em TI, ponderando interesses relacionados à TI das partes interessadas internas e externas.

Com base em cinco princípios e no conjunto de sete facilitadores, o COBIT 5 usa métodos para descrever ações que são exemplos de boas práticas para realizar governança e gestão da TI corporativa, otimizando investimento e uso da informação e da tecnologia para o benefício das partes interessadas. Muitas dessas práticas e atividades de apoio exercem "controle" sobre o processo de entrega de resultado desejado.

Esses cinco princípios, descritos mais adiante nos itens 2.3.1 a 2.3.5, são: a) A capacidade e o benefício; b) A necessidade do *stakeholder*; c) O empreendimento fim-a-fim; d) O arcabouço único e integrado; e) A abordagem holística.

2.2.1 A governança e a gestão

O COBIT 5 elucida os papéis de governança (comprometimento) e gestão (envolvimento), fornecendo clara distinção entre elas, com modelo de processo revisto refletindo essa diferença e mostrando o seu relacionamento. Essas duas disciplinas abrangem tipos divergentes de atividades, exigem estruturas organizacionais não coincidentes e servem a propósitos distintos.

O termo “governança” é derivado do verbo grego “Kubernáo”, que significa “para dirigir”. Refere-se às possibilidades e aos mecanismos que auxiliam as áreas da organização a avaliar condições e opções, determinando também direção, monitoramento, conformidade, desempenho e progresso e, dessa forma, alinha planos e objetivos de negócio, a fim de atender aos objetivos específicos da companhia.

A governança assegura que necessidades, condições e opções das partes interessadas sejam avaliadas para determinar equilibrados e consensuais objetivos corporativos a serem alcançados; proporciona o estabelecimento da direção por meio de priorização e tomada de decisão, e o monitoramento de desempenho, de conformidade e de progresso em comparação à direção e objetivos. Em muitas companhias, ela é responsabilidade do conselho de administração, sob a liderança do presidente.

Por outro lado, a gestão envolve uso de recursos, como pessoas, processos, práticas, etc., para atingir meta determinada, sendo meio ou instrumento pelo qual o conselho de administração alcança resultado ou objetivo. Ela abrange planos de gerenciamento, construção, organização, funcionamento e controle de atividade operacional em alinhamento com a direção definida pelo corpo governante para atingir os objetivos do empreendimento. Em muitas organizações, é de responsabilidade da direção executiva, sob a liderança do *chief executive officer* (CEO) – diretor executivo chefe (em tradução livre). Corpo governante é pessoa ou grupo de pessoas que são responsáveis pelo desempenho e pela conformidade da organização, tomando parte da alta administração.

As diferentes funções de governança e de gestão da segurança da informação são visíveis pelo modelo de referência de processo do COBIT 5, o qual permite focar sobre as atividades empresariais relevantes e inclui processos de

governança e de gestão, cada qual com seu próprio conjunto de responsabilidades. O exercício prático de governança e gestão eficazes exige uso adequado de facilitadores.

2.2.2 O facilitador

A governança e a gestão, eficiente e eficaz, da TI e da informação empresarial exigem abordagem holística, considerando-se diversos componentes que interagem entre si. O COBIT 5 define um conjunto de facilitadores para apoiar a implementação de sistema compreensivo de governança e gestão para TI e informação corporativas. Esses facilitadores são agentes tangíveis e intangíveis que, individual e coletivamente, influenciam o funcionamento da governança e da gestão da TI corporativa.

O objetivo dos facilitadores é promover a implementação de modelo de desempenho e sistema de gestão da TI corporativa. Os facilitadores são definidos como apoio para alcançar os objetivos de governança do empreendimento, sendo regidos pela graduação de objetivos, isto é, os objetivos de nível superior relacionados à TI definem o que os diferentes facilitadores devem alcançar.

Eles estão definidos em categorias, tais como: Processos; Estruturas Organizacionais; Cultura, Ética e Comportamento; Princípios, Políticas e Arcabouços; Informação; Serviços, Infraestrutura e Aplicações; Pessoas, Habilidades e Competências.

O facilitador Processos descreve um conjunto organizado de práticas e atividades para alcançar determinados objetivos e produzir conjunto de saídas de apoio para atingir metas gerais relacionados a TI.

Estruturas Organizacionais é o facilitador com as principais entidades de tomada de decisão na organização.

O facilitador Cultura, Ética e Comportamento relaciona o indivíduo e a corporação e é frequentemente subestimado como fator de sucesso em atividades de governança e gestão.

Princípios, políticas e estruturas é o veículo que traduz o comportamento desejado em orientações práticas para o cotidiano da gestão.

Informação é o facilitador que lida com informações produzidas e utilizadas pela corporação, e a permeia, sendo necessário para manter a organização funcionando e bem governada. No nível operacional, ele também é frequentemente o produto-chave do próprio empreendimento.

O facilitador Serviços, Infraestrutura e Aplicações inclui a infraestrutura, a tecnologia e os aplicativos que fornecem processamento e serviços de TI à corporação.

E, finalmente, Pessoas, Habilidades e Competências é o facilitador ligado a pessoas necessárias para a conclusão bem-sucedida das atividades, para a tomada de decisões corretas e a execução de ações corretivas.

2.2.3 O COBIT 5 e a segurança

As orientações do COBIT 5 estão ligadas a expectativas, preocupações e questões de partes interessadas relacionadas à TI corporativa. Como a segurança ajuda a apoiar a missão da empresa e a realização de objetivos de negócio, nesse arcabouço há processos específicos sobre segurança, como os de gerenciamento de risco, da segurança, da continuidade e de serviços de segurança, e da garantia de melhoria de risco (APO12 Manage risk, APO13 Manage security, DSS04 Manage continuity, DSS05 Manage security services, e EDM03 Ensure risk optimisation, respectivamente), que fornecem orientações básicas sobre como definir, operar e monitorar sistema genérico de gestão de segurança.

O COBIT 5 também tomou a abordagem holística de modelo de componentes inter-relacionados do Business Model for Information Security (BMIS) – Modelo de Negócios para Segurança da Informação (em tradução livre), e os incorporou aos componentes do arcabouço, abordando segurança da informação, especificamente, com foco no Information Security Management System (ISMS), sistema de gestão de segurança da informação (em tradução livre) com o APO13 Manage Security do domínio de gestão Align, Plan and Organise (APO), estabelecendo a importância da segurança da informação dentro do arcabouço de processo COBIT 5.

Esse processo evidencia a necessidade de gestão do empreendimento para planejar e estabelecer ISMS adequado para apoiar princípios

de governança de segurança da informação e objetivos de negócios de segurança impactados, resultantes do domínio de governança Evaluate, Direct and Monitor (EDM). A governança da segurança da informação é o sistema pelo qual atividades de segurança da informação da organização são dirigidas e controladas.

2.3 O COBIT 5 FOR INFORMATION SECURITY

O COBIT 5 for Information Security - COBIT 5 para Segurança da Informação (em tradução livre), publicado em 2012, está baseado nos mesmos princípios do COBIT 5, oferecendo orientação da ISACA na governança corporativa e gestão de segurança da informação, usando orientações e exemplos para fornecer visão abrangente ampliada do COBIT 5, exprimindo conceitos e componentes do COBIT 5 a partir da perspectiva de segurança da informação.

Ele baseia-se no arcabouço do COBIT 5, a partir do qual informações pertinentes à segurança da informação foram filtradas e complementadas com orientação mais detalhada, prática e específica, assegurando, assim, a coerência com a arquitetura do produto originador, e valor adicional para componentes de segurança da informação é criado por meio de explicações novas, atividades, processos e recomendações.

O COBIT 5 for Information Security alinha-se com outros arcabouços, padrões e modelos do mercado, como a série ISO/IEC 27000, Information Security Forum (ISF) Standard of Good Practice e BMIS, entregando visão de governança e de gestão da segurança da informação que fornece aos profissionais de segurança orientações detalhadas para o uso de COBIT 5, tais como estabelecer, implementar e manter a segurança da informação nas políticas de negócios, processos e estruturas da corporação.

A ISACA desenvolveu o COBIT 5 for Information Security principalmente como recurso educacional destinado a profissionais de segurança da informação, como chefe do escritório de segurança da informação e gestor de segurança da informação, e outros interessados em segurança da informação em todos os níveis da empresa.

O conteúdo incluído nesse guia aborda:

- Orientação sobre condutores de negócios corporativos e benefícios relacionados à segurança da informação;
- Como os princípios do COBIT 5 podem ser vistos e aplicados a partir da perspectiva dos profissionais de segurança da informação;
- Como facilitadores do COBIT 5 podem ser utilizados por profissionais de segurança da informação para apoiar a governança e gestão corporativa de programas de ação de segurança da informação;
- Como o guia COBIT 5 for Information Security alinha-se com outras normas de segurança da informação.

Ele faz referência a facilitadores, como funções e cargos, comissões e conselhos, processos e políticas. As características únicas de cada empreendimento permitem que esses facilitadores sejam usados de muitas formas, a fim de fornecer a necessária segurança da informação.

Além disso, a ISACA oferece, como adendo à governança de segurança da informação, os guias Information Security Governance: Guidance for Information Security Managers – “Governança de Segurança da Informação: Orientação para Gestores de Segurança da Informação” (em tradução livre) e Information Security Governance: Guidance for Boards of Directors and Executive Management –“Governança de Segurança da Informação: Guia para Conselhos de Administração e Executivo de Gestão” (em tradução livre), que foram analisados durante o desenvolvimento do COBIT 5 for Information Security.

Não obstante, para determinar a adequação de determinada informação, procedimento ou teste, o profissional de segurança deve aplicar seu próprio julgamento de ofício na circunstância específica apresentada pelo particular sistema ou ambiente de TI.

Além do fato de a segurança da informação ser essencial nas operações cotidianas corporativas, outros principais motivadores para o desenvolvimento do COBIT 5 for Information Security foram a necessidade de:

- Descrever a segurança da informação no contexto empresarial, incluindo:
    - O processo completo de negócio de TI e responsabilidades funcionais de segurança da informação;
    - Os aspectos que levam à governança e à gestão eficaz de segurança da informação, tais como estruturas organizacionais, políticas e cultura;
    - A relação e a ligação de segurança da informação com objetivos empresariais.

- As organizações:
    - Manterem riscos de informação em nível aceitável e para proteger as informações contra a divulgação não autorizada, modificações não autorizadas ou acidentais, e possíveis invasões;
    - Certificarem-se de que os serviços e sistemas estão continuamente disponíveis para as partes interessadas internas e externas, levando satisfação ao usuário com compromisso e serviços de TI;
    - Cumprirem com o crescente número de leis e regulamentos, bem como requisitos contratuais e políticas internas de informação e sistemas de segurança e proteção, e proporcionar transparência sobre nível de cumprimento;
    - Obterem êxito nos desafios acima, enquanto contém o custo de serviços de TI e proteção de tecnologia;
    - Conectar e, se for o caso, alinhar com outros importantes arcabouços e padrões de mercado;
    - Unir principais pesquisas, arcabouços e orientações da ISACA, com foco primário no COBIT e BMIS, e também considerando o Val IT, o Risk IT, o IT

> Assurance Framework (ITAF), a publicação intitulada Board Briefing on IT Governance e o recurso Taking Governance Forward (TGF).

2.3.1 A capacidade e o benefício

O uso do COBIT 5 for Information Security pode trazer capacidades relacionadas à segurança da informação para a corporação, podendo resultar em benefícios empresariais, tais como:

- Redução da complexidade e melhora da relação custo-efetividade devido à maior e mais fácil integração de padrões de segurança da informação, boas práticas e/ou diretrizes setoriais;
- Aumento da satisfação do usuário com programas de ação e resultados da segurança da informação;
- Melhor integração da segurança da informação na corporação;
- Inteligente conscientização e decisões de risco;
- Melhoria da prevenção, detecção e recuperação;
- Reduzido impacto dos incidentes de segurança da informação;
- Suporte avançado para inovação e competitividade;
- Melhoria da gestão de custos relacionados à função de segurança da informação;
- Melhor compreensão da segurança da informação.

Esses benefícios podem ser obtidos por meio do uso das capacidades desse arcabouço, a saber:

- Visão atual sobre governança – O COBIT 5 for Information Security fornece ponto de vista atualizado sobre governança e gestão de segurança da informação por meio do alinhamento com o

COBIT 5 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500 e outras iniciativas de governança de TI. Durante o seu desenvolvimento, importante orientação e padrões foram analisados;

- Visão fim a fim – O COBIT 5 for Information Security é modelo de processo que integra negócios e responsabilidades funcionais de TI. Ele fornece distinção entre práticas de governança e gestão de segurança da informação, delineando responsabilidades em diversos níveis da empresa, abrangendo etapas do começo ao fim do processo;

- Orientação holística – O arcabouço COBIT 5 for Information Security reúne orientação abrangente em segurança da informação, focando processos e facilitadores, incluindo informação, estruturas, cultura, políticas e sua interdependência.

2.3.2 A necessidade do *stakeholder*

As necessidades de partes interessadas têm de ser transformadas em estratégia corporativa de ação. Uma vez que cada empreendimento tem diferentes objetivos, eles devem usar a graduação de suas respectivas metas para personalizar o uso de conceitos do COBIT 5, a fim de satisfazer o seu próprio contexto.

Na graduação de objetivos, as necessidades das partes interessadas, que são influenciadas por diversos condutores, são traduzidas e especificadas em metas operacionais da companhia a serem satisfeitas, tornando envolvimento, responsabilidades e obrigações de partes interessadas corporativas no uso de TI mais explícitos e transparentes.

A graduação de metas do COBIT 5 traduz necessidades de interessados em objetivos específicos, factíveis e personalizados dentro do contexto da organização, em objetivos relacionados a TI e em metas de facilitador. Isto é, metas empresariais, por sua vez, requerem que objetivos relacionados a TI sejam alcançados e, finalmente, se traduzem em metas para diferentes facilitadores.

A segurança da informação participa das principais necessidades de partes interessadas, e isso se traduz em metas relacionadas à segurança da informação para a corporação, para a TI e, finalmente, para facilitadores de apoio.

O COBIT 5 for Information Security está baseado nos mesmos princípios que o arcabouço COBIT 5, como mencionado anteriormente. Nele, objetivos específicos de segurança da informação para processos são definidos em apoio às necessidades relacionadas à segurança da informação das partes interessadas. Da mesma forma, metas específicas relacionadas à segurança da informação são definidas para outros facilitadores.

2.3.3 O empreendimento fim a fim

O COBIT 5 integra a governança de TI da empresa em governança corporativa por:

- Cobrir todas as funções e processos dentro da empresa. O COBIT 5 foca a "função de TI" e trata informações e tecnologias relacionadas como ativos que precisam ser tratados como qualquer outro ativo por todos na empresa;
- Considerar facilitadores relacionados à governança e gestão de TI da corporação e fim a fim, ou seja, inclusive tudo e todos, interna e externamente, que sejam relevantes para governança e gestão da informação corporativa e relacionados à TI. Aplicando esse princípio à segurança da informação, o COBIT 5 for Information Security cobre todas as partes interessadas, funções e processos dentro da instituição que sejam relevantes para segurança da informação.

2.3.4 O arcabouço único e integrado

Há muitos padrões e melhores práticas relacionados à TI, cada qual com orientação em subconjunto de atividades relacionadas com TI. O COBIT 5 pretende cobrir o todo corporativo, fornecendo fundamento para integrar, de forma eficaz, outros arcabouços, normas e práticas utilizadas, com estrutura única e

integrada, que sirva como fonte de orientação em linguagem comum (não técnica e não culta em tecnologia).

O COBIT 5 alinha-se com outras normas e estruturas e, assim, permite que a corporação possa usá-lo de forma abrangente para governança e gestão do empreendimento de TI.

Mais especificamente, o COBIT 5 for Information Security reúne conhecimentos anteriormente dispersos por diferentes estruturas e modelos (COBIT, BMIS, Risk IT, Val IT) da ISACA com orientação de outras principais normas relacionadas à segurança da informação, como a série 27000 da ISO/IEC, o padrão de boas práticas em segurança da informação da ISF (ISF Standard of Good Practice) e o SP800-53A do U.S. National Institute of Standards and Technology (NIST) – Instituto de Padrões e Tecnologia Nacional dos EUA (em tradução livre).

2.3.5 A abordagem holística

O COBIT 5, como mencionado anteriormente, define facilitadores, os quais são agentes que, individual e coletivamente, influenciam o funcionamento da governança e gestão de empresas de TI e, relacionados nesse caso, à governança de segurança da informação.

O conjunto de facilitadores interligados apresentam ponto de vista abrangente e abordagem sistêmica necessários para a adequada segurança da informação.

3 OS FACILITADORES DO COBIT 5 NA PRÁTICA DA SEGURANÇA DA INFORMAÇÃO

3.1 A SEGURANÇA DA INFORMAÇÃO PELA ISACA

A ISACA define “segurança da informação” como a garantia de que, dentro da organização, informações estão protegidas contra divulgação para usuários não autorizados (confidencialidade), modificação indevida (integridade) e não acesso quando necessário (disponibilidade).

“Confidencialidade” significa preservar restrições autorizadas de acesso e divulgação, incluindo meios de proteção à privacidade e informações confidenciais. “Integridade” significa proteção contra modificação inadequada ou destruição de informação, e inclui garantia de não repúdio e autenticidade da informação. E “disponibilidade” significa garantir acesso oportuno e confiável e uso da informação. Embora existam outras definições desses termos, estas fornecem fundamentos de segurança da informação, uma vez que cobrem conceitos, conhecidos como "CID", de Confidencialidade, Integridade e Disponibilidade.

É importante notar que, embora o conceito CID seja mundialmente aceito, existem usos mais gerais do termo "integridade" no contexto mais amplo de negócios. Por exemplo, o COBIT 5 abrange este termo no facilitador Informação, como metas de completeza e exatidão da informação.

O COBIT 5 for Information Security está limitado ao ponto de vista de segurança deste termo e constrói sobre essa definição para descrever como a segurança da informação pode ser aplicada na vida real, tendo em conta os princípios do COBIT 5.

3.2 OS PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO PELA ISACA, PELO ISF E PELO (ISC)2

Os princípios de segurança da informação comunicam regras corporativas em apoio aos objetivos de governança e valores da empresa, conforme definido pelo conselho e pela diretoria executiva. Esses princípios devem ser em

número limitado e expressar os valores fundamentais da empresa, em linguagem simples e declarativa, tão clara quanto possível.

A ISACA, o ISF e o International Information System Security Certification Consortium [(ISC)2] desenvolveram 12 princípios independentes e não proprietários, que auxiliam profissionais de segurança da informação a agregar valor às suas organizações, apoiando com sucesso o negócio e promovendo boas práticas de segurança da informação.

Esses princípios são genéricos e aplicáveis a todas as empresas. No desenvolvimento de princípios de segurança da informação exclusivos para a empresa, esta lista pode ser usada como inspiração:

- Suporte ao negócio:
    - Concentrar-se no negócio para garantir que a segurança da informação esteja integrada em atividades empresariais essenciais;
    - Entregar qualidade e valor para partes interessadas, a fim de garantir que segurança da informação agregue valor e atenda aos requisitos de negócios;
    - Cumprir requisitos legais e regulamentares pertinentes para garantir que obrigações legais sejam cumpridas, expectativas das partes interessadas sejam geridas e penalidades civis ou criminais sejam evitadas;
    - Fornecer informações oportunas e precisas sobre desempenho da segurança da informação para apoio aos requisitos corporativos e gerenciar risco da informação;
    - Avaliar atuais e futuras ameaças de informação, a fim de analisar e estimar ameaças emergentes de segurança da informação, tão logo sejam conhecidas, para que ações tempestivas (oportunas e em tempo devido) possam ser tomadas para mitigar riscos;
    - Promover melhoria contínua em segurança da informação para reduzir custos, melhorar eficiência e

eficácia, e promover cultura de melhoria contínua da segurança da informação.

- Defesa do negócio:

    - Adotar abordagem baseada em risco para garantir que o risco seja tratado de maneira coerente e eficaz;
    - Proteger informações confidenciais para impedir a divulgação a pessoas não autorizadas;
    - Concentrar-se em aplicações críticas de negócios para priorizar os escassos recursos de segurança da informação, a fim de proteger as aplicações de negócio nas quais eventuais incidentes de segurança tenham impacto maior nos negócios;
    - Desenvolver sistemas seguramente para construção com qualidade e relação custo/benefício em que os empresários possam confiar.

- Promoção do comportamento responsável de segurança da informação:

    - Agir de forma ética e profissional para garantir que atividades relacionadas à segurança da informação sejam realizadas de forma confiável, responsável e eficaz;
    - Estimular cultura positiva de segurança da informação, a fim de fornecer influência segura positiva no comportamento de usuários finais, reduzir probabilidade de que ocorram incidentes de segurança, e limitar o seu potencial impacto nos negócios.

3.3 OS FACILITADORES DO COBIT 5 PARA IMPLEMENTAR A SEGURANÇA DA INFORMAÇÃO NA PRÁTICA

Os facilitadores definidos no COBIT 5 têm um conjunto de dimensões comuns que fornece uma maneira estruturada de lidar com eles, permite gerir suas interações e facilita resultados. Eles podem ser aplicados em situações práticas para implementar, na organização, a governança e a gestão de segurança da informação.

3.3.1 Os facilitadores de dimensão

As quatro dimensões comuns para esses facilitadores são: partes envolvidas, objetivos, ciclo de vida e boas práticas.

Cada facilitador tem partes interessadas que desempenham papel ativo e/ou têm interesse na execução. Por exemplo, os processos têm diferentes partes interessadas, que executam atividades no processo e/ou que têm interesse nos resultados do processo; estruturas organizacionais têm partes interessadas, cada qual com suas próprias funções e interesses, que participam dessas estruturas. As partes interessadas podem ser internas ou externas à corporação, todas com seus próprios, e por vezes conflitantes, interesses e necessidades. O *stakeholder* precisa traduzir os objetivos da organização, os quais, por sua vez, se traduzem em metas relacionadas com TI para o empreendimento.

Cada facilitador tem uma série de objetivos, resultados esperados, e os facilitadores fornecem valor ao atingir essas metas. O facilitador “objetivos é o último passo na graduação de metas do COBIT 5.

Cada facilitador tem um ciclo de vida, desde a concepção, passando pela existência operacional/útil, até o descarte. As fases do ciclo de vida consistem em: plano (inclui desenvolvimento e seleção de conceitos); projeto; construção/aquisição/criação/implementação; uso/operação; avaliação/monitoramento; e atualização/eliminação.

Para cada facilitador, boas práticas podem ser definidas. Boas práticas apoiam a realização das metas dos facilitadores e fornecem exemplos ou sugestões sobre a melhor forma de implementar o facilitador e que produtos de

trabalho ou entradas e saídas são obrigatórios. Uma vez que boas práticas estejam devidamente sintonizadas e integradas com sucesso dentro da organização, elas podem tornar-se melhores práticas para o empreendimento, por meio do acompanhamento das necessidades empresariais em constante mudança e monitoramento adequado.

3.3.2 Os facilitadores de gestão de desempenho

As companhias esperam resultados positivos da aplicação e utilização de facilitadores.

Para gerenciar o desempenho dos facilitadores, as seguintes perguntas devem ser monitoradas e respondidas a partir de métricas em base regular:

- As necessidades das partes interessadas são abordadas?
- O facilitador “objetivos” foi alcançado?
- O facilitador “ciclo de vida” está gerenciado?
- As boas práticas foram aplicadas?

As duas primeiras questões lidam com o resultado real do facilitador. As métricas usadas para medir até que ponto os objetivos são alcançados podem ser chamadas de "indicadores de resultado".

As duas últimas questões lidam com o real funcionamento do facilitador em si, e métricas para isso podem ser chamadas de "indicadores líderes".

3.3.3 O COBIT 5 for Information Security e os facilitadores

O COBIT 5 for Information Security fornece orientação específica relacionada com os seguintes facilitadores:

- Princípios, políticas e arcabouços de segurança da informação;
- Processos, incluindo detalhes e atividades específicos de segurança da informação;

- Estruturas organizacionais específicas de segurança da informação;
- Em termos de cultura, ética e comportamento, os fatores que determinam o sucesso da governança e gestão da segurança da informação;
- Tipos de informação específicos de segurança de informação para permitir governança e gestão da segurança da informação dentro da corporação;
- Capacidades de serviço necessárias para garantir a segurança da informação e funções relacionadas à companhia;
- Pessoas, habilidades e competências específicas para segurança da informação.

3.3.4 O facilitador Princípios, Políticas e Arcabouços

Princípios, Políticas e Arcabouços referem-se aos mecanismos de comunicação postos em prática para transmitir direção e instruções dos órgãos de governança e gestão.

Princípios, Políticas e Arcabouços é veículo para traduzir comportamento desejado de membros colaboradores do empreendimento para segurança da informação em orientações formais e práticas para o dia a dia de gestão. Esses princípios, políticas e arcabouços podem ser estruturados de acordo com dimensões do modelo facilitador.

No COBIT 5 for Information Security, há modelo que define, em alto nível, os diferentes componentes de Princípios, Políticas e Arcabouços, o qual é extensão do modelo genérico facilitador.

O modelo de Princípios, Políticas e Arcabouços indica que:

- As partes interessadas para princípios, políticas e arcabouços incluem diretoria e administração executiva, diretores de compliance, gerentes de risco, auditores internos e externos, prestadores de serviços e clientes, e agências reguladoras. Os suportes são dois:

alguns interessados definem e estabelecem políticas, outros precisam cumprir e alinhar-se com políticas;

- Os princípios, políticas e arcabouços são instrumentos utilizados para comunicar as regras do empreendimento em apoio a objetivos de governança e valores corporativos, conforme definido pela diretoria e pela gerência executiva. Os princípios devem ser em número limitado e expressos em linguagem simples. Políticas fornecem orientações mais detalhadas sobre como colocar princípios em prática, pois eles influenciam o modo como a tomada de decisão alinha-se com esses princípios;

- As políticas têm ciclo de vida que deve apoiar a realização dos objetivos definidos. Arcabouços são fundamentais porque proporcionam estrutura para definir orientação consistente, por exemplo, arcabouço de política define a estrutura na qual um conjunto coerente de políticas possa ser criado e mantido, e fornece ponto de fácil navegação dentro e entre as políticas individuais;

- As boas práticas exigem que políticas sejam parte de arcabouço global de política, fornecendo estrutura, hierárquica, na qual essas políticas devem se encaixar e claramente fazer a ligação com princípios subjacentes;

- O arcabouço de política precisa definir:

    - Aprovadores de políticas empresariais;
    - Consequências de não cumprimento da política;
    - Meios de tratamento de exceções;
    - Modo pelo qual a conformidade com a política vai ser verificada e medida.

A responsabilidade pelo desenvolvimento e pela manutenção do arcabouço e das políticas relacionadas é atribuída ao presidente do comitê diretor de segurança da informação. O arcabouço pode ser usado como espaço reservado, no qual cabem todas políticas/procedimentos, e para articulá-los com princípios identificados. Na prática, o arcabouço assessora o profissional de segurança da

informação e/ou outros usuários das políticas de segurança da informação em como consultar orientações disponíveis.

Os requisitos detalhados de segurança da informação e documentação devem ser consultados primeiro em caso de questão operacional. Caso a orientação operacional e/ou técnica adequada não exista, o usuário pode consultar procedimentos de segurança da informação e, consequentemente, políticas de segurança da informação específicas relacionadas. Essas políticas cobrem área suplementar de segurança da informação e fornecem orientação tática. A política de segurança da informação consiste de direção de alto nível em segurança da informação. O usuário pode consultar esta política geral quando não existe política detalhada. Finalmente, o usuário precisa aplicar princípios gerais quando a política geral de segurança da informação não é clara sobre o tema.

Quando o usuário identifica a necessidade de orientação mais detalhada, esta deve sempre ser comunicada ao gerente de segurança da informação.

Para o desenvolvimento da orientação específica para a organização, o comitê diretor de segurança da informação, ou aquele a quem essa função foi delegada, pode usar padrões de segurança da informação. Nesse contexto, o uso de padrões genéricos e obrigatórios de arcabouços e modelos como entrada para o arcabouço de política pode ser significativo. Dependendo da situação, normas obrigatórias, arcabouços e modelos devem ser considerados na elaboração dos princípios, políticas, procedimentos e requisitos. Por exemplo, quando a companhia toma a decisão de negócios para tornar-se certificada segundo a norma ISO/IEC 27001, ela se obriga a estar em conformidade com esse normativo. Corporações que fornecem e aceitam cartões de crédito precisam cumprir a norma internacional Payment Card Industry Data Security Standard (PCI DSS) – Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (em tradução livre).

Nesses casos, normas relacionadas utilizadas tornaram-se obrigatórias, devido às decisões de negócios realizadas. Como alternativa, o comitê diretor de segurança da informação pode querer utilizar normas e diretrizes de segurança da informação como boas práticas genéricas para desenvolver eficazmente princípios, políticas, procedimentos e requisitos necessários.

As políticas de segurança da informação fornecem orientações mais detalhadas sobre como colocar em prática princípios e como eles irão influenciar a tomada de decisão. Nem toda política relevante é escrita e apropriada pela função de segurança da informação. Elas são estruturadas em três grupos:

- A política de segurança da informação escrita pela função de segurança da informação, mas impulsionada pelo conselho de administração;
- Política de segurança da informação específica conduzida pela função de segurança da informação;
- Outras políticas que podem estar relacionados à segurança da informação, mas são movidas por outras funções na empresa. Nessas políticas, segurança da informação deve influenciar o desenvolvimento para garantir a realização dos requisitos de segurança da informação.

A seguinte lista de políticas relevantes é ilustrativa e não exaustiva:

- Política de segurança da informação;
- Política de controle de acesso;
- Política de segurança da informação pessoal;
- Política de segurança da informação física e ambiental;
- Política de gestão de incidentes;
- Política de continuidade dos negócios e de recuperação de desastres;
- Política de gestão de ativos;
- Regras de comportamento, isto é, uso aceitável;
- Política de aquisição de sistemas de informação, desenvolvimento de software e sua manutenção;

- Política de gestão de fornecedores;
- Política de comunicações e gestão de operação;
- Política de Compliance – Conformidade, em tradução livre;
- Política de gestão de risco.

Para cada política, os seguintes atributos devem ser descritos:

- Escopo;
- Validade, exceto para políticas de segurança da informação impulsionadas por outras funções dentro da empresa:
    - Aplicabilidade, isto é, definir para quais áreas da empresa esta política é aplicável;
    - Atualização e revisão, ou seja, quem é responsável por manter a política e qual é a frequência de revalidação;
    - Distribuição, a qual define como a política deve ser disseminada pela empresa.
- Objetivos, exceto para políticas de segurança da informação impulsionadas por outras funções dentro da empresa.

Essas políticas e, consequentemente o arcabouço de política, devem estar alinhadas com princípios e objetivos globais corporativos, estratégia e apetite de risco. Como parte das atividades de governança de risco, o apetite de risco da empresa é definido e deve estar refletido nas políticas. A companhia com aversão ao risco vai ter políticas diferentes da organização que assume riscos maiores, devido à natureza do empreendimento, ao ambiente em que opera e à sua postura quanto ao risco.

As políticas devem considerar a situação específica existente na empresa. O conteúdo das políticas empresariais muda de acordo com o contexto da organização e do ambiente em que atua. Essa situação específica é composta por fatores, tais como:

- Regulamentos aplicáveis exclusivos para a empresa;
- Requisitos operacionais e funcionais de negócios;
- Propriedade intelectual e necessidades de proteção de dados competitivos;
- Políticas de alto nível existentes e da cultura corporativa;
- Arquitetura única de projetos corporativos de TI;
- Regulamentos governamentais, como a Federal Information Security Management Act (FISMA) nos Estados Unidos;
- Padrões da indústria, por exemplo, PCI DSS.

Na orientação detalhada, sugestões são feitas sobre possível conteúdo de política de segurança da informação:

- Cobertura dentro da empresa;
- Gestão de orçamento e custos do ciclo de vida de segurança da informação;
- Planos estratégicos de segurança da informação e gestão de carteiras de projetos;
- Visão, objetivos e métricas;
- Inovação e melhores práticas;
- Criação de valor;
- Comunicação e relatórios às partes interessadas;
- Governança de tecnologia e arquitetura;
- Cultura e conscientização de segurança da informação;

- Propriedade atribuída às informações críticas pelas partes interessadas;
- Fornecedores e terceiros.

Essa lista pode fornecer orientação para desenvolver política única adaptada e alinhada à situação específica. A política pode existir em documento extenso, contendo elementos relevantes, ou em documento orientador, contendo diretrizes de alto nível conectadas a políticas mais detalhadas. Qualquer forma é aceitável, desde que o formato seja claramente descrito no arcabouço de política.

Conforme definido no COBIT 5 pelo processo APO01.03 – Maintain the enablers of the management system – “manter facilitadores do sistema de gestão” (em tradução livre), as políticas precisam ser gerenciadas em todo o seu ciclo de vida. Avaliação e atualização de políticas são necessárias em base regular, e mecanismo de gatilho para atualizações fora do ciclo de vida deve ser implementado também.

A evolução e as tecnologias emergentes, como as relativas ao uso de dispositivos móveis, mídias sociais, computação em nuvem, sistemas de *Shadow IT* – “sistemas construídos e usados nas empresas sem aprovação organizacional” (em tradução livre), ou o uso comercial de TI descentralizado devem acionar a necessidade de revisar e atualizar a política. Além disso, mudanças nos requisitos de conformidade regulamentar locais necessitam de revisão e atualização das políticas existentes, ou talvez de novas políticas.

Adicionalmente, em muitas empresas, é necessária a revisão de políticas por áreas externas à função de segurança da informação. Potenciais questões de privacidade, por exemplo, podem provocar envolvimento de funções legais e recursos humanos na aprovação de políticas.

O comitê diretor de segurança da informação permanece, em última análise, responsável pelo desenvolvimento de políticas e por sua atualização. Esse comitê de direção pode exigir a aprovação da gestão executiva, quando a política global de segurança da informação é adaptada.

Para maior clareza de papéis, é apropriado distinguir entre dois grupos dentro da alta administração: órgão de governança e gestão executiva.

O corpo de governança é pessoa ou grupo de pessoas que são imputáveis ou responsabilizáveis pelo desempenho e pela conformidade da organização.

E a gestão executiva é pessoa ou grupo de pessoas com responsabilidade delegada pelo corpo de governança para implementar estratégias e políticas a fim de realizar os propósitos da organização, podendo incluir CEOs, líderes de organizações governamentais, COOs, CFOs, CIOs, CISOs e funções similares.

Para políticas mais técnicas, o comitê gestor pode decidir de forma independente. Para pequenas empresas, políticas podem existir, mesmo no caso de não estarem documentadas e formalmente aprovadas.

3.3.5 O facilitador Processos

Há processos do COBIT 5 apresentados especificamente para obter segurança da informação, incluindo detalhes, como objetivos e métricas de segurança da informação, e atividades específicas de segurança da informação. O conteúdo de processo do COBIT 5 é reduzido ao que é relevante para segurança da informação e expandido para alinhar-se com fontes externas de segurança da informação. Para tal, há o COBIT® 5 – Enabling Processes – “Facilitando Processos” (em tradução livre), publicação complementar específica de segurança da informação.

Processos descrevem um conjunto organizado de práticas e atividades para atingir certos objetivos e produzir um conjunto de saídas, a fim de apoiar o cumprimento de objetivos relacionados à TI em geral, como descrito anteriormente.

No COBIT 5 for Information Security, há modelo que define, em alto nível, os diferentes componentes de processo, o qual é extensão do modelo genérico facilitador.

O COBIT 5 define “processo” como o conjunto de práticas influenciadas por políticas e procedimentos corporativos que obtém entradas a partir de fontes, incluindo outros processos, manipula entradas e produz saídas, como produtos e serviços.

O modelo de processo indica que:

- Processos têm partes interessadas internas, como, por exemplo, diretoria, gerência, funcionários, voluntários e reguladores; e externas, como clientes, parceiros de negócios e acionistas, cada qual com papéis e níveis de responsabilidade, como documentado na matriz de atribuição de responsabilidade RACI, que apresenta a relação entre papéis desempenhados e atividades. RACI é o acrônimo em inglês de “Responsible” (responsável), “Accountable” (aprovador), “Consulted” (consultado) e “Informed” (informado). Eles podem ser classificados como objetivos intrínsecos, objetivos contextuais, ou metas de acessibilidade e segurança. Em cada nível da graduação de metas, métricas são definidas para medir a extensão na qual os objetivos são alcançados. Além disso, a gestão de desempenho do facilitador descreve a extensão à qual as boas práticas são aplicadas. Métricas associadas podem ser definidas para ajudar com a gestão do facilitador;

- Cada processo tem um ciclo de vida, que é definido, criado, operado, monitorado e ajustado/atualizado ou descartado. Práticas de processos genéricos, tais como os definidos no COBIT® Process Assessment Model (PAM) – “modelo COBIT de Avaliação de Processo” (em tradução livre), da ISACA, baseado na norma ISO/IEC 15504, podem ajudar com definição, execução, monitoramento e melhoria de processos;

- Boas práticas internas são descritas em níveis crescentes de detalhe: práticas, atividades e atividades detalhadas. Boas práticas externas podem existir em qualquer forma ou nível de detalhes e, principalmente, referem-se a outros padrões e arcabouços. Os usuários podem se referir a essas práticas em todos os momentos, sabendo que o COBIT 5 for Information Security está alinhado com esses padrões e modelos nos quais informação relevante e mapeada será disponibilizada.

O alinhamento entre COBIT 5 for Information Security e outros padrões e modelos está descrito em detalhes. A informação detalhada, relacionada a processo e específica de segurança da informação para processos de governança e gestão do COBIT 5, inclui:

- **Identificação do processo**

  Na descrição do processo, a seguinte informação deve estar identificada:

  - Rótulo do Processo – Composto por prefixo de domínio (EDM, APO, BAI, DSS ou MEA) e número do processo;
  - Nome do processo – Breve descrição, indicando principal assunto do processo;
  - Área – Governança ou gestão;
  - Nome de domínio, dentre as seguintes opções: Evaluate, Direct and Monitor (EDM) – “Avaliar, Dirigir e Acompanhar” (em tradução livre); Align, Plan and Organise (APO) – “Alinhar, Planejar e Organizar” (em tradução livre); Build, Acquire and Implement (BAI) – “Construir, Adquirir e Implementar” (em tradução livre); Deliver, Service and Support (DSS) – “Entrega, Serviço e Suporte” (em tradução livre); e Monitor, Evaluate and Assess (MEA) – “Monitorar, analisar e avaliar” (em tradução livre).

- **Descrição do processo**

  Descreve o processo com detalhes e contém:

  - Visão global do que o processo faz, ou seja, o objetivo do processo;
  - Visão global de alto nível de como o processo realiza a finalidade;

- **Declaração de propósito do processo**; a descrição da finalidade geral do processo;
- Metas e métricas do processo. Para cada processo, número limitado de objetivos de processos específicos de segurança da informação deve estar incluído e, para cada meta de processo, número limitado de exemplos de métricas específicas de segurança da informação deve estar listado, refletindo a clara relação entre objetivos e métricas;
- A descrição detalhada das práticas de processamento, contendo, para cada prática:
    - Título da prática e descrição;
    - Entradas da prática específicas de segurança da informação e saídas (produtos de trabalho), com indicação de origem e destino;
    - Atividades de processo específicas de segurança da informação.

Como mencionado anteriormente, há o princípio orientador, no COBIT 5, da distinção entre governança e gestão. Em consonância com esse princípio, cada organização deverá implementar processos para fornecer governança e gestão global de segurança da informação.

Ao considerar processos de governança e gestão no contexto da companhia, a diferença entre os tipos de processos reside nos seus objetivos.

Os processos de governança lidam com os objetivos de governança de realização de benefícios e de melhoria de risco e de recursos. Eles incluem práticas e atividades que visam avaliar as opções estratégicas, fornecer orientação para a segurança da informação e acompanhamento do resultado, como representado no domínio EDM, em consonância com os conceitos da Norma 38500 da ISO/IEC.

Os processos de gestão incluem práticas e atividades destinadas a cobrir áreas de responsabilidade de *planning*, *building*, *running and monitoring* (PBRM) – “planejamento, construção, execução e monitoramento” (em tradução

livre), da segurança da informação. Os processos de gestão fornecem cobertura fim a fim de segurança da informação.

Os resultados dos dois tipos de processos são distintos e são destinados a diferentes audiências. No entanto, internamente, processos requerem atividades de planejamento, construção ou implementação, execução e monitoramento dentro deles próprios.

Tal como descrito anteriormente, facilitadores estão interligados e interagem dinamicamente, isto é, para alcançar principais objetivos corporativos, a companhia deve sempre considerar o conjunto interligado de facilitadores. Portanto, cada facilitador:

- Necessita da entrada de outros facilitadores para ser totalmente eficaz. Por exemplo, Processos precisam de Informação; Estruturas Organizacionais precisam de Aptidões e de Comportamento;
- Oferece saída para benefício de outros facilitadores. Por exemplo, Processos fornecem Informações; Habilidades e Comportamentos fazem Processos eficientes.

3.3.6 O facilitador Estruturas Organizacionais

As Estruturas Organizacionais são definidas como principais entidades de tomada de decisão na organização e relevantes para a segurança da informação.

No COBIT 5 for Information Security, há modelo que define, em alto nível, os diferentes componentes da Estrutura Organizacional, o qual é extensão do modelo genérico facilitador.

O modelo de estrutura organizacional indica que:

- Os papéis de partes interessadas das estruturas organizacionais, incluindo fazer, influenciar e aconselhar decisão, variam, assim como o suporte, isto é, o interesse que eles têm nas decisões tomadas pela estrutura;

- As metas para o facilitador Estruturas Organizacionais para si mesmo incluem: ter mandato adequado, princípios operacionais bem definidos e aplicações de outras boas práticas. O resultado do facilitador Estrutura Organizacional deve incluir bom número de atividades e decisões;

- A Estrutura Organizacional tem ciclo de vida. É criada, existe e é ajustada, e, finalmente, pode ser dissolvida. Durante a sua criação, mandato, com razão e propósito para sua existência, deve ser definido;

- Bom número de boas práticas para estruturas organizacionais pode ser distinguido.

As partes interessadas são o primeiro componente do modelo facilitador Estruturas Organizacionais. Do ponto de vista da segurança da informação, as partes interessadas estão organizadas em duas categorias:

- Papéis e estruturas específicos de segurança da informação. Esses papéis e estruturas são internos à função de segurança da informação;
- Papéis e estruturas relacionados à segurança da informação. Esses papéis e estruturas não são organizados ou preenchidos por membros da função de segurança da informação. As questões de segurança da informação e os temas são discutidos ou tratados por esses papéis e estruturas, por exemplo, usuários e proprietários de processos de negócios.

Funções e estruturas de segurança da informação representadas a seguir são comumente encontradas dentro da organização típica:

- Chief information security officer (CISO) – “Chefe do Escritório de Segurança da Informação” (em tradução livre), como definido no COBIT 5, é o responsável geral pelo programa de segurança de informação corporativa;
- Information security steering committee (ISSC) – “Comitê Diretor de Segurança da Informação” (em tradução livre), garante, por meio de monitoramento e avaliação, que boas práticas em matéria de segurança da informação sejam aplicadas eficaz e consistentemente em toda a corporação;
- Information security manager (ISM) – “Administrador de Segurança da informação” (em tradução livre), como definido no COBIT 5, é o responsável geral pela gestão dos esforços de segurança da informação.

Além dessas funções e estruturas específicas de segurança da informação, dois exemplos de estruturas relacionadas estão descritos abaixo:

- Enterprise Risk Management (ERM) Committee – “Comitê de gestão de risco organizacional” (em tradução livre) – é o responsável pela tomada de decisão da companhia para avaliar, controlar, aperfeiçoar, financiar e controlar riscos das fontes, com a finalidade de aumentar o valor de curto e longo prazo da empresa com seus *stakeholders*;
- Custodiante da informação/empresários – contato entre negócios e funções de segurança da informação.

Para cada um deles, as seguintes boas práticas têm sido descritas:

- Composição – conjunto de habilidades apropriado deve ser exigido dos membros do grupo organizacional;
- Mandato, princípios de funcionamento, amplitude de controle e nível de autoridade – esses elementos descrevem os mecanismos práticos de como a estrutura opera, os limites dos direitos da estrutura organizacional de decisão, as responsabilidades e obrigações, bem como o caminho de escalonamento ou ações necessárias em caso de problemas;
- Gráfico RACI de alto nível – matriz de atribuição de responsabilidade RACI ligando atividades de processo às estruturas organizacionais e/ou funções individuais na organização. Eles descrevem o nível de envolvimento de cada função para cada prática de processo: responsável, aprovador, consultado ou informado;
- Entradas/Saídas – a estrutura requer entradas, normalmente informações, antes que possa tomar decisões informadas, e produz saída, por exemplo, decisões, outras informações ou pedidos de entradas adicionais.

Papéis específicos complementares de segurança da informação podem ser criados conforme a organização. Exemplos de funções típicas em equipe de segurança da informação são:

- Administrador de segurança da informação;
- Arquiteto de segurança da informação;
- Administrador de conformidade e auditoria em segurança da informação.

Em pequenas empresas, tarefas abrangidas por esses papéis podem ser realizadas pelo gestor de segurança da informação. Descrições detalhadas desses grupos e funções, assim como orientação prática adicional sobre essas estruturas, podem ser encontradas nesse guia.

Esses papéis e estruturas são adequados para companhia que lida com informações confidenciais e também para a que atingiu tamanho e complexidade organizacional. Para empreendimento maior ou que necessita de foco mais robusto em segurança da informação, elaborada segurança da informação organizacional é apropriada, e grupos e funções adicionais podem ser adicionados.

Especial atenção deve ser dada à relação entre segurança da informação e TI nas corporações. Nos casos em que a segurança da informação se reporta diretamente à TI, pode haver conflito de interesses. A TI, por sua natureza, presta serviço à organização, enquanto a segurança da informação gerencia o risco relacionado à proteção de informações. Essa dicotomia poderia levar a TI a substituir práticas de segurança da informação em nome do serviço ao cliente. Portanto, deve ser estabelecido certo grau de independência entre TI e segurança da informação.

É importante notar que a posição da(s) função(ões) de segurança da informação na organização é fator-chave para determinar a capacidade da organização de proteger as informações. Esse posicionamento pode ser a diferença entre segurança da informação proativa, alinhada com iniciativas empresariais, e simples adendo, em que risco deve ser mitigado, limitando, assim, muitas vezes, as opções de tratamento de riscos.

O conselho de administração exerce a responsabilidade final para todas as questões, incluindo segurança da informação. Essa responsabilidade pode e deve ser delegada ao nível adequado dentro da empresa. Considerando que segurança da informação é questão crítica de negócio, a organização deve sempre atribuir a responsabilidade final sobre segurança da informação ao membro sênior da gerência executiva, evitando, assim, provável exposição do conselho a alegações de negligência pelos órgãos reguladores ou outras partes interessadas, na eventual ocorrência de incidentes.

A decisão real para delegar responsabilidade geral depende da situação específica da companhia. As vantagens e desvantagens a considerar na

decisão para determinar a potencial função para relatórios de segurança da informação são as seguintes:

- CEO – Riscos de informação são elevados ao nível mais alto na corporação. Riscos de informação devem ser apresentados em formato compreensível para o CEO. Dada à multiplicidade de atribuições do CEO, riscos de informação podem ser monitorados e gerenciados em nível muito alto de abstração ou podem não ser plenamente compreendidos em seus detalhes relevantes;

- Chief Information Officer (CIO) – Questões de segurança da informação e soluções podem ser alinhadas com iniciativas de TI. Riscos de informação podem não ser tratados devido a outras iniciativas de TI e os prazos terem precedência sobre segurança da informação. Há potencial conflito de interesses, pois o trabalho realizado pelos profissionais de segurança da informação pode estar focado em TI e não em segurança da informação, isto é, pode haver foco insuficiente no negócio;

- Chief Financial Officer (CFO) – Questões de segurança da informação podem ser abordadas a partir do ponto de vista de impacto nas finanças dos negócios. Riscos de informação podem não ser tratados devido a iniciativas financeiras e prazos terem precedência sobre segurança da informação, havendo potencial conflito de interesses;

- Chief Risk Officer (CRO) – Riscos de informação são elevados à posição que pode considerar risco também pelas perspectivas estratégicas, operacionais, financeiras, de reputação e de conformidade. Este papel não existe na maioria das organizações, sendo mais frequentemente encontrado em instituições de serviços financeiros. Nas corporações em que o CRO não está presente, as decisões de risco organizacional podem ser decididas pelo presidente ou conselho de administração;

- Chief Technology Officer (CTO) – “Diretor de tecnologia” (em tradução livre). A segurança da informação pode ser parceira e incluída em futuros roteiros tecnológicos. Riscos de informação podem não ser tratados em razão de as direções tecnológicas terem precedência sobre segurança da informação;

- Chief Operating Officer (COO) – Questões de segurança da informação e soluções podem ser abordadas do ponto de vista do impacto para operações comerciais. Riscos de informação podem não ser tratados em razão de as iniciativas operacionais e os prazos terem precedência sobre a segurança da informação;

- Conselho de Administração (relatório indireto) – Riscos de informação são elevados ao nível mais alto na corporação, e devem ser apresentados em formato compreensível pelos membros do conselho e, portanto, pode tornar o nível muito alto para ser relevante.

3.3.7 O facilitador Cultura, Ética e Comportamento

O comportamento dos indivíduos e das corporações é, muitas vezes, subestimado como fator de sucesso na governança e gestão de segurança da informação.

Cultura, Ética e Comportamento pode ser estruturado de acordo com as dimensões, anteriormente citadas.

No COBIT 5 for Information Security, há modelo do processo mostrando os diferentes componentes da Cultura, Ética e Comportamento, o qual é extensão do modelo genérico facilitador.

O modelo de cultura, ética e comportamento indica que:

- A Cultura, Ética e Comportamento das partes interessadas compreende toda a corporação e também intervenientes externos, como agências reguladoras, auditores externos e órgãos de supervisão;
- O suporte é duplo: Partes interessadas, por exemplo, jurídico, gestores de risco, gestores de RH, conselho de remuneração e funcionários, tomadores de decisão, implementadores e aplicadores de comportamentos desejados; e outros que precisam se alinhar com regras e normas definidas;
- Por conseguinte, ao influenciar a cultura, ambas as partes interessadas necessitam ser consideradas. Por exemplo, funcionários internos precisam estar cientes da situação de segurança da informação, assim como consultores externos, fornecedores e outras partes externas.
- As metas para esse facilitador relacionam-se à ética organizacional, determinada pelos valores que a organização quer viver, à ética individual, determinada pelos valores pessoais de cada indivíduo na empresa, e a comportamentos individuais;
- Culturas organizacionais, postura ética, comportamentos individuais, etc. têm ciclos de vida. A partir da cultura existente, a organização pode identificar mudanças necessárias e trabalhar para sua implementação. Diversas ferramentas descritas em boas práticas podem ser usadas;
- Boas práticas para criar, incentivar e manter o comportamento desejado em toda a empresa incluem:
    - Comunicação em toda a organização de comportamentos desejados e os valores empresariais subjacentes;

- A consciência do comportamento desejado, reforçada pelo exemplo de comportamento exercido pela direção e por outros líderes;
- Incentivos para encorajar e impedimentos para impor comportamentos desejados, regras e normas, que forneçam mais orientações sobre o comportamento organizacional desejado e a ligação muito clara com os princípios e políticas da corporação colocadas no lugar.

O comportamento humano é um dos principais fatores que determinam o sucesso do empreendimento, e o dos membros da corporação coletivamente determina a cultura empresarial.

Muitos fatores conduzem o comportamento. Há os externos, como crenças, etnia, situação socioeconômica, localização geográfica e experiências pessoais; e relações interpessoais nas companhias, objetivos e ambições pessoais.

A cultura é definida em BMIS como padrão de comportamentos, crenças, suposições, atitudes e maneiras de fazer as coisas. A publicação Creating a Culture of Security da ISACA amplia a liderança de pensamento em torno da cultura e da segurança da informação e descreve que toda corporação possui cultura de segurança da informação. Na maioria dos casos, não há intenção e consistência, na medida de sua existência no todo; em outros, é robusta e orienta as atividades diárias de funcionários e outras pessoas que entram em contato com a corporação.

A cultura transcende a corporação e evolui no tempo. Comportamentos são adaptados e consciência cultural em relação à segurança da informação pode aumentar ou diminuir. É importante compreender a cultura existente, de modo que alterações positivas possibilitem que a cultura de segurança possa ser feita. Existem muitas metodologias de aferição para estimar a cultura corporativa e, além de medi-la, a efetividade das medidas de segurança da informação também deve ser examinada para avaliar a cultura de segurança subjacente.

Para uma visão adequada da cultura de segurança da informação, comportamentos dos intervenientes precisam ser medidos ao longo do tempo. Exemplos de tais medições incluem:

- Força de senhas;
- Uso do cartão de Passe (crachá);
- Número de travas de equipamentos móveis, como laptop, distribuídos e utilizados por colaboradores;
- Discussão pública/aberta de informação confidencial;
- Falta de abordagem de segurança, como compartilhamento de senhas, utilização não autorizada, etc.;
- Proteção de senha do usuário na prática;
- Adesão ao sistema e às práticas de gerenciamento de mudanças de aplicativos;
- Conclusão de registros e de prestação de contas de visitantes;
- Porcentagem de apropriada marcação e rotulagem de informação (cópia eletrônica e impressa).

Como dados estáticos, essas métricas têm pouco valor, pois só quando a evolução ao longo do tempo é examinada, podem essas métricas simples fornecer mecanismo de avaliação sólido para a cultura de segurança da informação.

Para influenciar a cultura, a corporação precisa de defensor para realizar mudanças na organização. Patrocinadores são aqueles que estão ansiosos para falar e servir de exemplo para outros. Defensores podem ser altos executivos da organização, mas a atividade não se limita a esse grupo dentro da organização. Os membros da equipe podem ser patrocinadores, enquanto ativamente fornecem o pano de fundo para mudança e cumprimento da cultura.

A Creating a Culture of Security fornece número de candidatos comuns que podem servir como patrocinador de segurança da informação:

- Gestores de risco;
- Profissionais de segurança da informação;
- Executivos de nível C: CEO, COO, CFO ou CIO;
- Chefe de RH.

A liderança, os tomadores de decisão, neste contexto de segurança da informação, pode ser igualmente importante. Defensores são necessários para influenciar a liderança na tomada de decisões, considerando os requisitos de segurança da informação. É óbvio que a liderança e os patrocinadores podem sobrepor-se, no entanto, eles são mencionados em contexto diferente. A liderança é classificada como:

- Gerência executiva;
- Gestão de negócios;
- CISO/ISM.

Comportamentos desejáveis identificados, que influenciam positivamente a cultura para a segurança da informação e sua aplicação efetiva na vida cotidiana, incluem:

- A segurança da informação ser praticada nas operações diárias;
- As pessoas respeitarem a importância das políticas e princípios de segurança da informação;
- A orientação de segurança da informação suficiente e detalhada ser fornecida às pessoas, as quais são incentivadas a participar e questionar a situação de segurança da informação atual;
- Todos serem responsáveis pela proteção de informações dentro da organização;

- As partes interessadas estarem cientes de como identificar e responder às ameaças para o empreendimento;
- A gestão proativa suportar e antecipar inovações de segurança da informação e comunicar à corporação. A companhia ser receptiva para explicar e lidar com novos desafios de segurança da informação;
- A gestão de negócios envolver, em colaboração interfuncional contínua, a fim de permitir eficientes e eficazes programas de segurança da informação;
- A gerência executiva reconhecer o valor de segurança da informação para os negócios.

Para cada comportamento definido, os seguintes atributos são descritos nesse guia:

- Ética organizacional - determinada pelos valores pelos quais a corporação quer viver;
- Ética individual - determinada pelos valores pessoais de cada indivíduo na companhia e, em grande medida, dependem de fatores externos, tais como crenças, etnia, situação socioeconômica, localização geográfica e experiências pessoais;
- Liderança - maneiras que a liderança pode influenciar o comportamento desejado:
    - Como a comunicação, a aplicação e as regras e normas podem ser usadas para influenciar o comportamento;
    - Incentivos e recompensas podem ser usados para influenciar o comportamento.
    - Sensibilização.

Mais informações detalhadas sobre a cultura de segurança da informação podem ser encontradas em BMIS e em Creating a Culture of Security.

3.3.8 O facilitador Informação

Esse facilitador contém orientações sobre como a informação embutida na organização pode ser usada para governar e gerir a segurança da informação dentro da corporação.

A informação é generalizada em todas as empresas e é necessária para manter a organização funcionando e bem governada. No nível operacional, a informação é muitas vezes o produto-chave do empreendimento.

Informação, e por consequência a comunicação, não é apenas o principal tema de segurança da informação, mas também elemento essencial para a segurança da informação. Informação como facilitador de segurança da informação significa que a administração pode utilizar a informação como base de decisão. Por exemplo, o ISSC pode usar o perfil de segurança da informação para desenvolver estratégia de segurança da informação.

No COBIT 5 for Information Security há modelo que define em alto nível os diferentes componentes da informação, o qual é extensão do modelo genérico facilitador.

O modelo de informação indica que:

- As partes interessadas internas e externas devem ser identificadas e suas principais áreas de responsabilidade definidas, ou seja, a informação deve ser clara acerca da razão de eles se preocuparem, ou estarem interessados;
- Os objetivos da informação são divididos em três subdimensões de qualidade:
    - Qualidade intrínseca – medida que os valores de dados estão em conformidade com os valores reais ou verdadeiros;
    - Qualidade contextual e representacional – medida que a informação é aplicável à tarefa do usuário da informação e é apresentada de forma inteligível e clara, reconhecendo que a qualidade da informação depende do contexto de uso;

- Qualidade de segurança/acessibilidade - medida que a informação está disponível ou que possa ser obtida.

- O ciclo de vida completo de informações precisa ser considerado e abordagens diferentes podem ser necessárias para obter informações em diferentes fases do ciclo de vida, como planejar, projetar, construir/adquirir, utilizar/operar, controlar e eliminar;

- Boas práticas definem informação como consistindo de seis camadas, apresentando atributos contínuos que vão desde o aspecto físico da informação, em que atributos estão ligados às tecnologias de informação e meios de comunicação – como captura, armazenamento, processamento, distribuição e apresentação da informação –, até a abordagem social, como uso da informação, senso de decisão e ação.

A lista a seguir contém exemplos de tipos de informações que são comuns no contexto de governança e gestão de segurança da informação. Esses tipos de informações variam de estratégia até painel operacional, cada qual com seu específico propósito na governança e gestão de segurança da informação. Ela não pretende ser exaustiva, e sim dar ideia de quão profundo a segurança da informação se estende por toda a organização. Dependendo da companhia, essa lista pode precisar ser estendida ou limitada. Exemplos de tipos de informação são:

- Estratégia de segurança da informação;
- Orçamento da segurança da informação;
- Plano de segurança da informação;
- Políticas;
- Requisitos de segurança da informação, que podem incluir:
    - Requisitos de configuração de segurança da informação;

- Service level agreement (SLA)/operating level agreement (OLA) – “Acordo de Nível de Serviço/acordo de nível operacional” (em tradução livre), respectivamente, para requisitos de segurança da informação.

- Material de sensibilização;
- Relatórios de avaliação de segurança da informação, que incluem:
  - Constatações de auditoria em segurança da informação;
  - Relatório de maturidade da segurança da informação;
  - Gestão de risco de segurança da informação:
- Análise de ameaças;
- Relatórios de avaliação de vulnerabilidade de segurança da informação.
- Catálogo de serviços de segurança da informação;
- Perfil de risco da informação, que inclui:
  - Registro de risco de informações;
  - Relatórios de violações e perdas, ou relatório consolidado de incidente.
- Painel de segurança da informação, ou equivalente, que inclui:
  - Incidentes de segurança da informação;
  - Problemas de segurança da informação;
  - Métricas de segurança da informação;

Para cada tipo de informação, a orientação mais detalhada é fornecida nesse guia, incluindo:

- Objetivos – descrições de série de metas a serem alcançadas, utilizando as três categorias definidas no modelo de informação;

- Ciclo de vida – a descrição específica dos requisitos de ciclo de vida, além de abordagem geral, conforme descrito no ciclo de vida da informação;

- Boas práticas para este tipo de informação – a descrição do conteúdo e estrutura típicos.

Identificar intervenientes de informação é essencial para aperfeiçoar desenvolvimento e distribuição de informações em toda a companhia. O guia fornece abordagem para resumir criadores e destinos de cada tipo de informação comum.

Por exemplo, as partes interessadas em informações relacionadas à segurança da informação dentro de empresa típica podem ser estruturadas, incluindo:

- Descrição de partes interessadas – versão simplificada da lista genérica de estruturas organizacionais de COBIT 5, complementada com série de partes interessadas externas adicionais para esse domínio específico;

- Tipos de informação, conforme descrito acima;

- Indicação da natureza do relacionamento da parte interessada para cada tipo de informação:

    - A – Aprovador;
    - O – Originador;
    - I – Informado do tipo de informação;
    - U – Usuário do tipo de informação.

Modelo contendo tipos de informação e potenciais interessados com base no COBIT 5 está disponível nesse guia.

Informações de tipos específicos de segurança de informação, tais como os exemplos apresentados acima, também estão vinculadas por ciclo de vida. Além disso, a função de segurança da informação tem importante papel facilitador para atuar neste ciclo de vida. Essa dualidade no contexto da informação, como

facilitador do ciclo de vida e de usuário de informações, leva à crescente importância da segurança da informação dentro da corporação.

A gestão do conhecimento está descrita no processo BAI08 Enabling Processes – “Ativação de Processos” (em tradução livre) – do COBIT 5. Esse processo elabora, no ciclo de vida, que a informação é necessária para resultar a ser segura e eficientemente administrada na companhia. O ciclo de vida completo de informação precisa ser considerado para garantir sua correção e utilização aperfeiçoada. Além disso, diferentes abordagens podem ser necessárias para a informação em diferentes fases do ciclo de vida. As seguintes fases podem ser distinguidas:

- Planejar/projetar/construir/adquirir – as informações são identificadas, adquiridas e classificadas nessa fase. Atividades nessa fase podem referir-se a desenvolvimento de padrões e definições, por exemplo, definições e procedimentos de coleta de dados; a criação de registros de dados, a aquisição de dados e a carga de arquivos externos.
- Utilizar/operar - Essa fase inclui:
    - Armazenar – a fase em que a informação é mantida eletronicamente ou em cópia impressa, ou mesmo apenas na memória humana. Atividades nessa fase podem referir-se ao armazenamento de informação em formato electrônico, por exemplo, arquivos eletrônicos, bases de dados, *data warehouses* – “armazéns de dados” (em tradução livre) –, ou em cópia impressa, por exemplo, documentos em papel.
    - Compartilhar – a fase em que a informação é disponibilizada para uso por meio de método de distribuição. Atividades nessa fase podem referir-se aos processos envolvidos na obtenção de informações para locais onde podem ser acessados e utilizados, por exemplo, distribuição de documentos por correio eletrônico (*e-mail*). Para obter informações mantidas

eletronicamente, essa fase do ciclo de vida pode, em grande parte, coincidir com a fase de armazenamento, por exemplo, o compartilhamento de informação por meio do acesso a banco de dados, servidores de arquivos/documentos.

- Usar – a fase em que a informação é usada para atingir objetivos. Atividades nesta fase podem referir-se a diferentes tipos de uso da informação, por exemplo, tomada de decisão gerencial, a execução de processos automatizados, e pode também incluir atividades como recuperação de informação e conversão de informações de uma forma para outra.

- Monitorizar – a fase em que é assegurado que a fonte de informação continua a funcionar corretamente, isto é, continua a ser útil. Atividades nesta fase podem referir-se a manter as informações atualizadas, bem como outros tipos de atividades de gerenciamento de informações, por exemplo, aumento, limpeza, fusão e remoção de dados de informações duplicadas em *data warehouses*.

- Eliminar – a fase em que a fonte de informação é descartada quando já não é útil. Atividades nessa fase podem se referir a informações de arquivamento ou destruição.

As fases do ciclo de vida de informações estão alinhadas com as práticas do processo BAI08. A descrição específica dos requisitos do ciclo de vida e a abordagem geral são fornecidas na orientação detalhada desse guia.

3.3.9 O facilitador Serviços, Infraestrutura e Aplicações

Serviços, Infraestrutura e Aplicações fornece informações, processamento e serviços de informações à organização, podendo ser estruturado de acordo com dimensões, anteriormente citadas.

No COBIT 5 for Information Security, há modelo do processo mostrando, em alto nível, os diferentes componentes de serviços, infraestrutura e aplicações, o qual é extensão do modelo genérico facilitador.

O modelo de serviços, infraestrutura e aplicações indica que:

- Capacidades de serviço, isto é, prazo combinado para serviços, infraestrutura e aplicações, às partes interessadas podem ser internas e externas. Os serviços podem ser entregues por partes internas ou externas, por exemplo, departamentos internos de TI, gestores de operações e prestadores terceirizados; e usuários de serviços também podem ser internos, por exemplo, usuários de negócios; e externos à corporação, por exemplo, parceiros, clientes e fornecedores. Os suportes de cada parte interessada precisam ser identificados e focar sobre a prestação de serviços adequados ou na recepção de serviços solicitados de fornecedores;

- Objetivos da capacidade de nível de serviço são expressos em termos de serviços, aplicações, infraestrutura e tecnologia, e níveis de serviço, considerando-se quais serviços e níveis de serviço são mais econômicos para a companhia. Mais uma vez, os objetivos se relacionam aos serviços e como eles são fornecidos, bem como os seus resultados, ou seja, a contribuição para os processos de negócio suportados com sucesso;

- Capacidades de serviços têm ciclo de vida. As capacidades de serviços futuros ou planejadas são geralmente descritas na arquitetura-alvo. Abrange blocos de construção, tais como aplicações futuras e do modelo de infraestrutura alvo, e também descreve as ligações e relações entre esses blocos de construção;

- Boas práticas para capacidades de serviço incluem:

    - Definição de princípios de arquitetura, diretrizes gerais que regem aplicação e utilização dos recursos relacionados à TI dentro da corporação;

- Definição de visão mais adequada da arquitetura, para atender às necessidades dos diferentes *stakeholders*;
- Posse de repositório de arquitetura, que pode ser utilizado para armazenar diversos tipos de saídas arquitetônicas, e níveis de serviço que precisam ser definidos e realizados pelos prestadores de serviços.

Boas práticas externas para arcabouços de arquitetura e capacidades de serviço existente são orientações, modelos ou padrões que podem ser usados para acelerar a criação de arquitetura de entregas.

Capacidades de serviço são requeridas para fornecer segurança da informação e funções relacionadas à corporação. Serviços exigem infraestrutura e aplicações apropriadas, e também são fornecidos por meio de combinação de outros facilitadores, como processos, informação e estruturas organizacionais.

A lista a seguir contém exemplos de potenciais serviços relacionados à segurança, como podem aparecer em catálogo de serviços. Normalmente, esses serviços ligam-se a processos do COBIT 5 e a suas práticas e atividades, e solicitam informações, entradas e saídas, e estruturas organizacionais, como gráficos RACI, funções ou papéis específicos de segurança. Ela fornece visão orientada a serviços em atividades relacionadas com segurança, e não tenciona duplicar ou reproduzir processos de segurança:

- Fornecer arquitetura de segurança;
- Proporcionar conscientização da segurança;
- Proporcionar o desenvolvimento seguro, desenvolvimento em consonância com normas de segurança;
- Fornecer avaliações de segurança;
- Fornecer sistemas adequadamente protegidos e configurados, de acordo com requisitos e arquitetura de segurança;
- Proporcionar acesso de usuários e direitos de acesso em conformidade com requisitos de negócio;

- Fornecer proteção adequada contra *software* malicioso, como *malware*, ataques externos e tentativas de intrusão;
- Fornecer resposta adequada a incidentes;
- Fornecer testes de segurança;
- Fornecer serviços de monitoramento e de alerta para eventos relacionados à segurança.

Para cada capacidade de serviço, os blocos de construção de serviços têm sido descritos nesse guia:

- A descrição detalhada do serviço, fornecendo funcionalidade de negócios;
- Atributos, descrevendo para cada serviço entradas e tecnologias de suporte, incluindo aplicações e infraestrutura;
- Objetivos, que descrevem a qualidade e as metas de conformidade para cada capacidade de serviço e métricas relacionadas;

3.3.10 O facilitador Pessoas, Habilidades e Competências

As pessoas têm de demonstrar habilidades e competências necessárias para assegurar que atividades sejam concluídas com êxito e decisões corretas sejam tomadas.

Pessoas, Habilidades e Competências pode ser estruturado de acordo com dimensões, anteriormente citadas.

No COBIT 5 for Information Security, há modelo do processo mostrando diferentes componentes de pessoas, habilidades e competências, o qual é extensão do modelo genérico facilitador.

O modelo de Pessoas, Habilidades e Competências indica que:

- Diferentes partes interessadas podem assumir diferentes papéis, por exemplo, gerente de negócios, gerente de projeto, parceiro, concorrente, recrutador, treinador, desenvolvedor

especialista técnico de TI, ISM, CISO e regulador, e cada papel exige um conjunto de habilidades distintas;

- Metas para habilidades e competências se relacionam com níveis de educação e qualificação, habilidades técnicas, níveis de experiência, conhecimento e habilidades comportamentais necessárias para fornecer com sucesso e executar atividades de processos, papéis organizacionais, etc. Metas para pessoas incluem níveis corretos de disponibilidade de pessoal e taxa de rotatividade;

- Habilidades e competências têm ciclo de vida. A corporação deve saber qual é sua base de habilidade atual e o plano para o que ele precisa vir a ser, sendo influenciada, entre outros fatores, pela estratégia e pelos objetivos da organização. Habilidades precisam ser desenvolvidas, por exemplo, por meio da formação; adquiridas, por exemplo, por meio do recrutamento; e implantadas em funções dentro da estrutura da organização e podem precisar ser eliminadas, por exemplo, se a atividade é automatizada ou terceirizada. Periodicamente, a companhia deve avaliar a base de competências para compreender a evolução ocorrida;

- Boas práticas de habilidades e competências incluem a necessidade de definir os requisitos de habilidades objetivas para cada papel assumido pelas diversas partes interessadas, podendo ser descritos por meio de diferentes níveis em distintas categorias de habilidades, para os quais a definição de qualificações deve estar disponível. As categorias de habilidades correspondem às atividades realizadas relacionadas à TI, neste caso, às funções relacionadas com a segurança da informação.

Esse guia descreve habilidades e competências para o nível de habilidade mais ideal possível. Na realidade, no entanto, nem sempre as corporações podem requerer o nível de habilidade excelente ou ser capazes de utilizar recursos que demonstrem nível ótimo de habilidade.

Para operar de forma eficaz a função de segurança da informação dentro da organização, indivíduos com conhecimentos e experiência adequados, por exemplo, habilidades e competências, devem exercer essa função.

Abaixo habilidades e competências típicas relacionadas com segurança são listadas: governança de segurança da informação; formulação da estratégia de segurança da informação; gestão de riscos da informação; desenvolvimento da arquitetura de segurança da informação; operações de segurança da informação; avaliação e testes e conformidade da informação.

Embora essas habilidades também possam se traduzir em posição específica em grandes corporações, por exemplo, habilidades de arquitetura de segurança da informação, podem igualar a posição de arquiteto de segurança da informação, não sendo o caso, às vezes, em pequenas empresas.

Para cada habilidade e competência acima referenciada, os seguintes atributos são descritos nesse guia:

- Definição de habilidade;
- Objetivos - conforme definido anteriormente;
- Facilitadores relacionados – habilidades e competências são necessárias para realizar atividades do processo e tomar decisões em estruturas organizacionais. Por outro lado, processos visam apoiar o ciclo de vida de habilidades e competências.

Atributos para habilidades e competências alinhadas com análises práticas de certificações como CISA, CISM, CGEIT e CRISC da ISACA, e Certified Information System Security Professional (CISSP) da (ISC)2, acrescentam valor à segurança da informação. A certificação CISM ou designação equivalente é sugerida para habilidades definidas anteriormente, pois certificação é meio objetivo de prova a empregadores de que profissionais têm conhecimento básico adequado dentro do tema de domínio.

Habilidades e competências seguem ciclo de vida. A função de segurança da informação deve identificar sua base de habilidade atual e alinhar essa base de competências para o conjunto de habilidades necessárias, sendo influenciada por, entre outros assuntos, estratégia e objetivos de segurança da

informação. Existem habilidades a serem desenvolvidas, por exemplo, por meio de sala de aula e treinamento prático (*hands-on*); ou adquiridas, por exemplo, por meio do recrutamento; e implantadas em funções dentro da estrutura. Habilidades podem precisar ser realinhadas se, por exemplo, a atividade é automatizada ou terceirizada. Periodicamente, por exemplo, em base anual, a corporação precisa avaliar a sua base de competências para compreender a evolução que ocorreu, a qual alimenta processo de planejamento para próximo período. A avaliação também pode alimentar processo de reconhecimento e recompensa para recursos humanos.

Nota: Atributos que descrevem habilidades e competências são conjuntos de critérios e não descrição prescritiva do trabalho. Decisões de ocupação devem ser feitas nos fatores descritos anteriormente, juntamente com ajuste global do indivíduo na corporação.

4 O ESTÁGIO ATUAL DA SEGURANÇA DA INFORMAÇÃO NO SENADO FEDERAL

4.1 O SENADO – ESTRUTURA, PROCESSO LEGISLATIVO E FUNÇÕES

O corpo funcional dessa Casa é composto por mais de seis mil servidores, entre efetivos e comissionados, mais de dois mil funcionários terceirizados e mais de três centenas de estagiários.

Os senadores compõem quase duas dezenas de comissões, entre temporárias e permanentes. O Senado também conta com mais de uma dezena de conselhos que auxiliam em discussões e na produção legislativa.

Conforme o Portal Transparência, de modo geral, as funções legislativas do Senado Federal são descritas na Constituição Federal, principalmente no art. 52, como: processar, julgar e escolher autoridades, além de autorizar operações financeiras públicas, incluindo dívida.

Baaklini (1993, p. 113), no livro “O Congresso e o Sistema Político no Brasil”, argumenta sobre a alta relevância da informação para os processos críticos do Legislativo Federal, e um capítulo desse texto é dedicado ao principal fornecedor de serviços de TI para o Senado Federal, a saber, a então empresa e hoje secretaria Prodasen:

> A necessidade de reagir de forma adequada e no momento certo aos problemas da sociedade exige que o Congresso fortaleça sua capacidade informacional. As informações [...] permitem ao Congresso responder às iniciativas do presidente, participar em pé de igualdade com o Executivo na introdução de políticas públicas, escapar da influência dos grupos de interesses e responder às preocupações do eleitorado.

4.2 A GESTÃO DE RISCOS NO SENADO FEDERAL

O Senado Federal produz, processa, armazena e transmite informações, as quais tem muito valor, e há motivos plausíveis para que elas sejam protegidas por todos.

A governança corporativa de sistemas de informação (SI), assim como os riscos organizacionais, está no escopo temático do Sistema de Governança Corporativa e Gestão Estratégica do Senado, conforme o art. 3º do Ato do Primeiro Secretário (APS) n. 16/2011, que o instituiu, além de recomendações, por meio de acórdãos do Tribunal de Contas da União (TCU) sobre SI.

Em junho de 2013, conforme mensagem veiculada na intranet do Senado Federal, a Comissão Diretora aprovou, por meio do ATC 16/2013, a instituição da Política de Gestão de Riscos Organizacionais, a qual foi elaborada com ampla consulta aos órgãos da Casa, com o objetivo de minimizar vulnerabilidades diante de cenários imprevistos e em especial, negativos.

É preciso considerar que essa política é instrumento importante para facilitar a integração de iniciativas relacionadas à gestão de riscos organizacionais e à segurança corporativa, possibilitando promover maior garantia do cumprimento de objetivos estratégicos do Senado Federal.

É essencial a existência dessa política para que processos organizacionais críticos da Câmara Alta tenham planos de continuidade operacional. A incorporação dessa política refletirá na maturidade e na profissionalização da condução da gestão do Senado Federal.

A segurança e os riscos de informação são explicitados nessa política, determinando que o modelo de segurança de informação deva assegurar disponibilidade, integridade e preservação das informações; que o acesso a elas seja decorrência da relação funcional e da necessidade de conhecer; e obrigando a todos com acesso aos dados do Senado Federal.

As diretrizes desse documento oferecem efetividade ao Mapa Estratégico Institucional do Senado Federal para o período de 2013-2023, o qual estabeleceu, de maneira expressa, a meta de aprimorar significativamente a gestão de riscos na administração da instituição.

No mesmo sentido, a Agenda Estratégica da Administração do Senado, instituída pela Comissão Diretora em 2011, constituiu o objetivo de implementar modelo de governança corporativa e gestão estratégica em que um dos escopos de atuação é a governança corporativa de riscos organizacionais.

Os princípios de segurança da informação comunicam regras corporativas em apoio aos objetivos de governança e aos valores organizacionais,

conforme definido pela alta administração. Esses princípios devem ser em número limitado e expressar os valores fundamentais da organização, em linguagem simples e declarativa, tão clara quanto possível.

4.3 A FUNÇÃO DE GESTÃO DE SEGURANÇA E RISCOS DE INFORMAÇÃO APLICADA AO PROCESSO LEGISLATIVO

A missão da função de segurança e riscos de informação no processo legislativo é prover e gerir soluções de proteção para as informações, referentes a esses processos, que a corporação produza, processe, armazene e transmita, as quais devem permanecer íntegras, disponíveis e com o seu grau sigilo resguardado.

Em sua origem, o Prodasen, de certa forma, já nasceu com esta missão. Esta afirmação decorre da obra de BAAKLINI – O Congresso e o Sistema Político do Brasil – quando diz:

> No dia 16 de outubro de 1970, o presidente do Senado nomeou um grupo de trabalho para estudar e preparar um relatório sobre a viabilidade do projeto de desenvolvimento de um centro de computação de grande porte ligado ao Congresso Nacional. (...) Em janeiro de 1971, o grupo de trabalho apresentou suas recomendações ao presidente do Senado. (...) A missão de tal centro era adquirir os recursos e as tecnologias necessárias para **coletar, processar, armazenar e recuperar as informações importantes para a melhoria da eficiência e eficácia do processo legislativo**. (Grifo do autor).

Assim, pode-se inferir que a missão do Prodasen seja prover e gerir soluções de tecnologia para as informações que o Senado produz, processa, armazena e transmite, as quais devem permanecer íntegras, disponíveis e com seu grau sigilo resguardado.

Para cumprimento dessas finalidades, pode-se recomendar que:

- Equipamentos destinados às atividades do Senado Federal, ao armazenamento e à recuperação de seus dados, ao desenvolvimento, à implantação, manutenção e operação de seus sistemas de informação, à implementação e operação de suas redes de comunicação de dados, a seu serviço de correio eletrônico e suas

funcionalidades complementares, sejam fornecidos por serviços de TI da própria Casa, incluindo comunicações realizadas por meio de serviço móvel pessoal e serviço telefônico fixo comutado;

- A Câmara Alta discipline e estabeleça procedimentos, abrangência e prazos de implementação, considerando peculiaridades de suas comunicações e sua capacidade de ofertar satisfatoriamente redes de computadores e seus serviços pertinentes;

- Admita-se auditoria para fins de verificação e aprimoramento contínuo da necessária gestão da segurança da informação e das comunicações, que proteja disponibilidade, integridade, confidencialidade e autenticidade de informações, em especial sua inviolabilidade.

4.4 A PESQUISA INTERNA COM GESTORES DE TI

Os gestores responsáveis pela governança e gestão de TI do Senado Federal participaram recentemente do levantamento de informações, nos planos estratégico, tático e operacional, sobre atividades empreendidas no desenvolvimento de sistemas, na infraestrutura e no planejamento da área de Tecnologia da Informação.

Esses administradores colaboraram fornecendo dados, por meio de formulário estruturado com questões objetivas, as quais admitiam uma única resposta entre cinco alternativas, a saber: a) Não se aplica; b) Não adota; c) Iniciou plano para adotar; d) Adota parcialmente; e) Adota integralmente. Essa pesquisa não compreendeu a obtenção de evidências comprobatórias dos retornos conseguidos.

Essas perguntas abordaram, inclusive, o domínio de segurança da informação. A análise de tendências (maiorias e agrupamentos) das respostas fornecidas sobre esse aspecto indica que a incorporação de boas práticas concernentes a políticas e responsabilidades, assim como a controles e atividades, é adotada pela maioria das unidades.

4.4.1 O Indicativo de boas práticas incorporadas

Os destaques positivos apurados nesse levantamento, quanto à adoção de boas práticas referentes à segurança da informação, são:

- Política de controle de acesso à informação e aos recursos e serviços de TI;
- Política de Cópias de segurança (backup);
- Processo de Gestão de Ativos;
- Processo de Gestão de Riscos de Segurança da Informação (exceto norma de cumprimento obrigatório);
- Processo de Gestão de Vulnerabilidades de TI (exceto norma de cumprimento obrigatório);
- Processo de Gestão de Incidentes de Segurança da Informação (exceto norma de cumprimento obrigatório);
- Classificação e tratamento de informações;
- Monitoramento do uso dos recursos de TI.

4.4.2 O Indicativo de boas práticas não incorporadas

Por outro lado, nessa pesquisa, pode-se considerar como aspectos contraproducentes relativos à adoção de boas práticas quanto à segurança da informação:

- Gestor de segurança da informação formalmente designado;
- Equipe de tratamento e resposta a incidentes de segurança da informação formalmente instituída;
- Formalização por norma de cumprimento obrigatório para:
    - Processo de Gestão de Riscos de Segurança da Informação;
    - Processo de Gestão de Vulnerabilidades de TI;

- Processo de Gestão de Incidentes de Segurança da Informação;
- Ações periódicas de conscientização, educação e treinamento para seus colaboradores.

4.4.3 A Pesquisa semelhante do TCU

Desde 2007, a Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), do Tribunal de Contas da União (TCU), vem, reiterada e periodicamente, realizando levantamento, a fim de acompanhar e manter base de dados atualizada, com a situação de governança de tecnologia da informação (TI) em instituições representativas de segmentos diversos da Administração Pública Federal (APF).

No tocante ao tema de segurança da informação, os resultados obtidos em 2012 demostram progresso na:

- Nomeação de funcionários para a gestão da segurança da informação;
- Formalização da política de segurança da informação (PSI).

Também se observa tendência crescente de organizações que têm o processo de classificação de informações. Há de se considerar o advento da Lei 12.527/2011, que regula o acesso a informações mantidas pelo Estado, haja vista que a ausência de classificação pode implicar tratamento inadequado da informação.

Por outro lado, revelou-se índice regressivo de adoção relacionado com os seguintes processos:

- Inventário de ativos de informação;
- Análise de riscos;
- Gerenciamento de incidentes de segurança da informação.

Dessa forma, pode-se avaliar que as respostas indicam capacidade inicial, com tendência à intermediária, quanto a controles sobre elementos críticos da gestão de segurança da informação, em linha com normas da família NBR ISO/IEC 27000 e acórdãos do TCU, como o Acórdão 1.603/2008 – Plenário, especialmente o item 9.1.3.

4.5 OS NORMATIVOS NACIONAIS

Ressalta-se que o Brasil não conta com ato legal exclusivo para tratamento de segurança da informação, e do conjunto de sua legislação diversos podem ser aplicados nesse contexto.

4.5.1 A legislação e a Administração Pública Federal

Há a Lei 9.983, de 14 de julho de 2000, cujo artigo 313-A trata da inserção de dados falsos em sistema de informações, e o artigo 313-B, da modificação ou alteração não autorizada de sistema de informações.

A Medida Provisória 2.200, de 28 de Junho de 2001, institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

O Decreto 3.505, de 13 de junho de 2000, institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

O Decreto 4.553, de 27 de dezembro de 2002, dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.

Além desses, existem dispositivos infralegais, tais como instruções normativas da Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão (MPOG) e normas complementares do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Por exemplo, a gestão de riscos de segurança da informação e comunicações é normatizada, no Poder Executivo Federal do Brasil por meio da Norma Complementar 04/IN01/DSIC/GSI/PR.

4.5.2 O regramento no Senado Federal

A Política de Gestão de Riscos Organizacionais do Senado Federal, como anteriormente mencionado, foi instituída pelo Ato da Comissão Diretora (ATC) 16/2013.

Segundo o Regulamento Administrativo do Senado Federal (RASF), ao Escritório de Governança e Gestão Estratégica compete coordenar as ações técnicas de gestão de riscos organizacionais e segurança corporativa (RASF, art. 256 do ATC 8/2014). Adiciona ainda o RASF a incumbência aos Escritórios Setoriais de Gestão de colaborar na formulação das estratégias, políticas, diretrizes e ações corporativas, incluindo as relacionadas aos temas de segurança da informação, assim como de assessorar a unidade à qual se subordina, no seu âmbito de atuação e quando pertinente, na gestão de riscos e da segurança da informação (RASF, § 4º do art. 256 do Ato da Comissão Diretora - ATC 8/2014).

Demais regulamentos atinentes:

- Acesso e uso da internet e das redes sociais por meio da Rede do Senado Federal (Ato do 1º-Secretário - APS n. 14/2011).
- Uso e administração do sistema de correio eletrônico do Senado Federal (APS n. 6/2010).
- Uso e administração dos recursos computacionais e da rede do Senado Federal (APS n. 54/2009).
- Uso e administração do serviço de acesso à rede sem fio nas dependências do Senado Federal (APS n. 7/2008).
- Uso e administração do serviço de acesso remoto da rede local do Senado Federal – SARE, baseado na tecnologia VPN (VIRTUAL PRIVATE NETWORK) (APS n. 25/2003).

4.5.3 Os Acórdãos do Tribunal de Contas da União

Entre as recomendações do Tribunal de Contas da União (TCU), podem-se destacar:

- Implementar gestão de segurança da informação (Acórdão TCU 1.603/2008 - Plenário);
- Implementar e aperfeiçoar gestão de riscos de TI (Acórdãos TCU 1.603/2008 e 2471/2008 - Plenário);
- Aculturar sistematicamente os servidores da organização quanto à segurança da informação (Acórdão TCU 2471/2008 - Plenário).

4.5.4 A Norma ABNT NBR ISO/IEC 27001:2006

Segundo a Norma ABNT NBR ISO/IEC 27001:2006, a direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de claro direcionamento, demonstrando seu comprometimento, definindo atribuições de forma explícita e reconhecendo responsabilidades pela segurança da informação.

Por essa mesma norma, atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes. Ainda, indica a norma que responsabilidades pela segurança da informação devem estar claramente definidas.

Acrescenta que o enfoque da organização para gerenciar segurança da informação e sua implementação – como controles, objetivo dos controles, políticas, processos e procedimentos para segurança da informação – deve ser analisado criticamente, de forma independente, em intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

E finaliza que a direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem segurança da informação conforme estabelecido em políticas e procedimentos da organização.

4.6 A GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO EM OUTROS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

4.6.1 A gestão de riscos de segurança da informação no Judiciário Federal

O Conselho da Justiça Federal (CJF) instituiu, por meio da Resolução n. 6, de 7 de abril de 2008, a Política de Segurança da Informação do Conselho e da Justiça Federal de primeiro e segundo graus.

Para tanto, tomou como referências as normas ABNT NBR ISSO/IEC 27005:2008 e 31000:2009, além do documento do Gabinete de Segurança Institucional da Presidência da República intitulado “Gestão de Riscos de Segurança da Informação e Comunicações”.

A política instituída no âmbito do Judiciário abrange conceitos e definições, princípios e diretrizes, procedimentos e responsabilidades.

Destaca-se, na política, a diretriz que confere ao processo de gestão de riscos de SI caráter contínuo e permanente, alinhado ao modelo de melhoria contínua (Plan-Do-Check-Act - PDCA).

Também são definidas responsabilidades, cabendo à alta administração dos órgãos ligados ao CJF a aprovação dos respectivos processos de gestão de riscos de segurança informacional.

Por fim, cria rede de Comissões Locais de SI (CLSI) para coordenar ações de gestão de riscos no âmbito do judiciário federal.

4.6.2 A gestão de riscos de segurança da informação no Executivo Federal

No âmbito do poder executivo federal, a coordenação da gestão de riscos de SI está a cargo do Gabinete da Segurança Institucional da Presidência da República (GSI/PR).

Como já citado, desde o ano 2000, com a edição do Decreto n. 3.505, a Administração Pública Federal teve instituída sua política de segurança da informação, com abrangência para todos os ministérios e entidades da Administração Direta Federal.

A norma jurídica em comento definiu objetivos e responsabilidades de cada partícipe no processo de gestão de riscos de segurança informacional, deixando a cargo do Conselho de Defesa Nacional a normatização e fiscalização da execução da política no âmbito do executivo federal.

Para tal, instituiu o Comitê Gestor da Segurança da Informação, como órgão auxiliar desse conselho na consecução dos objetivos da política.

Esse comitê é integrado por representante de cada Ministério e de órgãos do Executivo Federal, designados pelo chefe do GSI/PR.

4.6.3 A gestão de riscos de segurança da informação na Câmara dos Deputados

No âmbito da Câmara dos Deputados, a política de segurança informacional foi instituída em 2012, com o Ato da Mesa n. 47, de 16 de julho daquele ano.

A política abrange todos os usuários de conteúdos informacionais e de recursos de tecnologia da informação providos pela Câmara.

Compreende um conjunto de princípios, objetivos, diretrizes e requisitos e define atribuições e instrumentos de gestão da segurança da informação naquela Casa legislativa.

Cria, a exemplo do Poder Executivo, o Comitê Gestor de Segurança da Informação (CGSI), composto por servidor representante de diversas áreas da Câmara, coordenado alternadamente, a cada dois anos, pelo Centro de Documentação e Informação e pelo Centro de Informática.

O CGSI fica encarregado de implantar e revisar periodicamente a política de segurança informacional no âmbito da Câmara, supervisionado pela Diretoria-Geral dessa Casa legislativa.

Na justificação da instituição da política, a Câmara destaca a importância estratégica da informação para consecução de suas atribuições institucionais e para interação dessa instituição com a sociedade, em especial a brasileira.

4.6.4 A gestão de riscos de segurança da informação no Tribunal de Contas da União (TCU)

A política corporativa de segurança da informação do TCU (PCSI/TCU), aprovada pela Resolução – TCU n.º 217, de 15 de outubro de 2008 (BRASIL, 2008e), estabelece que esse papel seja desempenhado pela Secretaria-Geral da Presidência (Segepres), por meio da Assessoria de Segurança da Informação e Governança de Tecnologia da Informação (Assig) e pelo Comitê de Segurança da Informação (CSI).

O CSI, instituído pela PCSI/TCU, tem por finalidade formular e conduzir diretrizes para a política de segurança da informação do Tribunal, analisar periodicamente sua efetividade, propor normas e mecanismos institucionais para melhoria contínua e assessorar, em matérias correlatas, a Comissão de Coordenação-Geral (CCG) e a Presidência do Tribunal.

Tal comitê é composto por dois representantes de cada Secretaria-Geral, além de representante da Secretaria de Infraestrutura de TI (Setic) e do titular da Assig, que o preside.

A composição heterogênea e representativa de interesses e setores diversos do Tribunal atende às boas práticas de segurança da informação, propicia ampla discussão e confere legitimidade às propostas submetidas por esse Comitê às instâncias superiores.

5 O COBIT 5 FOR INFORMATION SECURITY COMO FACILITADOR DO ESCRITÓRIO SETORIAL DE SEGURANÇA E RISCOS DE INFORMAÇÃO EM TI

5.1 ADAPTAR O COBIT 5 FOR INFORMATION SECURITY PARA O AMBIENTE CORPORATIVO

A segurança da informação é valiosa para a corporação apenas quando é suficientemente adaptada à situação única em que a organização existe e opera. Essa situação única é criada por diversos elementos que tornam desafiante a mudança do ambiente.

Os facilitadores específicos de segurança da informação podem ser usados para aumentar ainda mais a maturidade, a capacidade e o desempenho da segurança da informação dentro do empreendimento. Adaptar esses facilitadores específicos de segurança da informação para ambiente corporativo é o desafio.

A ISACA oferece orientação à aplicação prática e abrangente sobre a governança de TI da companhia em sua publicação COBIT® 5 Implementation, que é baseada em ciclo de vida de melhoria contínua, sem pretender ser abordagem prescritiva, e sim guia para profissionais de segurança da informação que precisam integrar a segurança no âmbito operacional global da corporação, apoiado por kit de ferramentas de implementação contendo recursos a ser continuamente melhorados.

O seu conteúdo inclui:

- Autoavaliação, medição e ferramentas de diagnóstico;
- Apresentações destinadas a públicos diversos;
- Artigos relacionados e mais explicações.

Assim, o objetivo é apresentar implementação e melhoria contínua do ciclo de vida em alto nível e descrever essa orientação genérica a partir da perspectiva de segurança da informação. Além disso, a relação dos atuais arcabouços de segurança da informação, boas práticas e padrões está descrita nesse guia.

5.2 IMPLEMENTAR AS INICIATIVAS DE SEGURANÇA DA INFORMAÇÃO

5.2.1 Considerar o contexto de segurança da informação da corporação

A organização precisa definir e implementar seus próprios facilitadores de segurança da informação, dependendo de fatores no ambiente interno e externo específico da organização, tais como:

- Ética e cultura relacionados à segurança da informação;
- Leis, regulamentos e políticas;
- Normas contratuais aplicáveis;
- Políticas e práticas existentes;
- Nível de maturidade atual de facilitadores de segurança da informação;
- Recursos de segurança da informação e recursos disponíveis;
- Práticas da indústria;
- Padrões e estruturas existentes e obrigatórios sobre segurança da informação.

Requisitos de segurança da informação do empreendimento precisam ser definidos com base em:

- Plano de Negócios e intenções estratégicas;
- Estilo de gestão;
- Perfil de risco da informação;
- Apetite pelo risco.

Portanto, a abordagem para a implementação de iniciativas de segurança da informação é diferente para cada organização, e o contexto precisa ser entendido e considerado para adaptar o COBIT 5 for Information Security de

forma eficaz. É igualmente importante para alavancar e desenvolver facilitadores específicos de segurança de informação existentes.

O COBIT 5 for Information Security conecta-se a outros arcabouços de segurança da informação, boas práticas, padrões e normas, sendo sustentado também por eles, devendo fornecer ao profissional de segurança da informação detalhes sobre tópicos específicos para otimizar facilitadores descritos nesse guia.

A conexão do COBIT 5 for Information Security a esses arcabouços subjacentes, boas práticas e normas é descrita a seguir. Em geral, os fatores-chave de sucesso para implementação bem-sucedida de facilitadores de segurança da informação incluem:

- Direção e delegação para iniciativas de segurança da informação, bem como compromisso e apoio contínuo visível prestado pela alta administração;
- Iniciativas de segurança da informação para entender o negócio e objetivos de TI apoiadas pelas partes;
- Comunicação eficaz e capacitação das mudanças necessárias asseguradas;
- COBIT 5 for Information Security e outros apoiando boas práticas e padrões adaptados ao contexto único da corporação;
- Foco em ganhos rápidos e prioridade em melhorias benéficas que sejam fáceis de implementar;
- Financiamento adequado e comprometimento de recursos;
- Recursos humanos adequadamente qualificados que possam implementar facilitadores.

5.2.2 Criar o ambiente adequado

É importante aproveitar o COBIT para que iniciativas de segurança da informação sejam devidamente reguladas e controladas. As principais iniciativas relacionadas à TI, muitas vezes, falham devido a inadequações de direção, apoio e

supervisão pelas partes interessadas, e não é diferente a implementação de facilitadores de segurança da informação, aproveitando esse guia. Apoio e orientação das principais partes interessadas são fundamentais para garantir que melhorias sejam alcançadas e mantidas. Em ambiente corporativo fraco, tal como uma obscura estratégia de segurança da informação em geral, esse apoio e participação são ainda mais importantes.

Uso de facilitadores, aproveitando COBIT 5 for Information Security, deve ser solução para atender às necessidades e questões reais de negócios, em vez de constituir um fim em si mesmo. Requisitos de segurança da informação com base em pontos de dor atuais e dirigentes devem ser identificados e aceitos pela administração como áreas que precisam ser abordadas. Verificações, diagnósticos ou avaliações em alto nível da saúde de capacidade com base nesse guia são ferramentas que podem ser usadas para aumentar a conscientização, criar consenso e gerar compromisso de ação. O compromisso e o apoio de partes interessadas precisam ser solicitados desde o início e, para consegui-los, objetivos de implementação e benefícios devem ser claramente expressos em termos de negócios e resumidos para delinear caso de negócio.

Com o compromisso obtido, recursos adequados devem ser fornecidos para apoiar programa de segurança da informação. Principais funções e responsabilidades do programa devem ser definidas e atribuídas. Cuidados devem ser tomados para manter compromisso das partes interessadas afetadas em base contínua.

Estruturas adequadas e processos de supervisão e direção devem ser estabelecidos e mantidos. Essas estruturas e processos também devem garantir alinhamento contínuo com governança da organização, abordagens de gestão de risco e estratégia de negócios.

Apoio visível e compromisso devem ser fornecidos pelas partes interessadas, tais como altos executivos, para definir clima ético geral da organização e garantir compromisso com o programa de segurança da informação em todos os níveis.

5.2.3 Reconhecer os pontos críticos e os eventos disparadores

Há fatores que podem indicar necessidade de melhorar facilitadores de segurança da informação. Pontos de dor ou eventos de disparo podem ser usados como ponto de partida para iniciativas de implementação, casos de negócios para melhorar o facilitador de segurança da informação podem estar relacionados com questões práticas e cotidianas, devendo melhorar o compromisso e criar senso de urgência dentro da companhia, sendo necessário para começar a implementação.

Além disso, ganhos rápidos podem ser identificados, e acrescentar valor pode ser demonstrado em áreas que são mais visíveis ou reconhecíveis na organização. Isso fornece plataforma para introdução de mudanças e pode ajudar na obtenção de difundido compromisso executivo sênior e apoio para mudanças mais generalizadas.

Exemplos de pontos típicos de dor para que novos ou revisados facilitadores de segurança da informação possam ser solução são:

- Incidentes de segurança da informação dentro da organização, ou com outras assemelhadas, como:
    - Perda de dados ou roubo causado por usuários não autorizados invadindo sistemas;
    - Negação de serviço em decorrência de ataques cibernéticos;
    - Modificação intencional, ou não, de informações críticas.
- Deixar de cumprir requisitos legais, regulamentares ou contratuais, tais como regras de privacidade.
- Incapacidade de lidar com a adoção de novas tecnologias devido a restrições de segurança da informação.
- Resultados da auditoria regularmente relatados com pobres capacidades de segurança da informação.

Além desses pontos de dor, eventos em ambiente interno e externo à corporação podem sinalizar ou desencadear concentração na governança e gestão de TI corporativa. Exemplos desses incluem:

- Nova regulamentação, conformidade de requisitos contratuais;
- Mudanças tecnológicas significativas ou mudanças de paradigma;
- Auditoria externa ou avaliações de consultoria;
- Fusões, aquisições ou outras grandes mudanças institucionais.

5.2.4 Permitir a mudança

Implementação bem-sucedida depende da gestão da mudança de forma eficaz. Em muitas organizações, há foco significativo sobre aspectos técnicos de programa de segurança da informação, mas não suficiente ênfase no gerenciamento de aspectos humanos, comportamentais e culturais da mudança e em motivar interessados para acolher essa mudança.

Não se deve presumir que sejam prontamente aceitas e adotadas mudanças propostas, por novos ou revisados facilitadores de segurança da informação, pelos intervenientes envolvidos ou afetados. A possibilidade de ignorância e/ou resistência à mudança tem de ser resolvida por meio de abordagem estruturada e proativa. Apoio dessa consciência ideal de implementação do programa deve ser alcançado por meio de plano de comunicação que defina para cada fase do programa, o que será comunicado, de que forma e por quem.

Melhoria sustentável pode ser alcançada, ganhando compromisso das partes interessadas por meio de persuasão e de defesa, ou se possível, por exigir o cumprimento da legislação, regulamentos ou acordos contratuais. Em outras palavras, questões humanas, comportamentais e culturais precisam ser consideradas para criar cultura em que partes interessadas são participantes ativos no cumprimento de metas organizacionais de segurança da informação.

Práticas do facilitador Cultura, Ética e Comportamento, apresentado anteriormente, são importantes ferramentas para reduzir resistência à mudança.

Influenciar comportamento por meio de comunicação eficaz, identificando incentivos e recompensas corretos e relevantes, e impor adesão a mudanças são fatores importantes a se ter em conta. Investir em práticas que influenciam permite aceitação de alterações feitas, sendo clara exigência de tempo e paciência de membros da equipe de segurança da informação.

5.2.5 Abordar o ciclo de vida

O ciclo de vida de implementação fornece modo para a organização lidar com complexidade e desafios normalmente encontrados durante implementações utilizando COBIT para tratar da segurança da informação.

Existem três componentes inter-relacionados no ciclo de vida:

- Melhoria contínua do ciclo de vida do núcleo – refletindo que esse não é projeto único;
- Capacitação de mudança – dirigindo-se aos aspectos comportamentais e culturais;
- Gestão do programa.

Como discutido anteriormente, um ambiente adequado necessita ser criado para garantir o sucesso da iniciativa de implementação ou melhoria. O ciclo de vida e suas sete fases estão ilustrados nesse guia, conforme segue:

Fase 1 – Iniciar programa. O objetivo dessa fase é de entender a amplitude (“largura” e “profundidade”) da alteração prevista, as partes afetadas, a natureza do impacto e o envolvimento exigido de cada grupo de intervenientes, bem como a atual prontidão e capacidade de adaptação à mudança.

Os pontos críticos e eventos de gatilho relacionados à segurança da informação devem ser cuidadosamente avaliados. Práticas operacionais apresentadas no facilitador Informação, anteriormente expostas, podem ser muito úteis para essa avaliação. Relatórios de avaliação de segurança da informação, incluindo descobertas de auditoria sobre segurança da informação e relatórios de risco, ou painel de segurança da informação, podem fornecer informações importantes sobre incidentes, problemas e riscos de segurança da informação.

Levantamentos com gerência executiva devem fornecer plataforma para estabelecer a vontade de mudar, apresentando temas e relatórios de forma clara e compreensível.

Fase 2 – Definir problemas e oportunidades. Essa fase está centrada na definição do âmbito da execução ou da iniciativa de melhoria. Diagnósticos de alto nível podem ser úteis para definir escopo e compreender áreas de alta prioridade para se concentrar. Avaliação do estado atual da fase é então realizada, e problemas ou deficiências são identificados por meio da avaliação de capacidade do processo. Iniciativas em larga escala devem ser estruturadas como iterações do ciclo de vida. Para iniciativa de implementação superior a seis meses, há risco de perda do impulso, concentração e apoio de *stakeholders*.

Para alcance da iniciativa de segurança da informação, o estado atual dos facilitadores de segurança da informação deve ser avaliado e verificado. Para processos, definição de escopo pode basear-se em objetivos de segurança da informação para processos associados de TI, conforme documentado na orientação de processo detalhado anteriormente. Também útil é considerar como cenários de risco podem destacar principais processos em que se concentrar.

Fase 3 – Definir roteiro. Durante essa fase, meta de melhoria é definida, seguida por análise mais detalhada, alavancada nesse guia e outras orientações, como em criar o ambiente adequado, anteriormente exposto, para identificar lacunas e possíveis soluções. Soluções podem ser ganhos rápidos e atividades difíceis e de longo prazo. Deve ser dada prioridade às iniciativas que são fáceis de conseguir e susceptíveis de produzir benefícios.

A seguir orientação adicional é fornecida em conexão comumente usada em arcabouços de segurança da informação, boas práticas e padrões. Fase importante no ciclo de vida de implementação está em definir alvo correto e determinar como relevantes arcabouços de segurança da informação; boas práticas e padrões podem ajudar a corporação a alcançar seu alvo.

Vitórias rápidas, iniciativas de alto impacto e de baixo esforço, para iniciativa de segurança da informação, são muitas vezes desafiantes. O equilíbrio constante entre garantia de segurança da informação e funcionamento da instituição deve ser considerado na definição dessas vitórias rápidas. Mudança visível é

necessária para a vitória rápida demonstrar rapidamente valor acrescentado para a organização.

Fase 4 – Programar plano. Essa fase planeja soluções práticas por meio da definição de projetos apoiados por casos de negócios justificáveis. Plano de mudança para implementação também é desenvolvido. Caso de negócio bem desenvolvido ajuda a garantir que benefícios do projeto sejam identificados e monitorados. Medidas podem ser definidas e monitoramento estabelecido usando objetivos e métricas do COBIT 5 for Information Security, a fim de garantir que alinhamento de negócios seja alcançado e mantido e o desempenho possa ser medido.

Fase 5 – Executar plano. Essa fase implementa soluções propostas em práticas cotidianas. Para obter sucesso, engajamento e compromisso demonstrado pela alta administração são necessários, assim como propriedade pelos negócios afetados e partes interessadas de TI.

Fase 6 – Realizar benefícios. Essa fase enfoca operação sustentável dos novos ou aperfeiçoados facilitadores e monitoramento da realização dos benefícios esperados. Em outras palavras, esta fase é utilizada para determinar se objetivos são alcançados e sustentáveis.

Fase 7 – Revisão eficaz. Durante essa fase, o sucesso global da iniciativa é revisto, são identificados novos requisitos de segurança da informação para a corporação e a necessidade de melhoria contínua é reforçada. Ao longo do tempo, o ciclo de vida deveria ser seguido iterativamente, construindo abordagem sustentável para segurança da informação.

CONSIDERAÇÕES FINAIS

Nesta era informacional, o processo decisório está cada vez mais relacionado à qualidade de informação e conhecimento, o que facilita o alcance de metas programadas por meio de uma gestão organizacional eficiente.

Considero que o cumprimento da missão organizacional em instituições modernas não possa prescindir da proteção das informações, e consequentemente das tecnologias que as suportam.

Assim sendo, o estabelecimento de área responsável pela garantia da qualidade das informações pode corroborar na melhoria contínua da estrutura de gestão de risco e segurança.

Deriva disso a importância desta pesquisa ao mostrar razões capitais para implementar escritório setorial de segurança e riscos de informação em TI.

Entre os vários normativos e boas práticas, nacionais ou não, cujas diretrizes se prestam a essa empreitada, fiz opção pelo arcabouço COBIT 5 for Information Security da instituição ISACA. Confio que argumentos expostos neste estudo confirmem a aplicabilidade do COBIT 5 for Information Security, devido a suas abrangência e adequação, como facilitador na estruturação de escritório setorial de segurança e riscos de informação em TI.

O Senado Federal exerce papel de relevância estratégica fundamental à realidade brasileira. As informações recebidas, transitadas e geradas nesta Casa, principalmente constantes de processos legislativos, são fundamentais ao exercício adequado de sua missão institucional.

Considerando a gestão de riscos de segurança da informação atual no Senado Federal, conforme supra esboçado, estruturar essa função em TI, em especial aplicada ao processo legislativo, pode ser ferramenta para aprimorá-la, e usar o COBIT 5 for Information Security pode facilitar essa tarefa.

Finalmente, conto que este trabalho, e os conceitos nele indicados, sirvam como base para destacar essas questões e contribuir na recomendação de caminhos.

A fim de avançar nesse tema, é recomendável realizar estudos de caso da utilização do COBIT 5 for Information Security como facilitador da instituição do escritório setorial de segurança e riscos de informação em TI

REFERÊNCIAS

BAAKLINI, Abdo I. **O Congresso e o sistema político no Brasil**. Rio de Janeiro: Paz e Terra, 1993.

BERNSTEIN, P. **Desafio aos deuses**: a fascinante história do risco. 3. ed. Rio de Janeiro: Campus, 1996.

BRASIL. **Decreto 8135, do Poder Executivo**, de 4/11/2013. Publicado no Diário Oficial da União (DOU) 215, de 5/11/2013, Seção 1, pag. 02. Disponível em:<http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=05/11/2013&jornal=1&pagina=2&totalArquivos=72>. Acesso em: 3 mar. 2014.

BRASIL. Tribunal de Contas da União (TCU). **Sumários Executivos: levantamento de governança de TI 2012.** Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2626584.PDF>. Acesso em 17 out. 2014.

BRASIL. Tribunal Regional do Trabalho da 11ª Região. **Escritório de Segurança de Informação**. Disponível em: <http://governanca.trt11.jus.br/escritorios/escritorio-de-seguranca-da-informacao/>. Acesso em: 13 mar. 2014.

DIAS, C. A.; TORRES, F. R. Segurança da informação no TCU: cumprindo as próprias recomendações. **Revista do Tribunal de Contas da União**, Brasília, n. 117, p. 57-66, jan/abr. 2010.

ENTERPRISE Security and Risk Management Office. State of North Carolina. Disponível em: <http://www.iso.scio.nc.gov/>. Acesso em: 1 nov. 2014.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT 5 for information security**. Rolling Meadows, 2012.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT 5 implementation**. Rolling Meadows, 2012.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT 5**: process reference guide. Rolling Meadows, 2011.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT 5**: the Framework. Rolling Meadows, 2011.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **COBIT process assessment model (PAM)**: using COBIT 4.1. Disponível em: <www.isaca.org/cobit-pam>. Acesso em: 20 set. 2014.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **Information security governance**: guidance for boards of directors and executive management. 2nd Edition. Rolling Meadows, 2006.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **Information security governance**: guidance for information security managers. Rolling Meadows, 2008.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. **The business model for information security (BMIS)**. Rolling Meadows, 2010.

IT GOVERNANCE INSTITUTE. **Board briefing on IT governance**. 2nd Edition, Rolling Meadows, 2003. Disponível em:<http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf>. Acesso em:30 out. 2014.

MACÊDO, D. **Implantação de escritório de segurança da informação**. Disponível em: <http://www.diegomacedo.com.br/implantacao-de-escritorio-de-seguranca-da-informacao/>. Acesso em: 1 mar. 2014.

PALMA, F. **Implantação de escritório de segurança da informação**. Disponível em: <http://www.portalgsti.com.br/2012/10/escritorio-de-seguranca.html?goback=.gde_2353556_member_174862309>. Acesso em: 4 mar. 2013.

ROSS, S. J. **Creating a culture of security**. Rolling Meadows: information systems audit and control association, 2011. Senado Federal institui Política de Gestão de Riscos. Disponível em: <https://intranetsenado.senado.gov.br/detalhenotdestaque?noticia_id=senado-federal-institui-politica-de-gestao-de-riscos>. Acesso em: 13 mar. 2014.

TREASURY BOARD OF CANADA SECRETARIAT. **Guideline on developing a departmental security plan**. Disponível em: <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=20010&section=text>. Acesso em: 1 out. 2014.