

COBIT 5 for Information Security

J. Souza Neto, PhD, CGEIT, CRISC, ITILF, COBITF, COBIT5F



© 2012 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Use of this publication is permitted solely for personal use and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

Informação!

- Informação é um recurso chave para todas as organizações.
- Informação é criada, usada, retida, divulgada e destruída.
- A Tecnologia da Informação tem um papel importante nessas ações.
- A Tecnologia da Informação tornou-se pervasiva em todos os aspectos da vida pessoal e profissional.

Que benefícios informação e tecnologia trazem para as organizações?

Benefícios para as Organizações



As organizações e os executivos se esforçam para:

- Manter a qualidade da informação para apoiar decisões de negócio.
- Gerar valor para o negócio a partir de investimentos habilitados por TI, isto é, alcançar objetivos estratégicos e realizar benefícios de negócio por meio do uso efetivo e inovador da TI.
- Atingir excelência operacional por meio da aplicação eficiente e confiável de TI.
- Manter o risco da TI num nível aceitável.
- Ottimizar o custo dos serviços de TI.

Como os benefícios podem ser realizados de modo a criar valor para as partes interessadas?

Valor para as Partes Interessadas



- A entrega de valor às partes interessadas requer uma boa Governança e gestão dos ativos de TI.
- O Conselho de Administração, a Diretoria e os gestores devem encarar a TI como uma parte significativa do negócio.
- Requisitos de conformidade externos legais, regulatórios e contratuais relacionados ao uso corporativo da TI e da informação estão crescendo e o seu não cumprimento cria ameaças relevantes.
- **O COBIT 5 provê um *framework* abrangente que apoia a organização no alcance dos seus objetivos e na entrega de valor por meio da Governança e da gestão efetivas da TI.**

O Framework COBIT 5

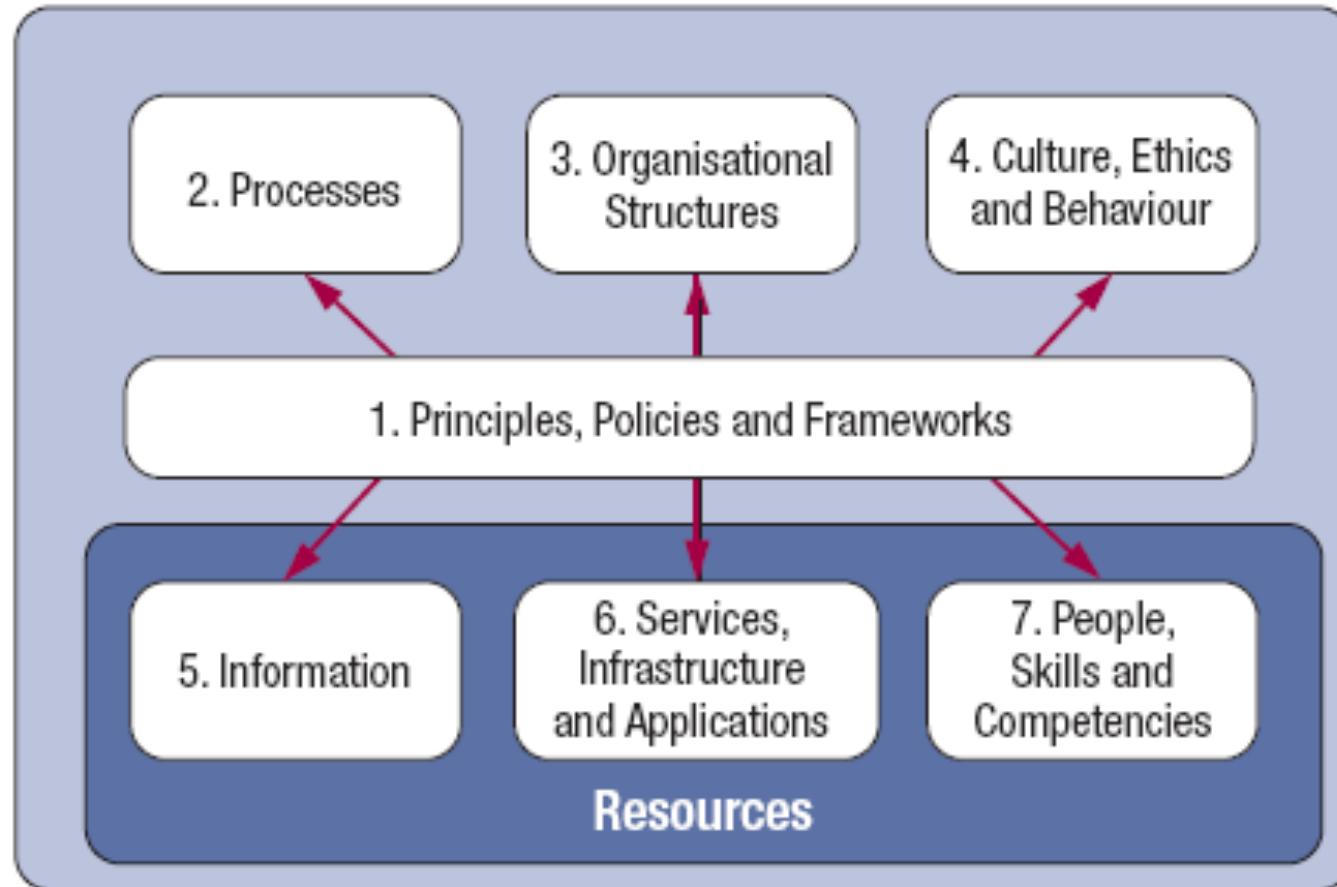
- De forma simples, pode-se dizer que o COBIT 5 ajuda as organizações a criar um valor ótimo a partir da TI, mantendo em equilíbrio a realização de benefícios e a otimização dos níveis de risco e do uso dos recursos.
- O COBIT 5 habilita a informação e a TI a serem governadas e gerenciadas de uma maneira holística em toda a organização, atuando integralmente nos processos fim-a-fim de negócio e nas áreas funcionais, considerando os interesses das partes interessadas externas e internas relacionados à TI.
- Os princípios e habilitadores do COBIT 5 são gerais e úteis para organizações de todos os tamanhos, sejam elas comerciais, do setor público ou do terceiro setor.

Princípios do COBIT 5



Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

Habilitadores do COBIT 5



Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

Governança e Gestão

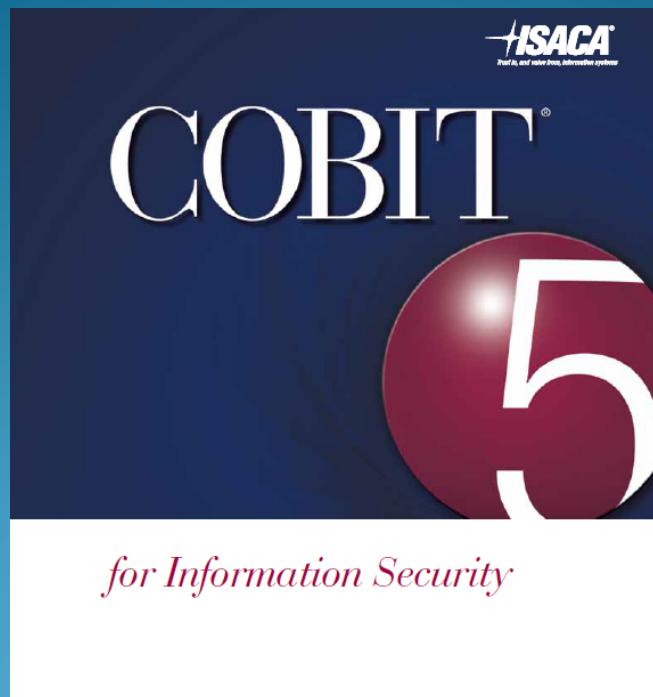


- A Governança assegura que as necessidades das partes interessadas são avaliadas para determinar objetivos corporativos acordados e balanceados, direcionando a ação por meio de priorização e tomada de decisão, e monitorando o desempenho e a conformidade em observância aos objetivos e direção acordados (EDM – *Evaluate, Direct and Monitor*).
A gestão Planeja, Constrói, Executa e Monitora as atividades em alinhamento com a direção definida pela Alta Administração para atingir os objectivos corporativos (PBRM – *Plan, Build, Run and Monitor*).

Em resumo ...

O COBIT 5 reúne os cinco princípios que permitem a uma organização construir uma *framework* eficaz de Governança e gestão baseado em um conjunto holístico de sete habilitadores que otimizam a informação e o investimento em tecnologia e o uso para o benefício dos *stakeholders*.

COBIT 5 for Information Security



Família de Produtos COBIT 5

COBIT® 5

COBIT 5 Enabler Guides

COBIT® 5:
Enabling Processes

COBIT® 5:
Enabling Information

*Other Enabler
Guides*

COBIT 5 Professional Guides

COBIT® 5 Implementation

COBIT® 5
for Information
Security

COBIT® 5
for Assurance

COBIT® 5
for Risk

*Other Professional
Guides*

COBIT 5 Online Collaborative Environment

COBIT 5 for Information Security



- ✓ Visão ampliada do COBIT5
- ✓ Explica cada componente do COBIT 5 numa perspectiva de Segurança da Informação.

O que este livro contém?



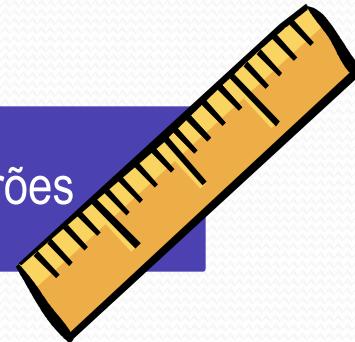
Guia dos direcionadores

Princípios numa perspectiva de
Segurança da Informação



Habilitadores para suporte

Alinhamento com padrões



Direcionadores



Os principais direcionadores para o desenvolvimento do *COBIT 5 for Information Security* incluem:

- 1.**A necessidade de descrever a Segurança da Informação num contexto corporativo
- 2.**Um incremento na necessidade das organizações de:
 - Manter os riscos em níveis aceitáveis.
 - Manter a disponibilidade de sistemas e serviços.
 - Estar em conformidade com o regulatório.
- 3.**A necessidade de estar relacionado e alinhado com outros padrões e *frameworks*
- 4.**A necessidade de consolidar todas as pesquisas, guias e *frameworks* da ISACA relacionados ao tema

Benefícios

O uso do ***COBIT 5 for Information Security*** pode resultar em diversos benefícios, tais como:

- Redução de complexidade e diminuição da relação custo/efetividade devido à melhoria na integração dos padrões de Segurança da Informação
- Melhoria na satisfação do usuário quanto aos resultados das iniciativas de Segurança da Informação
- Melhoria na integração das iniciativas de Segurança da Informação na organização
- Conscientização dos riscos e decisões relativas a risco baseadas em informações relevantes
- Melhoria em prevenção, detecção e recuperação de incidentes
- Redução do impacto dos incidentes de segurança
- Melhoria no suporte para inovação e competitividade
- Melhoria na gestão dos custos relacionados à Segurança da Informação
- Melhor compreensão da Segurança da Informação

Definição

A ISACA define Segurança da Informação como algo que:

garante que, na organização, a informação é protegida contra exposição indevida (confidencialidade), alterações impróprias (integridade) e impedimento de acesso (disponibilidade).

Uso dos Habilitadores COBIT 5 na Implementação da Segurança da Informação



COBIT 5 for Information Security fornece orientação específica com relação a todos os habilitadores

- 1. Políticas, Princípios e Frameworks** de Segurança da Informação
- 2. Processos**, incluindo detalhes e atividades específicos de Segurança da Informação
- 3. Estruturas Organizacionais** específicas de Segurança da Informação
- 4. Em termos de Cultura, Ética e Comportamento**, que fatores determinam o sucesso da governança e gestão de Segurança da Informação
- 5. Tipos de Informação** específicos de Segurança da Informação
- 6. Capacidades de Serviço** requeridas para prover funções de Segurança da Informação para uma organização
- 7. Pessoas, Habilidades e Competências** específicos para Segurança da Informação

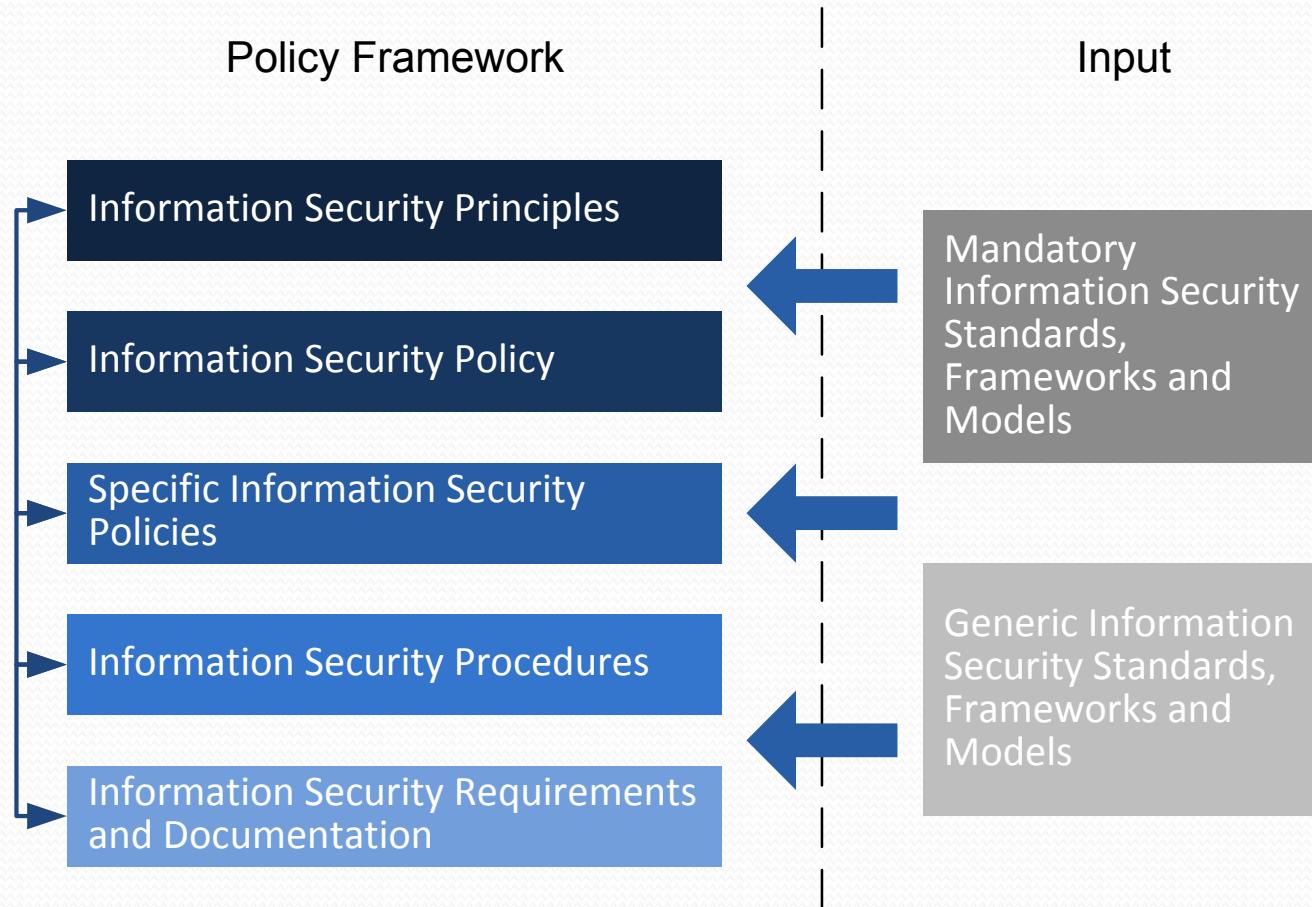
Habilitador Princípios, Políticas e *Frameworks*



Princípios, políticas e *frameworks* referem-se aos mecanismos de comunicação implantados para divulgar o direcionamento e as instruções das equipes de Governança e gestão, incluindo:

- Modelo de princípios, políticas e *frameworks*
- Princípios de Segurança da Informação
- Políticas de Segurança da Informação
- Adaptação de políticas ao ambiente corporativo
- Ciclo de vida de políticas

Habilitador Princípios, Políticas e Frameworks



Source: COBIT 5 for Information Security, figure 10. © 2012 ISACA® All rights reserved

Princípios de Segurança da Informação



Princípios de Segurança da Informação comunicam as regras da organização. Os princípios devem ser:

- Em número limitado;
- Descritos em linguagem simples.

Em 2010, a ISACA, o ISF e a ISC² criaram 12 princípios para ajudar os profissionais de Segurança da Informação a agregarem valor para suas organizações. Os princípios apóiam 3 tarefas:

- Apoiar o negócio.
- Defender o negócio.
- Promover um comportamento responsável em Segurança da Informação.

Os 12 Princípios

- Foco no negócio
- Entregar qualidade e valor às partes interessadas
- Estar em conformidade com os requisitos legais e regulatórios relevantes
- Prover informação tempestiva e precisa sobre o desempenho da segurança da Informação
- Avaliar ameaças atuais e futuras à informação
- Promover melhorias contínuas na informação

Os 12 Princípios

- Adotar uma abordagem baseada em risco
- Proteger informação classificada
- Concentrar-se em aplicações críticas de negócio
- Desenvolver sistemas de forma segura
- Atuar de uma maneira profissional e ética
- Promover uma cultura de Segurança da Informação positiva

Políticas de Segurança da Informação



Políticas fornecem uma orientação mais detalhada de como colocar os princípios em prática. Algumas organizações podem incluir políticas como:

- Política de Segurança da Informação
- Política de Controle de Acesso
- Política de Segurança de Informações de RH
- Política de Gestão de Incidentes
- Política de Gestão de Ativos

COBIT 5 for Information Security descreve os seguintes atributos de cada política:

- Escopo
- Validade
- Objetivos

Questão #1

No caso dos órgãos da APF,
qual é o regulatório básico
que norteia as Políticas e os
Princípios?

Questão #1

- Normas Complementares do DSIC/GSIPR, de 1 a 18
- NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão da Segurança da Informação
- NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação
- Norma NBR/ISO/IEC 27005:2008 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI).

Questão #1

Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2.848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

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

Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

Decreto 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

Habilitador Processos

O modelo de referência de processos do COBIT 5 subdivide as práticas e atividades relacionadas à TI de uma organização em áreas principais —Governança e gestão— com a gestão sendo organizada ainda em domínios de processos:

- O domínio Governança contém 5 processos; em cada processo, práticas de avaliar, direcionar e monitorar (*evaluate, direct and monitor - EDM*) são definidas.
- Os 4 domínios de gestão estão alinhados com as áreas de responsabilidade de planejar, construir, executar e monitorar (*plan, build, run and monitor - PBRM*).
- ***COBIT 5 for Information Security* examina cada um dos processos sob a perspectiva da Segurança da Informação.**

Habilitador Processos

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI10 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

Source: COBIT 5 for Information Security, figure 7. © 2012 ISACA® All rights reserved

Habilitador Estruturas Organizacionais



O COBIT 5 examina o modelo de estruturas organizacionais sob a perspectiva da Segurança da Informação. Ele define os papéis e estruturas de Segurança da Informação e também examina a questão da prestação de contas (*accountability*) em Segurança da Informação, fornecendo exemplos de papéis e estruturas específicos e qual a autoridade relacionada, e também avalia alternativas de reporte de Segurança da Informação e as vantagens e desvantagens de cada uma.

Habilitador Estruturas Organizacionais



Role/Structure

Chief information security officer (CISO) (defined in COBIT 5)

Information security steering committee (ISSC)

Information security manager (ISM) (defined in COBIT 5)

Enterprise risk management (ERM) committee

Information custodians/business owners

Questão #2

E no caso da APF, quais são as estruturas organizacionais e papéis recomendados para a Segurança da Informação?

Questão #2

- Gestor de Segurança da Informação e Comunicações
- Divisão/Seção/Coordenação de Segurança da Informação e Comunicações
- Gestor da Informação
- ETIR
- Comitê de Segurança da Informação e Comunicações

Habilitador Cultura, Ética e Comportamento

Examina a cultura, a ética e o modelo de comportamento a partir de uma perspectiva de Segurança da Informação, fornecendo exemplos detalhados e específicos de Segurança da Informação:

1) O ciclo de vida da Cultura – medindo comportamentos ao longo do tempo para avaliar a cultura de segurança – alguns comportamentos podem incluir:

- Força de senhas
- Falta de abordagem de segurança
- A adesão a práticas de gestão de mudanças

Habilitador Cultura, Ética e Comportamento



2) Liderança e Campeões - essas pessoas são necessárias para servir de exemplo e ajudar a influenciar a cultura:

- Os gestores de risco
- Os profissionais de segurança
- Executivos de nível C

3) Comportamento desejável - número de comportamentos identificados que ajudarão a influenciar positivamente a cultura de segurança:

- A Segurança da Informação é praticada nas operações diárias.
- As partes interessadas estão cientes de como responder às ameaças.
- A gerência executiva reconhece o valor de negócio da segurança.

Habilitador Informação

Informação não é apenas o principal assunto da Segurança da Informação, mas também é um factor chave.

1) Tipos de informação são examinados e revelam os tipos de informações de segurança relevantes, que podem incluir:

- Estratégia de Segurança da Informação
- Orçamento da Segurança da Informação
- Políticas
- Material de sensibilização
- *Etc*

Habilitador Informação



2) Partes interessadas das informações, bem como o ciclo de vida da informação também são identificados e detalhados a partir de uma perspectiva de segurança. Detalhes específicos de segurança, tais como o armazenamento, compartilhamento, uso e descarte de informações são discutidos.

Habilitador Serviços, Infraestrutura e Aplicações



Os serviços, infraestrutura e modelos de aplicações identificam as capacidades de serviços que são necessárias para prover Segurança da Informação e funções relacionadas a uma empresa. A lista no *slide* a seguir contém exemplos de serviços relacionados à segurança, em potencial, que poderiam aparecer em um catálogo de serviços de segurança.

Habilitador Serviços, Infraestrutura e Aplicações



- Prover uma arquitetura de segurança.
- Prover a conscientização da segurança.
- Prover avaliações de segurança.
- Prover respostas adequadas a incidentes.
- Prover proteção adequada contra *malware*, ataques externos e tentativas de intrusão.
- Prover serviços de monitoramento e de alerta para eventos relacionados à segurança.

Habilitador Pessoas, Habilidades e Competências



Para operar de forma efetiva uma função de Segurança da Informação dentro de uma empresa, os indivíduos com conhecimentos e experiências adequados devem exercer essa função. Algumas habilidades e competências típicos relacionadas com a segurança são:

- Governança de Segurança da Informação
- Gestão de Riscos da informação
- Operações de Segurança da Informação

O COBIT 5 para Segurança da Informação define os seguintes atributos para cada uma das habilidades e competências:

- As definições de qualificações
- Metas
- Habilitadores relacionados

Implementação de Iniciativas de Segurança da Informação



Considerando o contexto de Segurança de Informação corporativo, COBIT 5 para Segurança da Informação informa que cada empresa precisa definir e implementar seus próprios habilitadores de Segurança da Informação dependendo de fatores intrínsecos ao ambiente da empresa, tais como:

- Ética e cultura relacionados à Segurança da Informação
- Leis, regulamentos e políticas aplicáveis
- Políticas e práticas existentes
- Recursos disponíveis e capacidades de Segurança da Informação

Implementação de Iniciativas de Segurança da Informação



Além disso, os requisitos de Segurança da Informação da empresa precisam ser definidos com base em:

- Plano de negócios e as intenções estratégicas
- Estilo de gestão
- Perfil de risco de informação
- Apetite pelo risco

A abordagem para a implementação de iniciativas de Segurança da Informação será diferente para cada empresa e o contexto precisa ser entendido para se adaptar o *COBIT 5 for Information Security* de forma eficaz.

Implementação de Iniciativas de Segurança da Informação



Outras áreas-chave importantes na implementação de *COBIT 5 for Information Security* são:

- Criar o ambiente adequado
- Reconhecer pontos críticos e eventos “gatilho”
- Entender que a implementação de práticas de Segurança da Informação não é um evento único, mas um ciclo de vida

Usando o *COBIT 5 for Information Security* para conectar outros *Frameworks*, Modelos, Boas Práticas e Padrões



COBIT 5 for Information Security tem como objetivo ser um *framework* guarda-chuva para conectar outros *frameworks*, boas práticas e padrões de Segurança da Informação.

COBIT 5 for Information Security descreve a difusão da Segurança da Informação em toda a empresa e fornece um *framework* abrangente de habilitadores, mas outros *frameworks* também podem ser úteis, porque eles podem discorrer sobre temas específicos. Os exemplos são:

- Modelo de Negócios para Segurança da Informação (BMIS)-ISACA
- Norma de Boas Práticas de Segurança da Informação (ISF)
- Família ISO/IEC 27000
- NIST SP 800-53a
- PCI-DSS

Securing Mobile Devices



SECURING MOBILE DEVICES

Using COBIT® 5 for Information Security

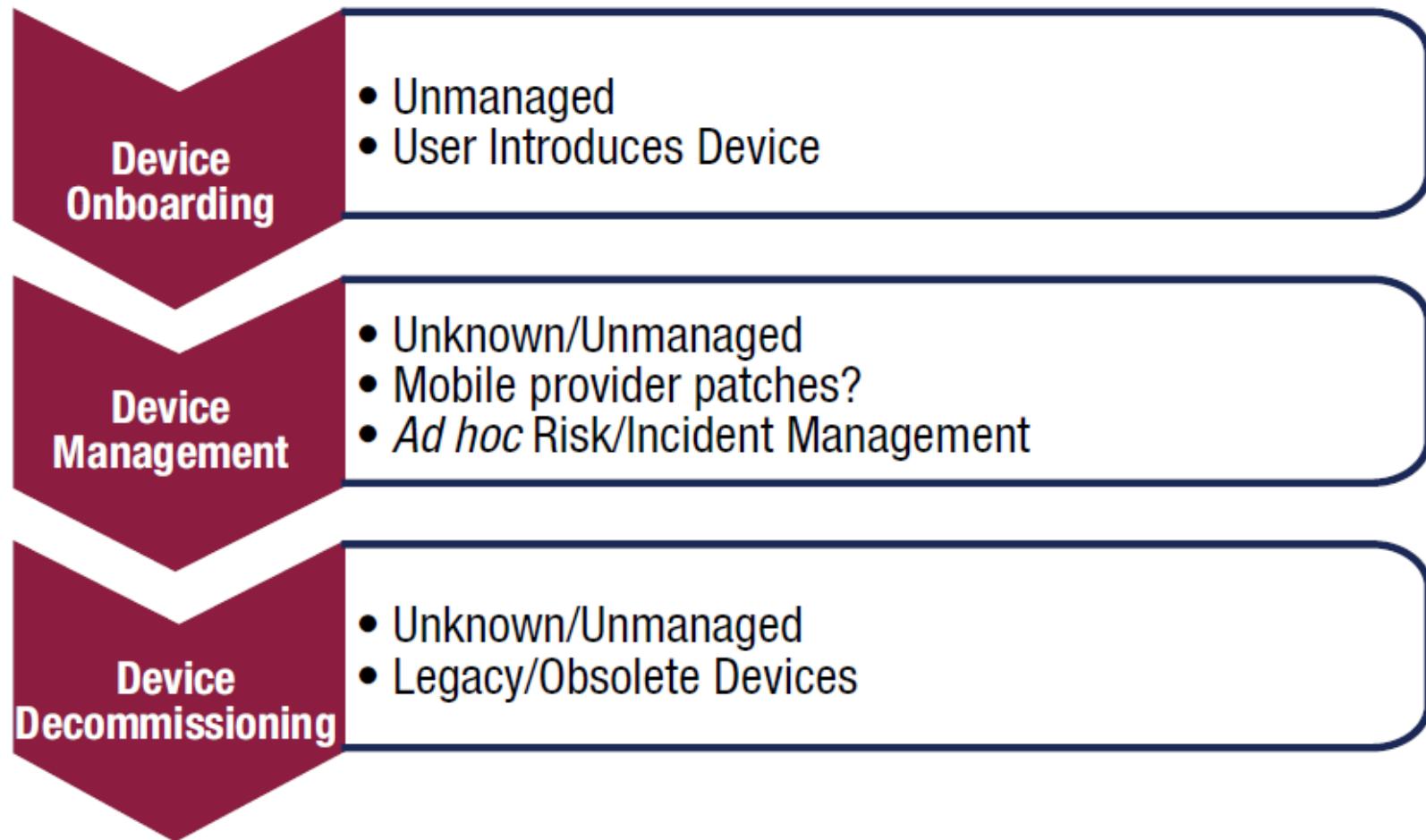
Vulnerabilidades, Ameaças e Riscos

Vulnerability	Threat	Risk
Information travels across wireless networks that are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, damage to enterprise reputation, compromised adherence to regulation, legal action
Mobility provides the users with the opportunity to leave enterprise boundaries, thereby eliminating many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network.	Malware propagation, which can result in data leakage, data corruption and unavailability of necessary data; physical theft
Bluetooth technology makes it very convenient for many users to have hands-free conversations; however, it is often left on and is then	Hackers can discover the device and then launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information

Riscos de Conexões não-autorizadas

Email	Simple to complex data transmission (including large files)
SMS	Simple data transmission, limited command and control (service command) facility
Hypertext Transmission Protocol (HTTP) get/post	Generic attack vector for browser-based connectivity, command and control
Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) socket	Lower-level attack vector for simple to complex data transmission
Domain name system (DNS) exfiltration	Lower-level attack vector for simple to complex data transmission, slow but difficult to detect
Bluetooth	Simple to complex data transmission, profile-based command and control facility, generic attack vector for close proximity
WLAN/Worldwide Interoperability for Microwave Access (WiMAX)	Generic attack vector for full command and control of target, equivalent to wired network

Ciclo de Vida de Componente BYOD



Processos do COBIT5 Relacionados

EDM01 Ensure governance framework setting and maintenance.

EDM02 Ensure benefits delivery.

AP003 Manage enterprise architecture.

AP004 Manage innovation.

AP006 Manage budget and costs.

AP012 Manage risk.

AP013 Manage security.

Processos do COBIT5 Relacionados

COBIT Process	Description	Application to Mobile Device Security Governance
EDM01 Ensure governance framework setting and maintenance.	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprises' mission, goals and objectives.	Recognize overarching governance provisions and apply them to mobile device security.
EDM02 Ensure benefits delivery.	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.	Apply cost-benefit analysis to the risk-weighted options for mobile device security governance.
AP003 Manage enterprise architecture.	AP003.01 Develop the enterprise architecture vision.	Prescribe adherence to architecture vision (or exceptions) at the policy level.
	AP003.02 Define reference	Prescribe alignment with reference

Categorias de Componentes Móveis

Category	Devices	Examples
1	Data storage (limited), basic telephony and messaging services, proprietary OS (limited), no data processing capability	Traditional cell phones
2	Data storage (including external) and data processing capabilities, standardized OS (configurable), extended services	<ul style="list-style-type: none">• Smartphones• Early pocket PC devices
3	Data storage, processing and transmission capabilities via alternative channels, broadband Internet connectivity, standardized OS (configurable), PC-like capabilities	<ul style="list-style-type: none">• Advanced smartphones• Tablet PCs

In addition to these three categories, a fourth category is emerging that combines advanced devices with non-PC devices. An example is the combination of household appliances¹⁶ or toys¹⁷ with smartphones, enabling remote control and other features.

Classificação de Riscos

Category/Risk	Category 1	Category 2	Category 3	Category 4
Physical				
Theft	Low	Medium	High	High
Loss	Medium	Medium	Medium	Medium
Damage/destruction	High	High	Low	Low
Organizational				
Agglomeration/heavy users	Low	Low	High	High
Complexity/diversity	Low	Medium	High	High
Technical				
Activity monitoring, data retrieval	Low	High	High	High
Unauthorized network connectivity	Low	Medium	High	High
Web view/impersonation	Low	Medium	High	High

Em Princípios, Políticas e *Frameworks* - Conjunto de Políticas Relacionadas

Mobile Device Use Policy	Subject/Area	COBIT 5 for Information Security Policy Set
Analyze business processes with mobile device dependencies, and prioritize accordingly.	Mobile device strategy	<ul style="list-style-type: none">• Information security policy• Business continuity and disaster recovery policy
Perform stakeholder analysis (internal and external) and derive requirements for mobile devices.	Mobile device strategy	Information security policy
Identify laws, regulations and governance rules for mobile device use, and define requirements.	Governance compliance	<ul style="list-style-type: none">• Information security policy• Compliance policy
Establish mobile device KPIs and regular reporting.	Governance compliance	<ul style="list-style-type: none">• Information security policy• Compliance policy
Identify threats to mobile devices (at all levels), anticipate future threats through technology	Risk	Risk management policy

COBIT 5 for Information Security

J. Souza Neto, PhD, CGEIT, CRISC, ITILF, COBITF,
COBIT5F

joaosouzaneto@ymail.com

