IBGP Instituto Brasileiro de GOVERNANÇA PÚBLICA

Uso de Dispositivos Móveis nas Organizações – BYOD Abordagem COBIT 5

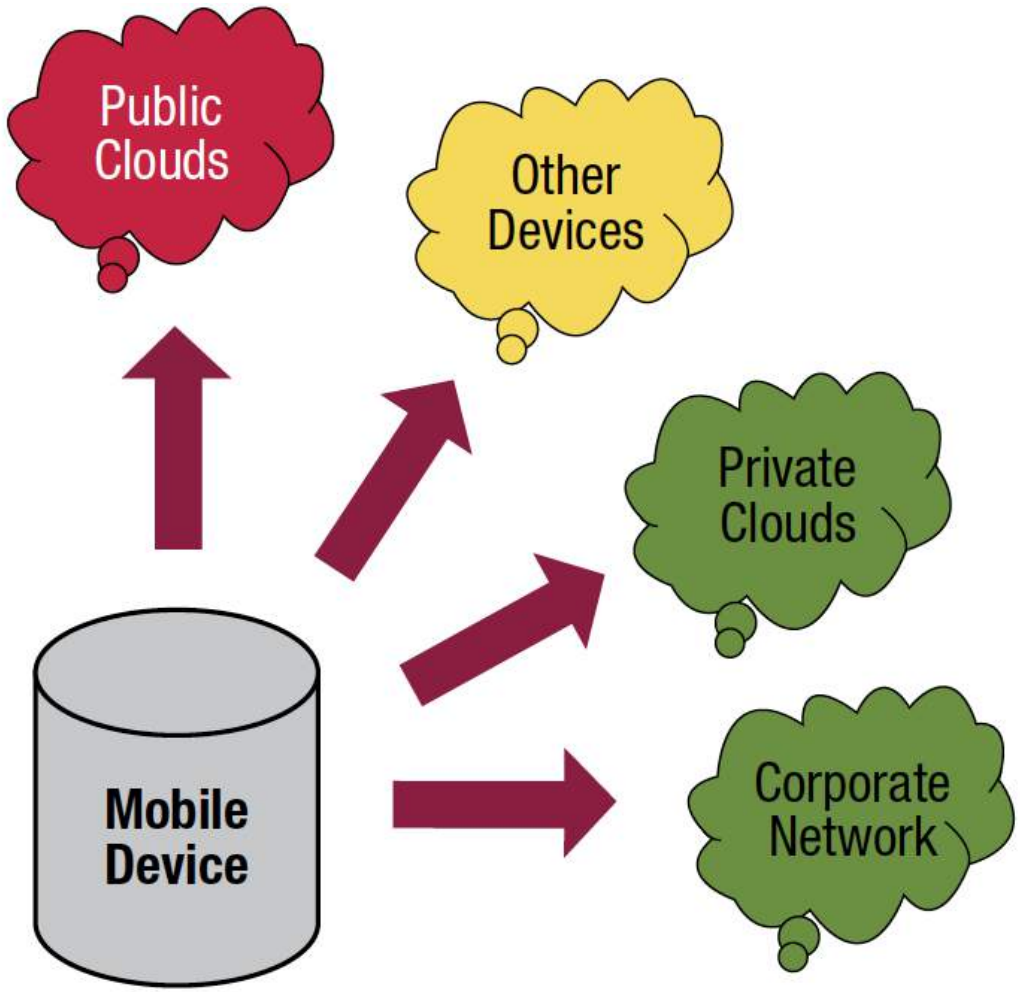
Prof. Dr. J. Souza Neto,
PMP. CSX, COBIT-INCS, CGEIT, CRISC, CLOUDF, ITILF,
COBIT 5 Implementation, COBIT 5 Assessor,
Certified COBIT Assessor, COBIT 5 *Approved Trainer*
souzaneto@ibgp.net.br

Agenda

- Dispositivos Móveis
- O Perímetro Organizacional
- Governança Corporativa de Dispositivos Móveis
- O Caso de Negócios
- Solução Corporativa, BYOD e Híbrida
- Mapa de Risco das Categorias de Dispositivos Móveis
- Habilitadores do COBIT 5
- Princípios de Segurança para Dispositivos Móveis

IBGP

Contexto



IBGP

Dispositivos Móveis

- Celulares tradicionais
- Smartphones
- Tablets
- Headsets Wireless
- GPS
- Drones
- Implantes médicos wireless
- …..

IBGP

Exemplos de Riscos à Segurança

- Aplicativos populares como Twitter ou Facebook exigir mais de dez privilégios críticas sobre os sistemas operacionais móveis, incluindo a alteração de dados, mudanças de configurações e o início ou a interrupção das chamadas de celulares.
- *Logs* para sistemas operacionais de dispositivos móveis contêm dados extremamente detalhados. Quando há um incidente com o dispositivo móvel, os dados relativos às últimas semanas são enviados para o provedor.
- ...

Como fica o Perímetro Organizacional?

- A mobilidade e a migração de poder de computacional para o dispositivo móvel corroeu o limite externo, o perímetro, da maioria das organizações.
- Modelos tradicionais de gestão de segurança da informação baseados em sistemas fechados são totalmente controlados pela empresa.
- Isso mudou drasticamente, pois os dispositivos móveis não estão sempre disponíveis para a atualização, aplicação de *patches* e aplicação de medidas de segurança.
- Normalmente, os dispositivos móveis incorporam sistemas abertos que usam serviços de nuvem como parte da estratégia de distribuição dos fabricantes ou como alternativas selecionadas pelos próprios usuários

IBGP

Como fica o Perímetro Organizacional? (cont.)

- Em contraste com computadores portáteis tradicionais, telefones inteligentes e dispositivos similares, geralmente, são menos transparentes no que diz respeito ao sistema operacional subjacente e à estratégia de aplicação de *patches*
- Em muitos casos, o gerenciamento de segurança da organização tem que contar com *patches* fornecida pelo fabricante ou pelo distribuidor, e a possibilidade de gerir ativamente estes dispositivos é limitada.
- Como consequência, a gestão da segurança tem de lidar com um ambiente sem perímetro definido que contém uma série de incógnitas e possíveis vulnerabilidades.

Governança Corporativa de Dispositivos Móveis

- Governança Corporativa de dispositivos móveis decorre das decisões estratégicas sobre como os dispositivos são trazidos para a empresa e como eles devem ser usados.
- Dados e informações armazenados em dispositivos móveis estão sujeitos a várias disposições de governança, da mesma forma que os usuários de telefonia e e-mail.
- Portanto, as empresas precisam alcançar um equilíbrio entre os seus interesses comerciais e os direitos dos seus usuários de usar livremente seus dispositivos móveis
- Isto pode não ser fácil, principalmente quando os usuários estão autorizados a trazer seus próprios dispositivos e os provedores de hardware e software móvel optarem por uma abordagem aberta. Isso pode criar riscos de segurança.

IBGP

O Caso de Negócios

- O uso de todas as formas de dispositivos móveis deve servir a um propósito de negócios, que está relacionado a metas e objetivos organizacionais que devem ser levados em conta na avaliação da tecnologias e dos elementos necessários à sua governança.
- Os limites estabelecidos pelos objetivos de negócio estratégicos determinarão a solução móvel selecionada. Isto inclui capacidades técnicas e considerações de custo-benefício.

IBGP

Definição do Caso de Negócios

- Para avaliar e selecionar a melhor abordagem para a governança da segurança, as empresas devem definir formalmente o caso de negócios, levando em consideração:
  - Riscos de segurança e impactos potenciais
  - Custo-benefício
  - Valor agregado em termos de produtividade/flexibilidade
  - Direcionadores estratégicos para a utilização de um dispositivo móvel

IBGP

Aplicando Val IT, Risk IT e COBIT na Construção do Caso de Negócios

- O COBIT 5 oferece uma série de processos que são úteis para apoiar a descrição de um caso de negócios formal.
- Os domínios do COBIT 5 são:
  - Avaliar, Direcionar e Monitorar (EDM)
  - Alinhe, Planejar e Organizar (APO)
  - Construir, Adquirir e Implementar (BAI)
  - Entregar, Prestar Serviços e Dar Suporte (DSS)
  - Monitor, Avaliar e Analisar (MEA)

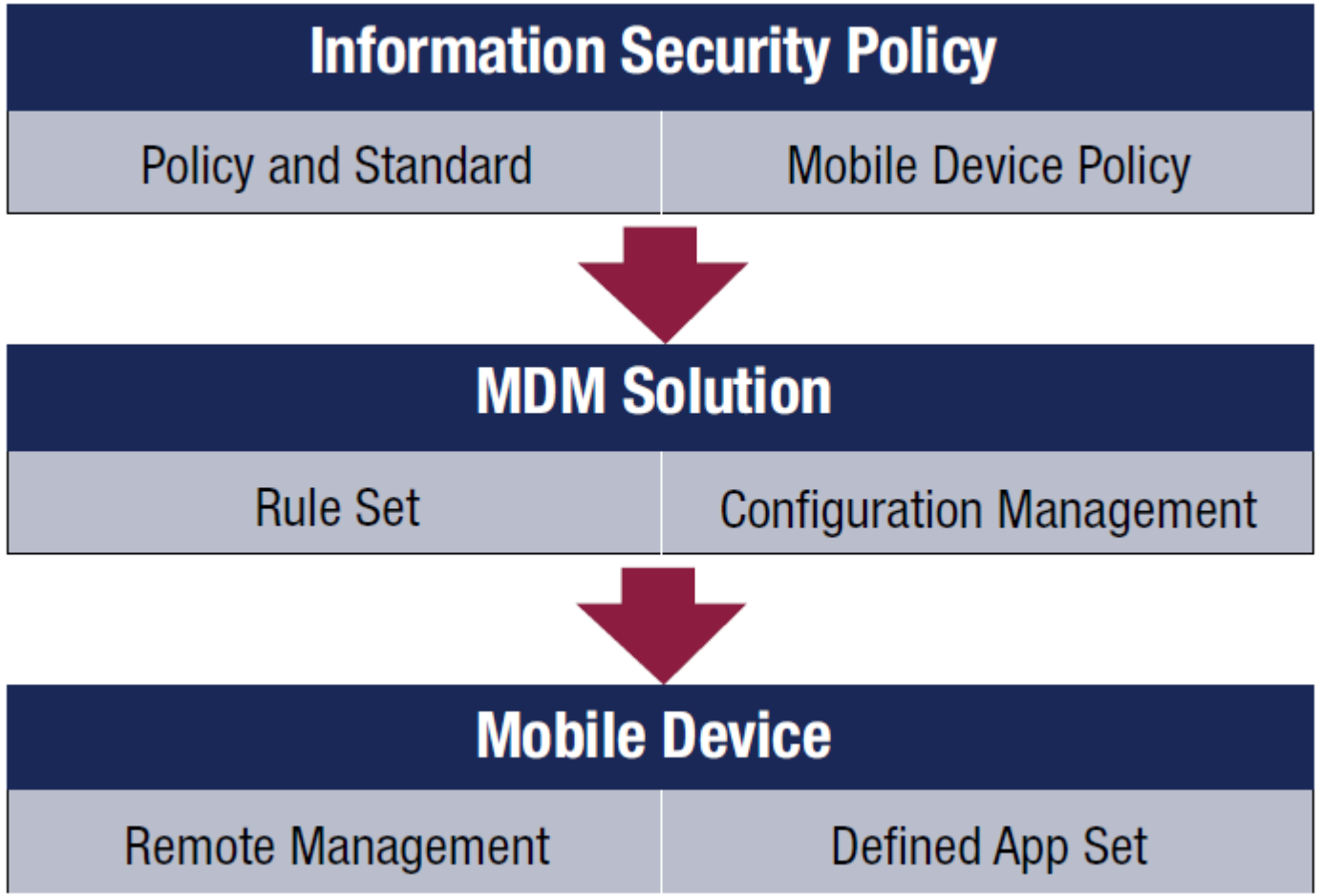
IBGP

Aplicando Val IT, Risk IT e COBIT na Construção do Caso de Negócios

COBIT 5	Val IT	Risk IT
EDM01 Ensure governance framework setting and maintenance.	VG5	RG1
EDM02 Ensure benefits delivery.	VG4	RG3
APO03 Manage enterprise architecture.	-	-
APO04 Manage innovation.	-	RG3
APO06 Manage budget and costs.	IM1, IM2, IM3, IM4, IM5	RE3, RR1
APO12 Manage risk.	-	All processes
APO13 Manage security.	-	RE1, RE2, RE3, RR1

IBGP

Solução Corporativa Padrão

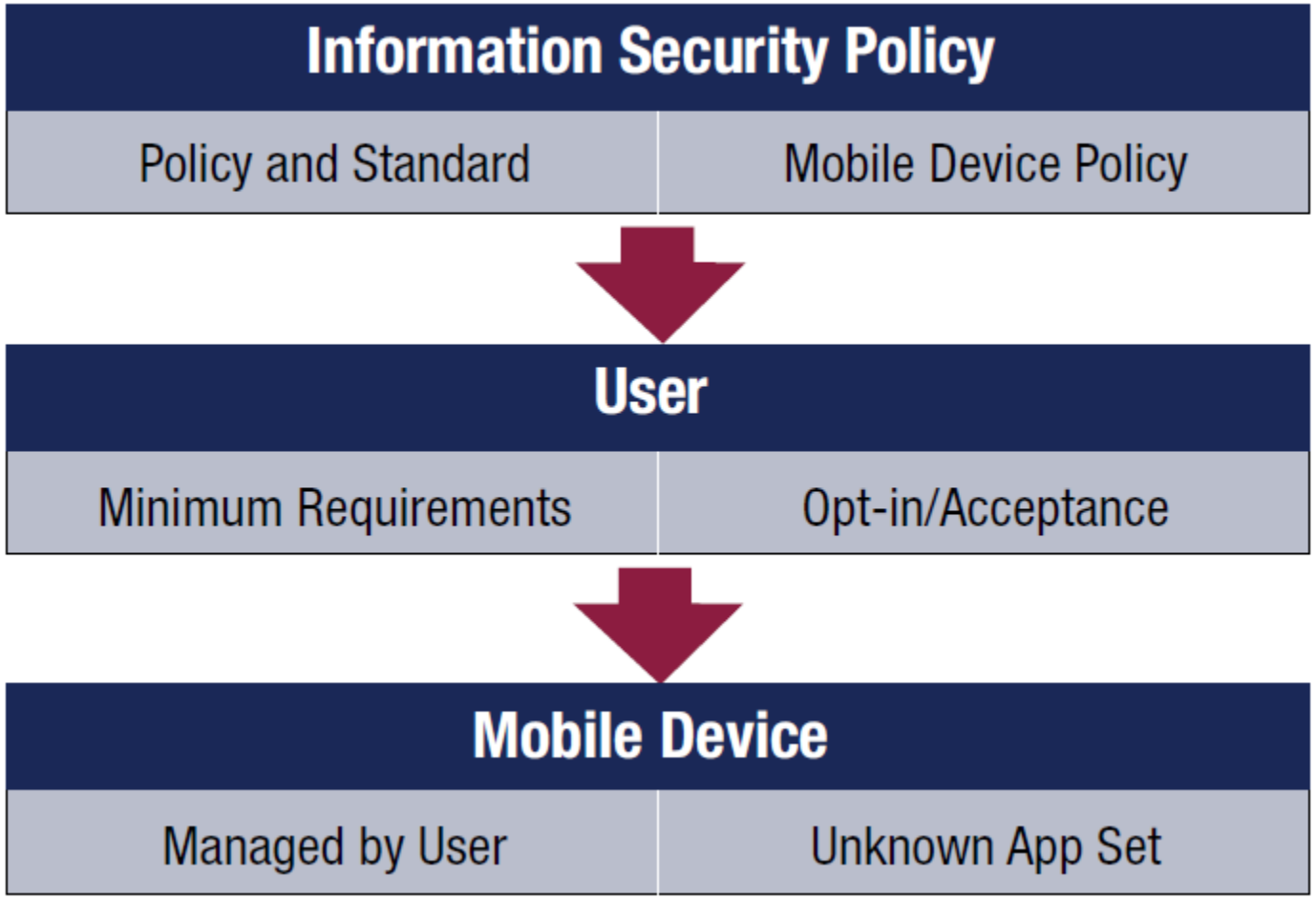


IBGP

Ciclo de Vida de um Dispositivo Móvel

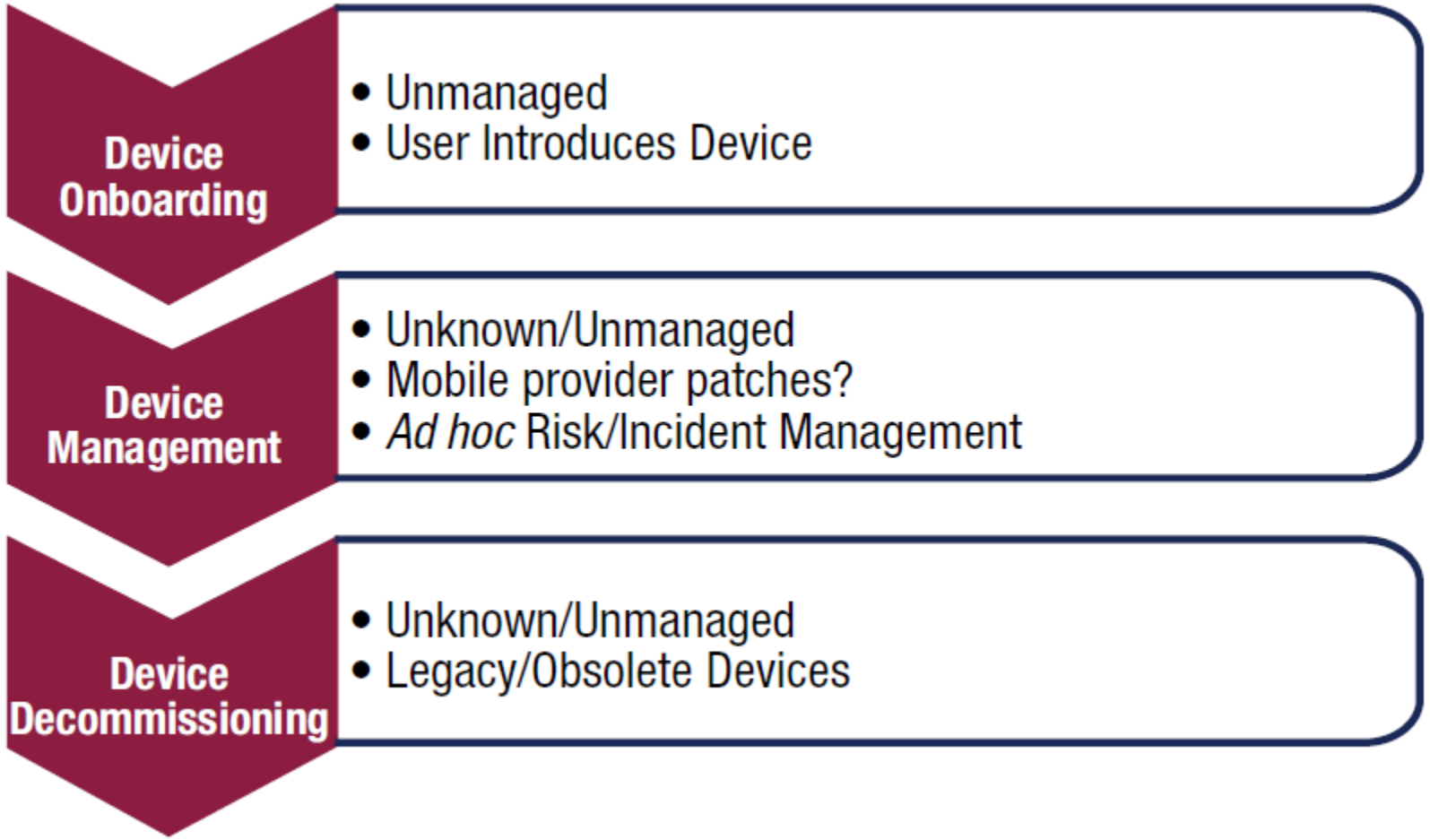
IBGP

Componentes de uma Solução BYOD



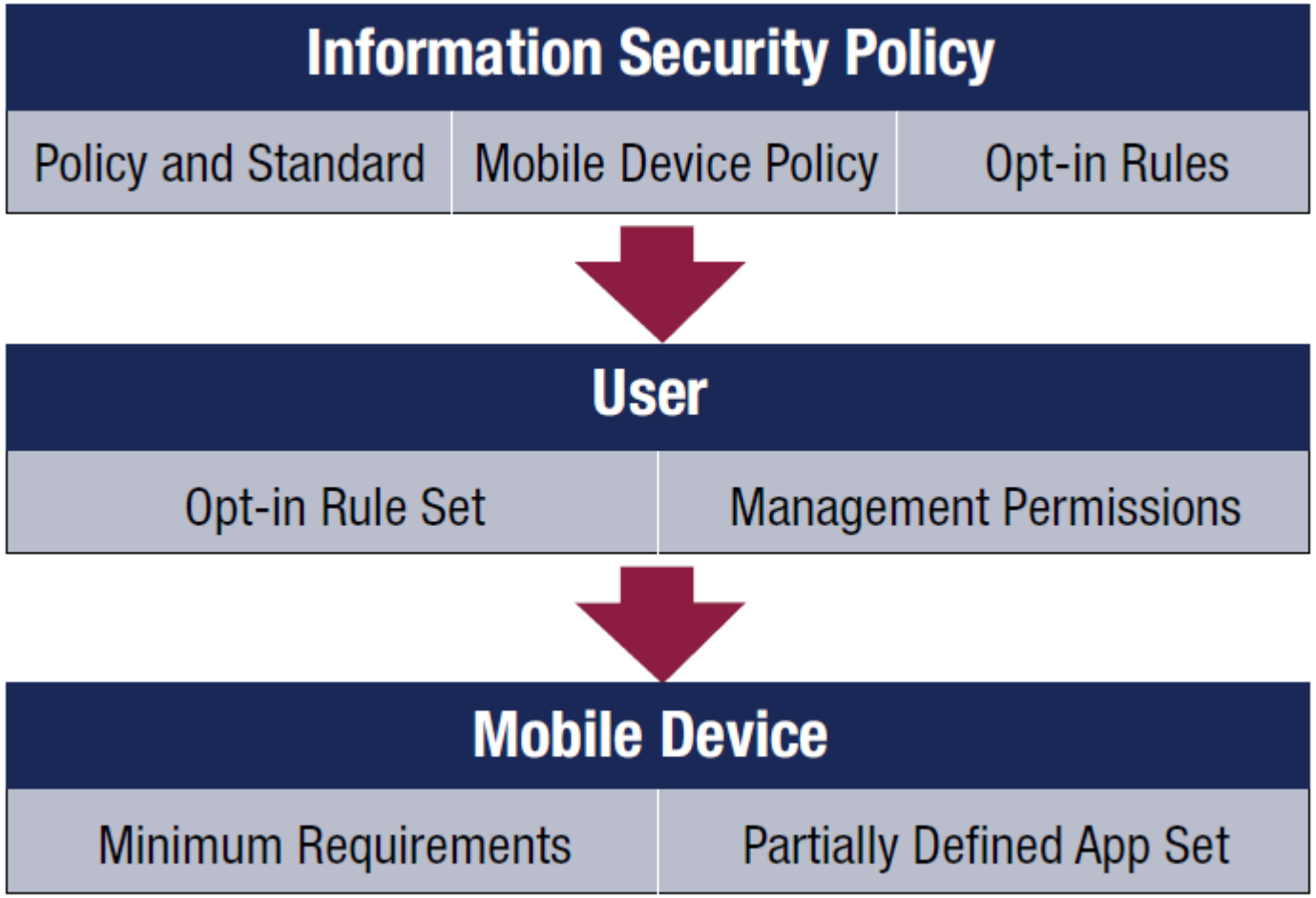
IBGP

Ciclo de Vida de um Dispositivo Móvel BYOD



IBGP

Solução Híbrida



IBGP

Ciclo de Vida de um Dispositivo Móvel na Solução Híbrida

Categorias de Dispositivos 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	• Smartphones • Early pocket PC devices
3	Data storage, processing and transmission capabilities via alternative channels, broadband Internet connectivity, standardized OS (configurable), PC-like capabilities	• Advanced smartphones • Tablet PCs

Quarta Categoria

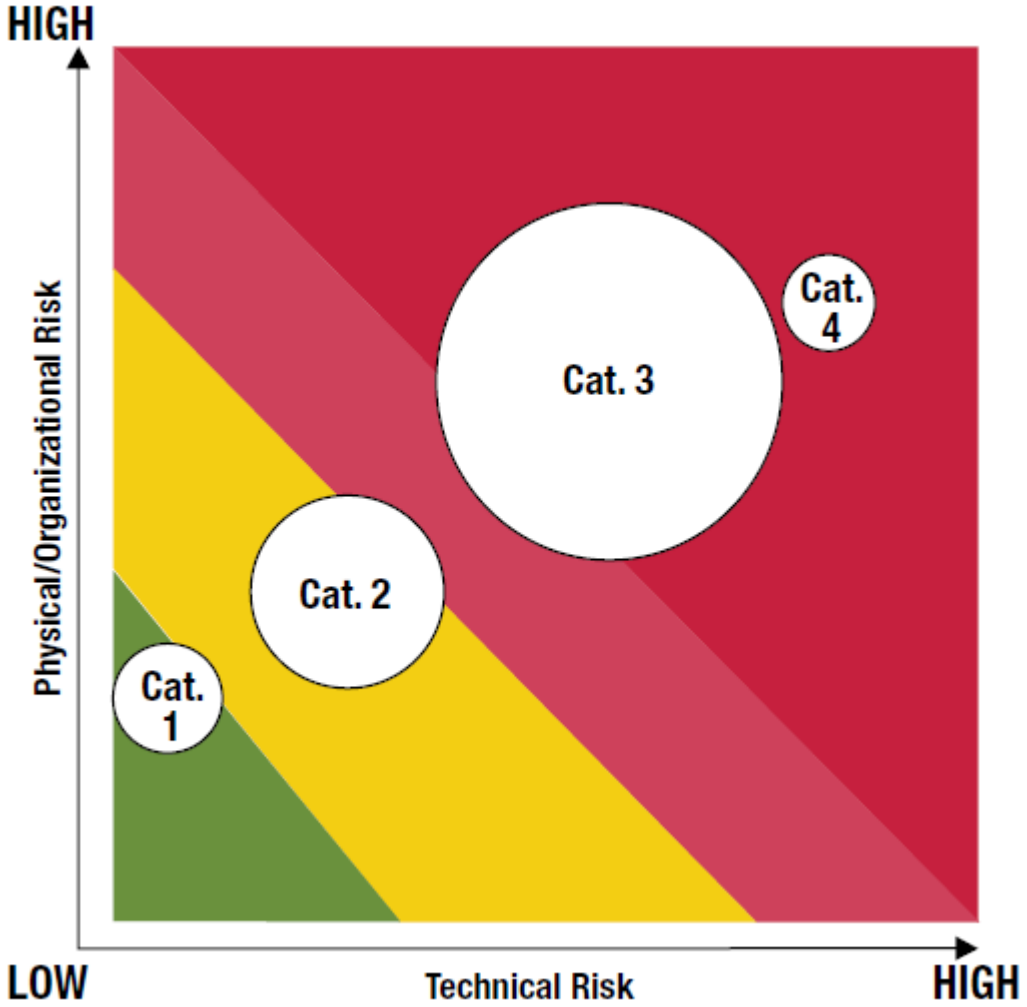
- Além dessas três categorias, uma quarta categoria está emergindo, que combina dispositivos avançados com dispositivos não-PC.
- Um exemplo, é a combinação de aparelhos eletrodomésticos ou brinquedos com smartphones, permitindo o controle remoto e outras características.

Classificação de Risco de Dispositivos Móveis

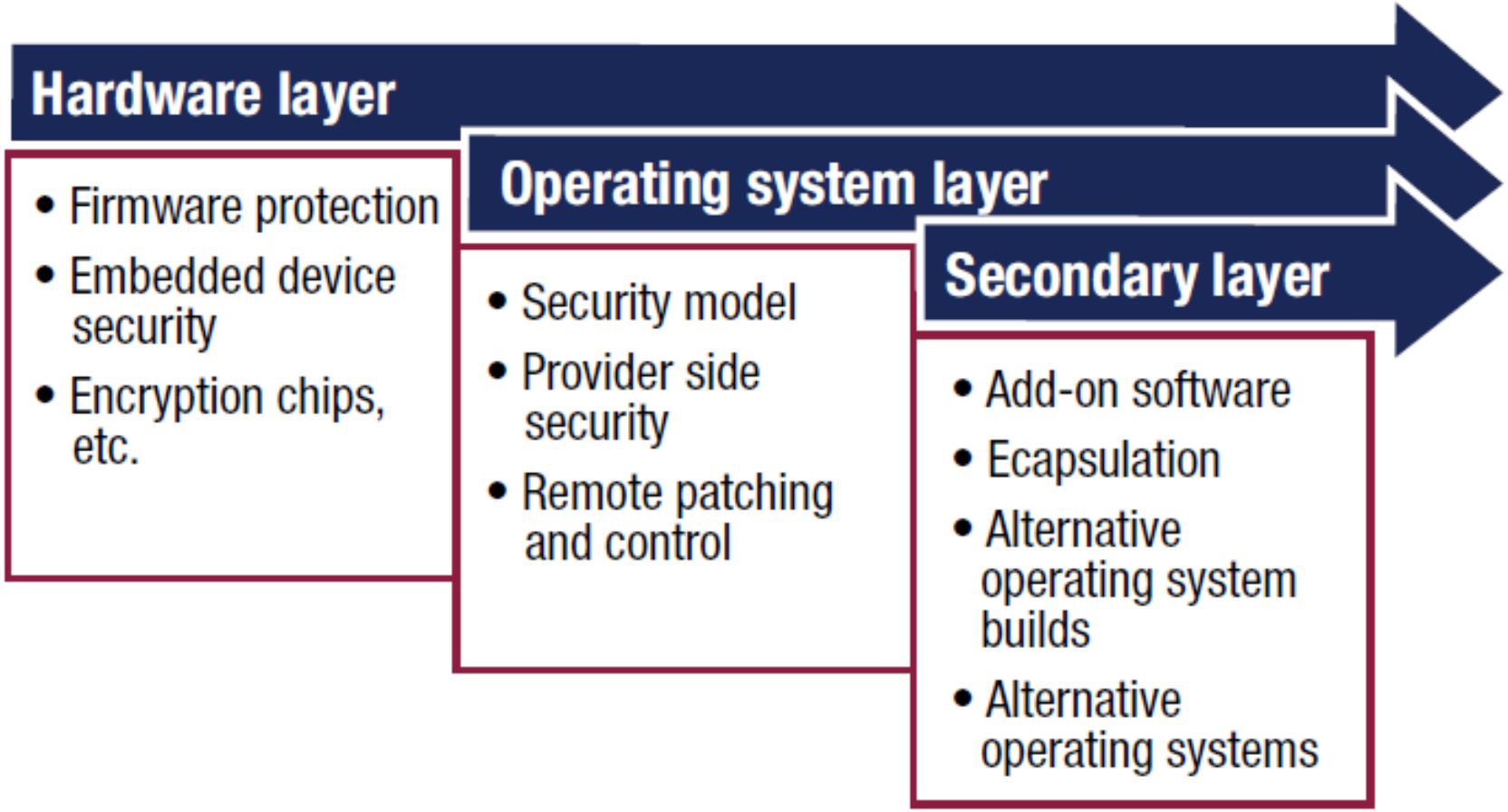
Category/Risk	Category 1	Category 2	Category 3	Category 4
Physical				
Theft	Low	Medium	High	High
Loss	Medium	Medium	Medium	Medium
Damage/destruction	High	High	Low	Low
Organizational				
Agglomeration/heavy users	Low	Low	High	High
Complexity/diversity	Low	Medium	High	High
Technical				
Activity monitoring, data retrieval	Low	High	High	High
Unauthorized network connectivity	Low	Medium	High	High
Web view/impersonation	Low	Medium	High	High
Sensitive data leakage	Low	High	High	High
Unsafe sensitive data storage	Medium	High	Medium	Medium
Unsafe sensitive data transmission	Low	High	Medium	High
Drive-by vulnerabilities	Low	High	High	High
Usability	Low	Low	High	High

IBGP

Mapa de Risco de Dispositivos Móveis



Camadas de Controles de Segurança



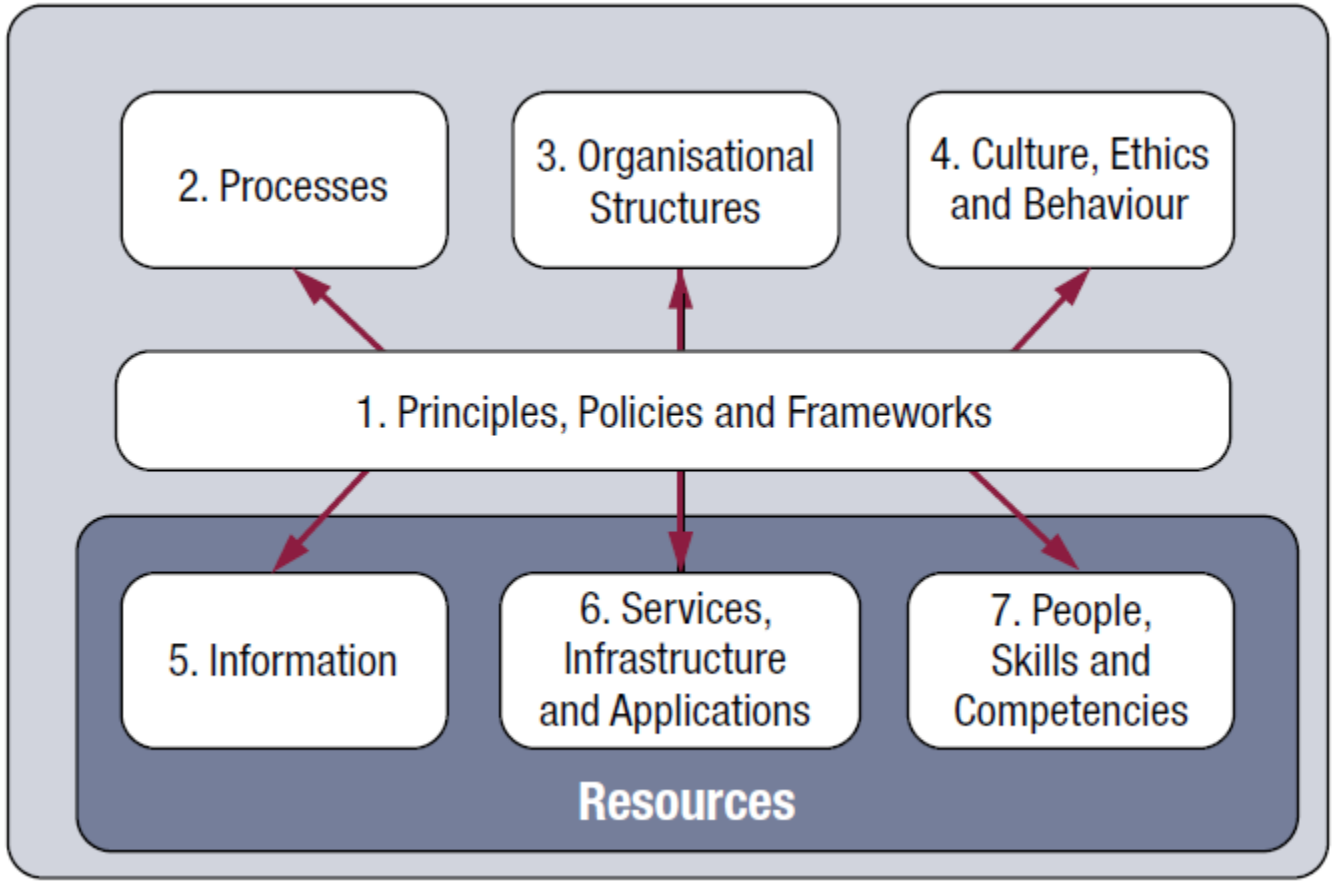
IBGP

COBIT 5 Process	Summary Description	Application to Mobile Device Security
DSS05.01 Protect against malware.	Implement measures to protect enterprise IT from the various types of malware.	Extend protective measures (e.g., third-party tools) to mobile devices, and ensure that they are functional and effective autonomously, without users having to bring in the device.
DSS05.02 Manage network and connectivity security.	Implement measures and restrictions for authentication, authorization and data transmission.	Use preapplied (device) controls to protect connectivity. Use additional tools for encryption and network/ device identification and authentication.
DSS05.03 Manage endpoint security.	Implement a security level equivalent to or greater than the normal organizational security level.	Use preapplied (device) controls to harden the device. Implement remote command and control to maintain system integrity.
DSS05.04 Manage user identity and logical access.	Manage rights in accordance with business needs and degree of risk/exposure.	Use preapplied (device) controls to enforce multifactor access. Extend existing practices, e.g., single sign-on, to the mobile device as appropriate.

Controles de Segurança COBIT 5 para Dispositivos Móveis

IBGP

Habilitadores do COBIT 5



1 - Políticas de Segurança

2 - Processos

- EDM01 Ensure governance framework setting and maintenance.
- EDM02 Ensure benefits delivery.
- EDM03 Ensure risk optimisation.
- EDM04 Ensure resource optimisation.
- EDM05 Ensure stakeholder transparency. cess
- APO01 Manage the IT management framework.
- APO02 Manage strategy.
- APO03 Manage enterprise architecture.
- APO04 Manage innovation.
- APO05 Manage portfolio.

IBGP

2 – Processos (cont.)

- APO06 Manage budget and costs.
- APO07 Manage human resources.
- APO09 Manage service agreements.
- APO10 Manage suppliers.
- BAI02 Manage requirements definition.
- BAI03 Manage solutions identification and build.
- BAI04 Manage availability and capacity.
- BAI06 Manage changes.
- BAI09 Manage assets.
- BAI10 Manage configuration.
- DSS03 Manage problems.

3 – Estrutura Organizacional

- Perfil do Gerente de Segurança da Informação

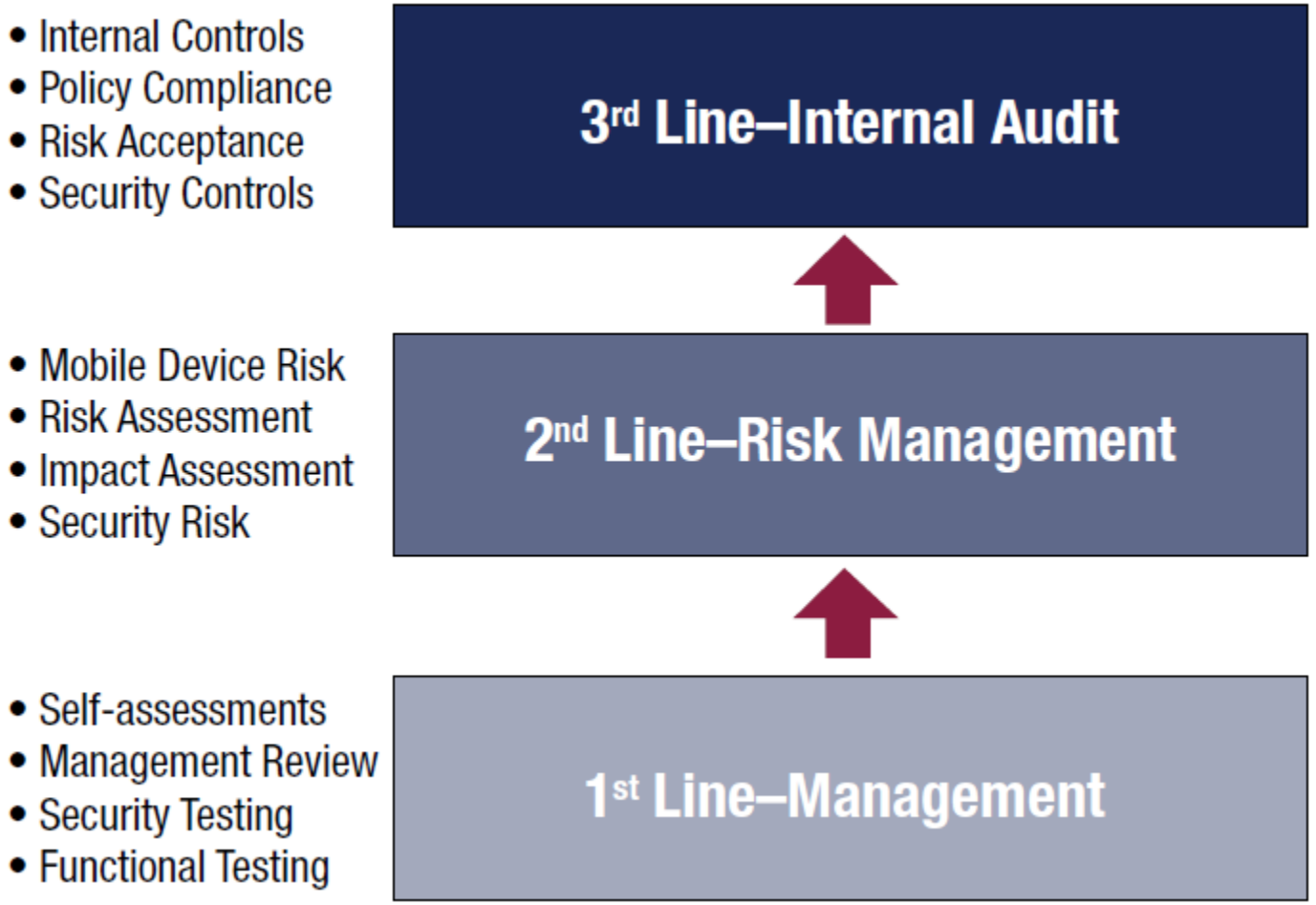
Area	Characteristic
Mandate	Overall responsibility for the management of information security efforts
Operating principles	Reports to the CISO (or, in some enterprises, to the business unit leads)
Span of control	Application information security, infrastructure information security, access management, threat management, risk management, awareness program, metrics, vendor assessments
Authority level/decision rights	Overall decision-making authority over information security domain practices
Delegation rights	Should not delegate decisions related to information security domain practice
Escalation path	Issues escalated to the CISO
Mobile device security	Accountability; responsibility in small and medium-sized enterprises, delegation to experts in larger enterprises

IBGP

4 – Cultura, Ética e Comportamento

Model Behavior	Application to Mobile Device Use
Information security is practiced in daily operations.	Security management and monitoring processes are applied to mobile devices to the agreed extent (standardized/BYOD/combined). End users understand and apply security measures completely and in a timely manner.
People respect the importance of information security principles and policies.	Users are aware of, and ideally actively involved in, defining mobile device security principles and policies. These are updated frequently to reflect day-to-day reality as experienced by the users.
People are provided with sufficient and detailed information security guidance and are encouraged to participate in and challenge the current information security situation.	Mobile device security is a fluid process with regular challenges by users. Security guidance for mobile devices is simple, to the point and relates to typical day-to-day security risk. The security situation is frequently and jointly assessed by users and security managers.
Everyone is accountable for the protection of	Security managers and users share

Linhas de Defesa



IBGP

Princípios da Segurança de Dispositivos Móveis

- Princípio 1: Conheça o valor para o negócio e o risco de uso dos dispositivos móveis.
- Princípio 2: Defina claramente o caso de negócio para o uso de dispositivos móveis.
- Princípio 3: Estabelecer uma segurança sistêmica para dispositivos móveis.
- Princípio 4: Estabelecer a governança da segurança para dispositivos móveis.
- Princípio 5: Gerencie a segurança dos dispositivos móveis por meio de habilitadores.
- Princípio 6: Coloque a tecnologia de Segurança em contexto.
- Princípio 7: Conheça o universo e os objetivos da avaliação com garantia.
- Princípio 8: Forneça uma garantia razoável sobre a segurança dos dispositivos móveis.

IBGP

IBGP Instituto Brasileiro de GOVERNANÇA PÚBLICA

Uso de Dispositivos Móveis nas Organizações – BYOD Abordagem COBIT 5

Prof. Dr. J. Souza Neto,
PMP. CSX, COBIT-INCS, CGEIT, CRISC, CLOUDF, ITILF,
COBIT 5 Implementation, COBIT 5 Assessor,
Certified COBIT Assessor, COBIT 5 *Approved Trainer*
souzaneto@ibgp.net.br