

Aspectos Legais e Éticos da Segurança Cibernética – P2

Universidade de Fortaleza

4.1 Proteção de Dados Pessoais e Privacidade desde a Concepção



Aplicabilidade:

- Desenvolvimento de novos sistemas de Tecnologia da Informação (TI), serviços, produtos, projetos e processos que envolvam o tratamento de dados pessoais; Políticas, normas e regimentos internos;
- Designs físicos;
- Iniciativas de compartilhamento de dados;
- Uso de dados pessoais para novos propósitos

4.1 Proteção de Dados Pessoais e Privacidade desde a Concepção

Estratégia

As estratégias de minimizar, ocultar, separar e resumir caracterizam-se como medidas que orientam aspectos técnicos do tratamento, enquanto as estratégias de informar, controlar, aplicar e demonstrar relacionam-se a medidas organizacionais de proteção à privacidade

Medidas Técnicas



Minimizar



Esconder



Separar



Resumir

Medidas Organizacionais



Informar



Controlar



Demonstrar e
Responsabilizar

4.1 Proteção de Dados Pessoais e Privacidade desde a Concepção

Estratégias de implantação

- **Criação de política/Norma e POP**
- **Capacitação e conscientização**
- **Implantação de processo de aplicação/evidenciação**

Obs.: O problema da concretização do conceito – Ver ISO 31700

Check-list de PbD

Item	Resposta	Observação
1. Qual o produto, serviço, processo ou ação que está sendo desenvolvido?		
2. Qual o propósito do produto, serviço, processo ou ação que está sendo desenvolvido?		
2. Quais dados pessoais serão utilizados? (Liste)		
3. O projeto envolve dados sensíveis? (Liste)		
4. De quem são os dados que serão tratados? (Liste)		
5. A atividade envolverá dados de crianças, adolescentes, idosos e pessoas vulneráveis (presos, pessoas institucionalizadas e doentes inconscientes)		
6. Quais dados pessoais serão utilizados? (Liste)		
7. Qual o volume de titulares e dados pessoais envolvidos?		

Check-list de PbD

Item	Resposta	Observação
11. Qual a origem dos dados que serão utilizados?		
12. Os titulares são informados da coleta de seus dados? Se sim como?		
13. os titulares serão informados da utilização de seus dados? Se sim como?		
14. Será utilizado alguma aplicação, sistema ou recurso de tecnologia da informação? Se sim qual? Se sim esse recurso é próprio ou de terceiros? Se for de terceiro ele já foi avaliado pelas áreas de Privacidade e Segurança da Informação		
15. Você aplicou alguma estratégia de minimizar os dados utilizados? Se sim qual?		
16. Você aplicou alguma estratégia de esconder os dados utilizados? Se sim qual?		
17. Você aplicou alguma estratégia de separar os dados utilizados? Se sim qual?		
18. Você aplicou alguma estratégia de resumir os dados utilizados? Se sim qual?		
19. Você aplicou alguma estratégia de informar os dados utilizados? Se sim qual?		
20. Você aplicou alguma estratégia de Controle sobre os dados utilizados? Se sim qual?		

4.2 Gestão do consentimento

Relembrando

@ Um dos elementos centrais autorizando o tratamento de dados pessoais, mas não o único!

@ O consentimento deverá referir-se a finalidades determinadas;

@ As autorizações genéricas para o tratamento de dados pessoais são nulas;

Obs.: É dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

4.2 Gestão do consentimento

Relembrando

@ Requisitos e características do consentimento válido ([EDPB Guidelines 05/2020](#)):

- . Registro por escrito ou por outro meio idôneo
- . Cláusula destacada das demais cláusulas contratuais
- . Manifestação livre
- . Informada
- . Inequívoca
- . Finalidade determinada
- . Revogável

4.2 Gestão do consentimento

Relembrando

@ Direitos do titular (quem consente):

- Acesso facilitado às informações sobre o tratamento de seus dados;
- Informações disponibilizadas de forma clara, adequada e ostensiva sobre:
 - . Finalidade específica do tratamento;
 - . Forma e duração do tratamento (respeito ao segredo comercial e industrial);
 - . Identificação do controlador;
 - . Contato do controlador;
 - . Possível compartilhamento dos dados pelo controlador e a finalidade;
 - . Os outros direitos fixados no artigo 18 da LGPD.

4.2 Gestão do consentimento

Relembrando

@ Cuidado:

- . Necessidade de confirmação do consentimento caso houver mudança da finalidade para o tratamento de dados pessoais e esta não seja compatível com o consentimento original (aviso prévio e que autoriza a revogação do consentimento)
- . Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato.

4.2 Gestão do consentimento

Relembrando

@ Repetindo:

- Escrito ou outra forma capaz de demonstrar a manifestação de vontade;
- Livre e esclarecido e especificado (consentimento genérico é nulo);
- Deve constar de cláusula destacada das demais;
- Ônus de licitude do consentimento é do controlador;
- Revogável;
- Necessidade de atualização em casos de mudança da finalidade.

4.2 Gestão do consentimento

Gestão do Consentimento

PARTE 1 CONTEXTO E OPÇÕES

1a

Estágio atual

Como o consentimento é atualmente gerenciado?

- Captura
- Gestão
- Uso

PARTE 2 CUSTOMIZANDO O CONSENTIMENTO

2a

Captura do consentimento

- Que tipos de consentimento são mais adequados para a Empresa?
- Como nós iremos comunicar os clientes as opções de consentimento?

2b

Gestão do consentimento

- Que nível de controle será dado ao cliente para alterar suas preferências?
- Através de que canais?
- Como desenvolver uma gestão de consentimento eficiente?

2c

Operando o consentimento dentro da Empresa

- Quem tem que conhecer os “flags” de consentimento?
- Quais processos deverão utilizar os “flags” de consentimento?
- Quem é o responsável pelo modelo de consentimento?

PARTE 3 IMPLANTANDO O NOVO MODELO

3a

Atualização do modelo de consentimento

- Como atualizar os processos de negócio?
- Como atualização os flags de sistemas?
- Como atualizar as interfaces de front-end para gestão da captura e preferências?
- Quando faremos pesquisas com clientes?

3b

Preparando o time

Qual o conteúdo do treinamento e comunicação para:

- Times de atendimento a cliente
- Marketing/ Analytics/ RH
- Operações de Dados

3c

Transferindo o consentimento atual para o modelo novo

- Como será o modelo de transferência para evitar re-opt-in para clientes atuais?
- Como será feita a transferência de flags de sistemas?
- Como estruturar a campanha de marketing informando atualizações?

(DIGITALJUD, 2019)

4.2 Gestão do consentimento

Gestão do Consentimento:

- Mapeamento
- Definição do processo de coleta/recebimento/validação
- Centrais ou canais de preferência

4.3 Avaliações e Gerenciamento de Fornecedores

Governança de parceiros (Operadores e Terceiros)

Objetivos:

- Mapeamento adequado do fornecedor (Fiscal, Trab., DP, Reputacional...);
- Identificação de riscos;
- Avaliação de riscos;
- Mitigação/Assunção;
- Avaliação contínua;

4.3 Avaliações e Gerenciamento de Fornecedores

Governança de parceiros (Operadores e Terceiros)

@ Mapeamento adequado do fornecedor:

- Estabelecimento de um processo/área;
- Tipos de informações que devem ser levantadas;
- Foco na relação com dados pessoais;
- Forma de coleta dessas informações:
 - . Avaliação passiva;
 - . Avaliação ativa;
 - . Método combinado.

4.3 Avaliações e Gerenciamento de Fornecedores

Governança de parceiros (Operadores e Terceiros)

@ Identificação de riscos dos fornecedores

- Avaliação das áreas de negócio, GRC, SI e PDP

- Eleição da biblioteca de riscos:

- . Priorização de itens relacionados a LGPD:

- a) Legais

- b) Organizacionais

- c) Segurança da informação

- . Inclusão de aspectos relacionados à área de negócio

4.3 Avaliações e Gerenciamento de Fornecedores

Governança de parceiros (Operadores e Terceiros)

@ Avaliação de riscos dos fornecedores

- Construção da matriz e da metodologia de avaliação
- Definição do apetite ao risco (Levar em consideração a criticidade do fornecedor e da área afetada);

@Mitigação/Assunção;

- Indicação de medidas e responsáveis para o acompanhamento;
- Contratação de seguros;

4.3 Avaliações e Gerenciamento de Fornecedores

Medidas de proteção de dados pessoais			
No contrato firmado com o parceiro, há Acordo de Tratamento de Dados Pessoais?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>
No contrato firmado com o parceiro, há cláusula de privacidade de tratamento de dados pessoais?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>
Parceiro tem Política de Privacidade?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>
Parceiro tem Política de Segurança da Informação?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>
Parceiro tem plano de resposta a incidentes de segurança da informação?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>
Parceiro nomeou Encarregado de Proteção de Dados Pessoais/Data Protection Officer?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>
Titular é informado sobre com qual(is) parceiro(s) seus dados são compartilhados?	Sim <input type="checkbox"/>	Não <input type="checkbox"/>	Não sabe informar <input type="checkbox"/>


4.4 Gestão da Transferência Internacional de Dados Pessoais

Medidas de prevenção e minimização de riscos regulatórios e operacionais:

- a) Mapeamento das atividades com transferência internacional;
- b) Avaliação dos riscos regulatórios do país de destino;
- c) Avaliação mínima de PDP e SI do fornecedor;
- d) Uso das bases legais que não exigem intervenção da ANPD;
- e) Estruturação de plano de migração capaz de evitar impactos operacionais.

5.1 Aspectos práticos de segurança da informação

Introdução a SI

- Para definir segurança, tornou-se comum o uso da tríade Confidencialidade, Integridade e Disponibilidade – CID. O objetivo desses termos é descrever a segurança usando palavras relevantes e significativas que tornam a segurança mais compreensível para o gerenciamento e os usuários e definem sua finalidade (ISACA, 2022).
- 

5.1 Aspectos práticos de segurança da informação



Confidencialidade: Protege os dados que precisam de proteção e permite o acesso a pessoas autorizadas enquanto impede o acesso a indivíduos não autorizados.

Integridade: Garantia que os dados não foram alterados de forma não autorizada.

Disponibilidade: Garantir que os dados estejam acessíveis a usuários autorizados quando e onde forem necessários, e na forma e formato requeridos.

5.1 Aspectos práticos de segurança da informação

Confidencialidade: A característica dos dados ou informações quando não são disponibilizados ou divulgados a pessoas ou processos não autorizados (NIST 800-66)

Medidas de proteção a confidencialidade:

5.1 Aspectos práticos de segurança da informação

Integridade: Integridade mede o grau em que algo é inteiro e completo, internamente consistente e correto. O conceito de integridade se aplica a: i) informações ou dados; ii) sistemas e processos para operações de negócios; iii) organizações; e iv) pessoas e suas ações.

Medidas de proteção a integridade:

5.1 Aspectos práticos de segurança da informação

Disponibilidade: A disponibilidade pode ser definida como (i) acesso oportuno e confiável à informação e a capacidade de usá-la, e (ii) para usuários autorizados, acesso oportuno e confiável a dados e serviços de informação.

Obs.: Criticidade - Uma medida do grau em que uma organização depende da informação ou sistema de informação para o sucesso de uma missão ou de uma função de negócios. NIST SP 800-60 vol. 1, Rev. 1

Medidas de proteção a disponibilidade:

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Os profissionais de segurança usam seus conhecimentos e habilidades para examinar o gerenciamento de risco operacional, determinar como usar os dados de risco de forma eficaz, trabalhar multifuncionalmente e relatar informações e descobertas acionáveis às partes interessadas. Termos como ameaças, vulnerabilidades e ativos são familiares para a maioria dos profissionais de segurança cibernética.

- Um **ativo** é algo que precisa de proteção.
- Uma **vulnerabilidade** é uma lacuna ou fraqueza nesses esforços de proteção.
- Uma **ameaça** é algo ou alguém que visa explorar uma vulnerabilidade para frustrar os esforços de proteção.

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Ativo

Qualquer coisa de valor pertencente a uma organização. Os ativos incluem itens tangíveis, como sistemas de informação e propriedade física, e ativos intangíveis, como propriedade intelectual.

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Vulnerabilidade

Fraqueza em um sistema de informação, procedimentos de segurança do sistema, controles internos ou implementação que pode ser explorada por uma fonte de ameaça. Fonte: NIST SP 800-128

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Ameaça

Qualquer circunstância ou evento com potencial para impactar adversamente as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais, indivíduos, outras organizações ou a nação por meio de um sistema de informação por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço.

Fonte: NIST SP 800-30 Rev 1

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Ameaça

Uma ameaça é uma pessoa ou coisa que toma medidas para explorar (ou fazer uso de) as vulnerabilidades do sistema de uma organização-alvo, como parte de atingir ou promover sua meta ou objetivos.

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Ameaça

No contexto da segurança cibernética, os agentes típicos de ameaças incluem o seguinte:

- Insiders (deliberadamente, por simples erro humano ou por incompetência grosseira).
- Indivíduos externos ou grupos informais (planejados ou oportunistas, descobrindo a vulnerabilidade).
- Entidades formais não políticas (como concorrentes de negócios e cibercriminosos).

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Ameaça

No contexto da segurança cibernética, os agentes típicos de ameaças incluem o seguinte:

- Entidades formais que são políticas (como terroristas, nações-estado e hacktivistas).
- Coletores de inteligência ou informações (pode ser qualquer um dos itens acima).
- Tecnologia (como bots de execução livre e inteligência artificial , que podem fazer parte de qualquer um dos itens acima).

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Controles de Segurança

Os controles de segurança referem-se aos mecanismos físicos, técnicos e administrativos que atuam como salvaguardas ou contramedidas prescritas para um sistema de informação para proteger a confidencialidade, integridade e disponibilidade do sistema e de suas informações. A implementação de controles deve reduzir o risco, esperançosamente a um nível aceitável.



5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Controles de Segurança Físicos

Os controles físicos atendem às necessidades de segurança baseadas em processos usando dispositivos físicos de hardware, como leitores de crachás, características arquitetônicas de prédios e instalações e ações de segurança específicas a serem tomadas pelas pessoas. Eles normalmente fornecem maneiras de controlar, direcionar ou impedir o movimento de pessoas e equipamentos em um local físico específico, como um escritório, fábrica ou outra instalação. Os controles físicos também fornecem proteção e controle sobre a entrada no terreno ao redor dos prédios, estacionamentos ou outras áreas que estão sob o controle da organização. Na maioria das situações, os controles físicos são apoiados por controles técnicos como forma de incorporá-los a um sistema de segurança geral.

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Controles de Segurança Técnicos

Os controles técnicos (também chamados de controles lógicos) são controles de segurança que os sistemas e redes de computadores implementam diretamente. Esses controles podem fornecer proteção automatizada contra acesso não autorizado ou uso indevido, facilitar a detecção de violações de segurança e atender aos requisitos de segurança de aplicativos e dados. Os controles técnicos podem ser definições de configuração ou parâmetros armazenados como dados, gerenciados por meio de uma interface gráfica do usuário (GUI) de software, ou podem ser configurações de hardware feitas com interruptores, plugues de jumper ou outros meios. No entanto, a implementação de controles técnicos sempre requer considerações operacionais significativas e deve ser consistente com o gerenciamento de segurança dentro da organização.

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

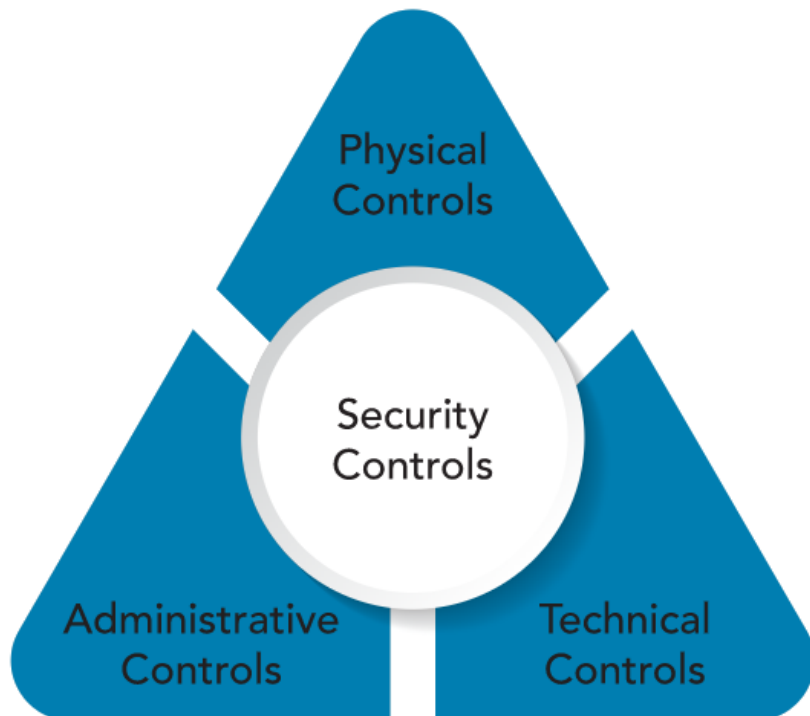
Controles de Segurança Administrativos

Os controles administrativos (também conhecidos como controles gerenciais) são diretrizes, guias ou conselhos dirigidos às pessoas dentro da organização. Eles fornecem estruturas, restrições e padrões para o comportamento humano e devem cobrir todo o escopo das atividades da organização e suas interações com partes externas e partes interessadas.

5.1 Aspectos práticos de segurança da informação

Terminologia de Gerenciamento de Risco aplicada a SI:

Controles de Segurança Administrativos

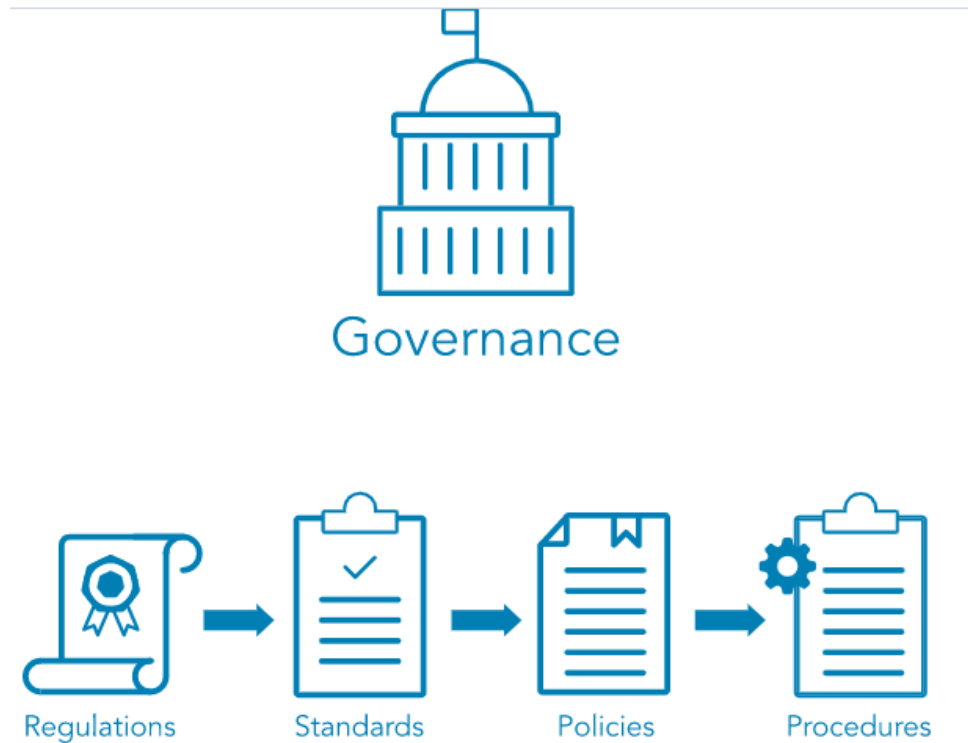


Administrative Control	Physical Control	Technical Control
Acceptable Use Policy	Badge Reader	Access Control List
Emergency Operations Procedures	Stop Sign in Parking Lot	
Employee Awareness Training	Door Lock	

5.1 Aspectos práticos de segurança da informação

Elementos de governança aplicadas a SI:

Elementos estruturais



5.1 Aspectos práticos de segurança da informação

Elementos de governança aplicadas a SI:

Elementos estruturais

- Os regulamentos são comumente emitidos na forma de leis, geralmente do governo (não confundir com governança) e geralmente acarretam penalidades financeiras por descumprimento.
- Os padrões são freqüentemente usados pelas equipes de governança para fornecer uma estrutura para introduzir políticas e procedimentos de apoio aos regulamentos.

5.1 Aspectos práticos de segurança da informação

Elementos de governança aplicadas a SI:

Elementos estruturais

- As políticas são implementadas pela governança organizacional, como a gestão executiva, para fornecer orientação em todas as atividades para garantir que a organização apoie os padrões e regulamentos do setor.
- Os procedimentos são as etapas detalhadas para concluir uma tarefa que oferece suporte às políticas departamentais ou organizacionais.

5.2 Construindo e implantando uma PSI

Etapas do processo de criação e implantação de uma PSI:

- Planejamento
- Implantação
- Monitoramento

5.2 Construindo e implantando uma PSI

Elementos de uma PSI (ISO 27001)

5.2 Política

A Alta Direção deve estabelecer uma política de segurança da informação que:

- a) seja apropriada ao propósito da organização;
- b) inclua os objetivos de segurança da informação (ver 6.2) ou forneça a estrutura para estabelecer os objetivos de segurança da informação;
- c) inclua o comprometimento de satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;
- d) inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

5.2 Construindo e implantando uma PSI

Elementos de uma PSI:

- Definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- Declaração do comprometimento da alta administração com a PSI, apoiando suas metas e princípios;
- Objetivos de segurança da instituição;
- Definição de responsabilidades gerais na gestão de segurança de informações;

5.2 Construindo e implantando uma PSI

Elementos de uma PSI:

- Orientações sobre análise e gerência de riscos;
- Princípios de conformidade dos sistemas informacionais com a PSI;
- Padrões mínimos de qualidade que esses sistemas devem possuir;
- Regras de controle de acesso a recursos e ativos;
- Regras de classificação das informações (de uso irrestrito, interno, confidencial e secretas);


5.2 Construindo e implantando uma PSI

Elementos de uma PSI:

- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- Princípios de supervisão constante das tentativas de violação da segurança de informações;
- Consequências de violações de normas estabelecidas na política de segurança;
- Princípios de gestão da continuidade do negócio e recuperação de desastre;
- Plano de treinamento em segurança de informações.

5.2 Construindo e implantando uma PSI

Implantação de uma PSI:

- i. Identificação dos recursos críticos;
 - ii. Classificação das informações e ativos;
 - iii. Definição, em linhas gerais, dos objetivos de segurança a serem atingidos;
 - iv. Análise das necessidades de segurança (identificação das possíveis ameaças, análise de riscos e impactos);
 - v. Elaboração de proposta de política;
- 

5.2 Construindo e implantando uma PSI

Implantação de uma PSI:

- vi. Discussões abertas com os envolvidos;
- vii. Apresentação de documento formal à alta administração;
- viii. Aprovação;
- ix. Publicação e divulgação;
- x. Treinamento e implementação;
- xi. Avaliação e identificação das mudanças necessárias e revisão.

5.3 Processo de Resposta Incidentes com Dados Pessoais

Notificações de incidentes

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional

- A) a descrição da natureza dos dados pessoais afetados;
- B) as informações sobre os titulares envolvidos;
- C) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- D) os riscos relacionados ao incidente e as medidas que foram adotadas para reverter ou mitigar os efeitos do prejuízo.

5.3 Processo de Resposta Incidentes com Dados Pessoais

Notificações de incidentes

Incidente de Segurança

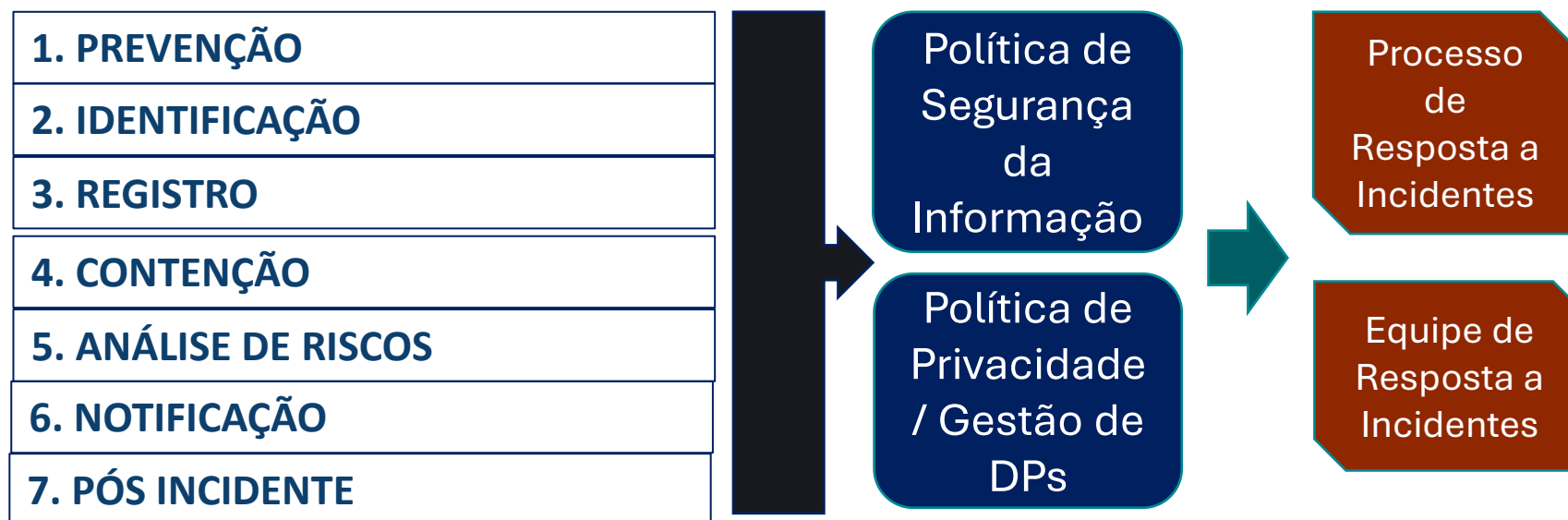
Qualquer violação à Política de Segurança da Informação, bem como qualquer **evento adverso**, indiferente de ser **confirmado ou sob suspeita**, que comprometa ou possa comprometer um dos três pilares da segurança da informação: **Confidencialidade, Integridade e Disponibilidade**.

Incidente de Segurança com Dados Pessoais

Qualquer **evento adverso**, indiferente de ser confirmado ou sob suspeita, relacionado à **violação na segurança de DADOS PESSOAIS**.

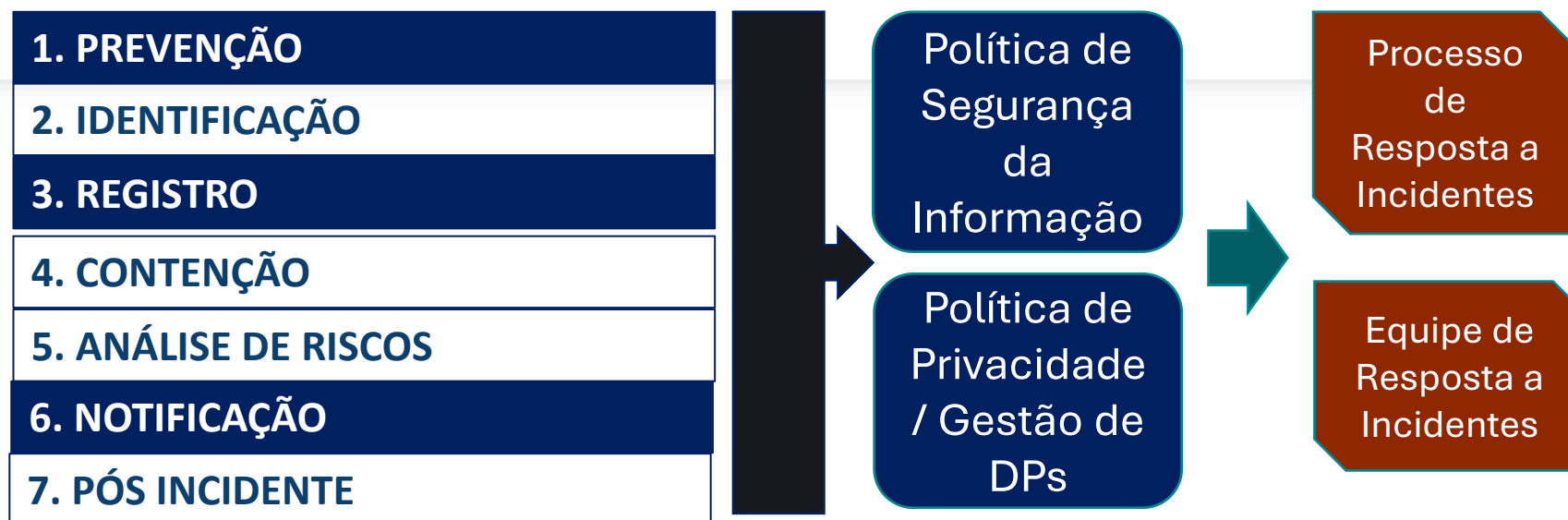
5.3 Processo de Resposta Incidentes com Dados Pessoais

Gestão de incidentes



5.3 Processo de Resposta Incidentes com Dados Pessoais

Gestão de incidentes



5.3 Processo de Resposta Incidentes com Dados Pessoais

PREVENÇÃO

Realizar avaliações de impacto a privacidade antes de iniciar qualquer projeto ou implementar qualquer tecnologia que contemple dados pessoais. Nos casos de **alto risco**, tomar as **medidas técnicas e organizacionais** apropriadas para proteger os dados pessoais contra incidentes.

Boas Práticas de Governança

**Políticas, Normas e
Procedimentos**

Ações educativas

**Mecanismos internos de supervisão
e de mitigação de riscos**

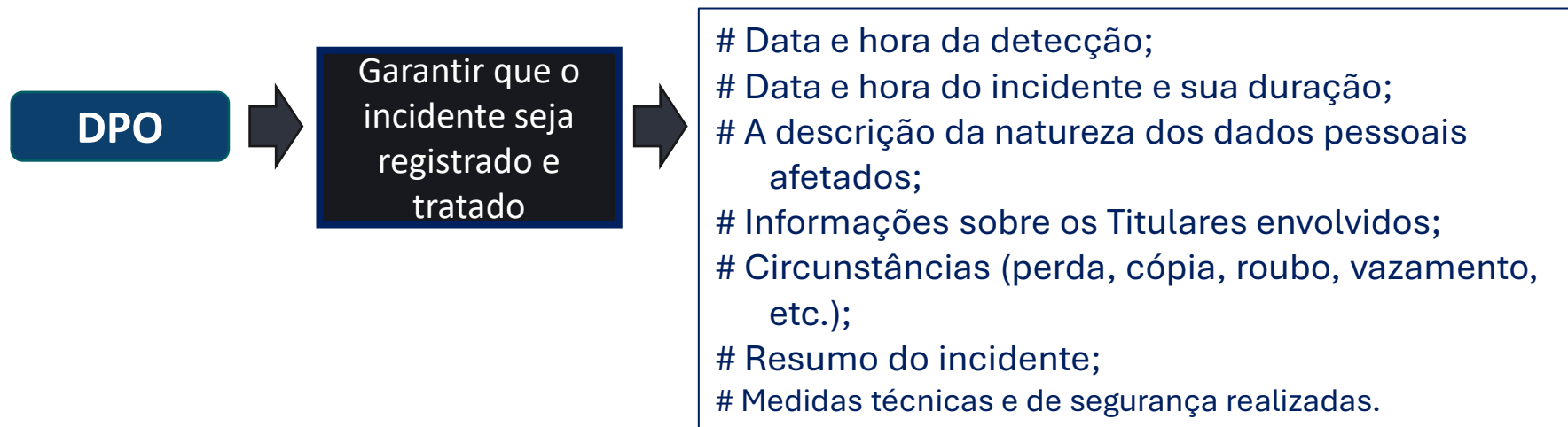
5.3 Processo de Resposta Incidentes com Dados Pessoais

REGISTRO



5.3 Processo de Resposta Incidentes com Dados Pessoais

REGISTRO



5.3 Processo de Resposta Incidentes com Dados Pessoais

NOTIFICAÇÃO

1. ANPD

2. CONTROLADOR

3. AVISO AOS TITULARES

4. DECISÃO DE NÃO NOTIFICAÇÃO

5.3 Processo de Resposta Incidentes com Dados Pessoais

NOTIFICAÇÃO

1. ANPD

2. CONTROLADOR

3. AVISO AOS TITULARES

4. DECISÃO DE NÃO NOTIFICAÇÃO

5.3 Processo de Resposta Incidentes com Dados Pessoais

NOTIFICAÇÃO



5.3 Processo de Resposta Incidentes com Dados Pessoais

NOTIFICAÇÃO

3. AVISO AOS TITULARES



Os Titulares de dados devem ser comunicados pelo controlador sobre a ocorrência de incidente de violação de Dados Pessoais que possa resultar em **RISCO** ou **DANO** relevante.

A comunicação deverá ser:

- @ Em linguagem clara e simplificada;
- @ Por meios que maximizem as chances de comunicação das informações a todos os Titulares dos dados afetados.

5.3 Processo de Resposta Incidentes com Dados Pessoais



FLUXO DE RESPOSTA A INCIDENTES COM DADOS PESSOAIS*

5.3 Processo de Resposta Incidentes com Dados Pessoais

Novo

Detectar

1. Sistemas de monitoramento SI
2. Colaboradores
3. Formulário
4. Automação
5. E-mail

Registrar

1. Ferramenta de gestão de privacidade e de SI.

5.3 Processo de Resposta Incidentes com Dados Pessoais

Novo

Acionar equipe de resposta

1. Envio de e-mail (Após o registro do incidente)
2. Envio de mensagem e contato telefônico (Eventos de médio e alto impacto)
3. Formalização de ata de mobilização do time de resposta à incidentes*

5.3 Processo de Resposta Incidentes com Dados Pessoais

Respondendo

Avaliar dimensão e riscos

1. Elaborar avaliação do impacto do incidente para os titulares dos dados pessoais (DPO)
2. Submeter avaliação ao ERI
3. Comunicar avaliação a Diretoria

Responder (Escalar/delegar)

1. Elaborar e executar plano de resposta ao incidente
2. Implantar medidas de contenção e resposta (Time Técnico)
3. Elaborar e executar plano de comunicação

Comunicação

1. Caso necessário seja comunicar:
 - a) Diretoria
 - b) ANPD
 - c) Titulares afetados
 - d) Sociedade/Mercado

5.3 Processo de Resposta Incidentes com Dados Pessoais

Solucionado

Resolver

1. Elaborar relatório de encerramento do incidente
2. Adoção das medidas técnicas, administrativas e legais cabíveis

Extra – EPD

Atribuições



Mapeamento de dados



Gestão de avisos e políticas



Solicitações dos titulares de dados
(DSAR)



Treinamento de conscientização



Gestão de riscos dos fornecedores



Conformidade de cookies



Resposta ao incidente



**Orientar stakeholders
quanto a proteção de
dados pessoais**

Extra – EPD

Treinamento

Certificações pessoais
(colaboradores)



Certified Information Privacy Professional
Certified Information Privacy Manager
Certified Information Privacy Technologists
Certificado no Brasil (CDPO/BR)



HealthCare Information
Security
and Privacy Practitioner



Trilha DPO

Certificações
institucionais



ISO 27.000 e 27.701*

Extra – O Processo de fiscalização

- Ciclos de fiscalização
- Fiscalização direta
- Orientação e depois punição*



Obrigado

joao@cmslaw.com.br
85 99812 6572