16º Seminário de Proteção à Privacidades e aos Dados Pessoais

Segurança e Privacidade da Informação – Conformidade com as Normas ISO e ABNT

Prof. Anderson Oliveira da Silva

linkedin.com/in/anderson-oliveira-da-silva-58221680

Gestor de Segurança da Informação
Encarregado de Dados Pessoais
anderson@inf.puc-rio.br

DEPARTAMENTO DE INFORMÁTICA PUC-RIO

PUC RIO

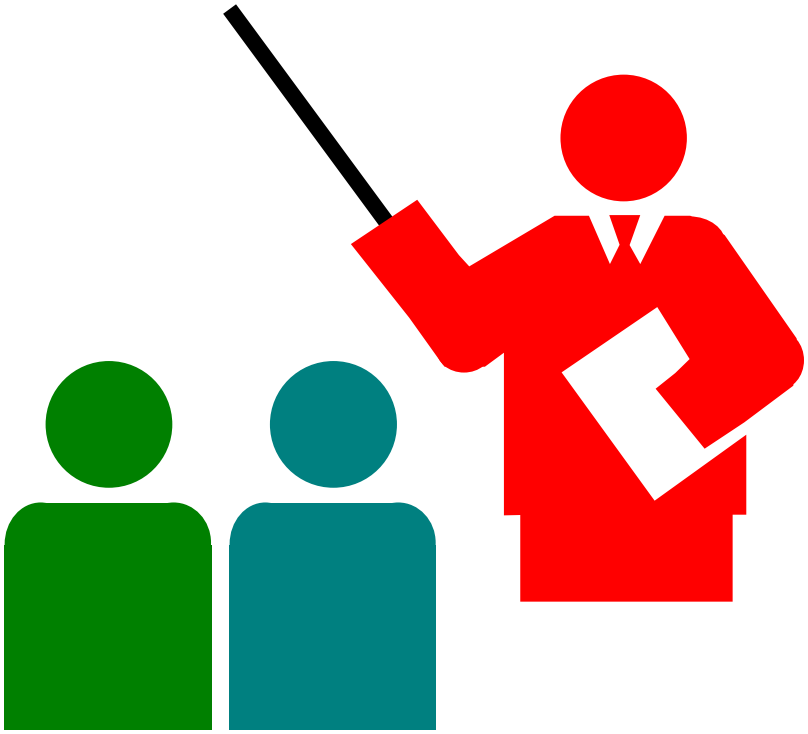
nic.br cgi.br

Ementa

Segurança e Privacidade da Informação – Conformidade com as Normas ISO e ABNT

- Proteção da Informação
- Compliance
- Pontos-Chaves
- ABNT NBR ISO/IEC 29100 – Estrutura de Privacidade
- ABNT NBR ISO/IEC 27001 – SGSI
- ABNT NBR ISO/IEC 27701 – SGPI
  - Extensão da ABNT NBR ISO/IEC 27001 e 27002
  - Controles Adicionais para Proteção da Privacidade

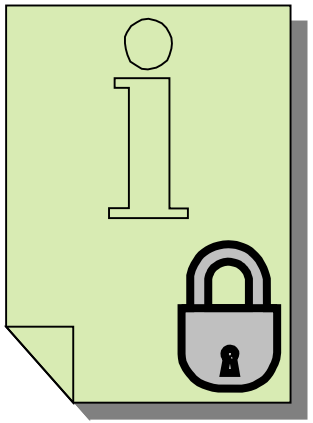
Segurança e Privacidade da Informação – Conformidade com as Normas ISO e ABNT



Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

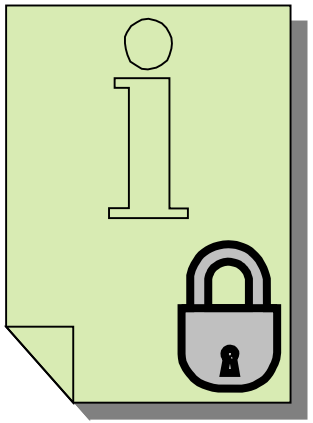
(Thomas R. Peltier, 2001)



Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

(Thomas R. Peltier, 2001)

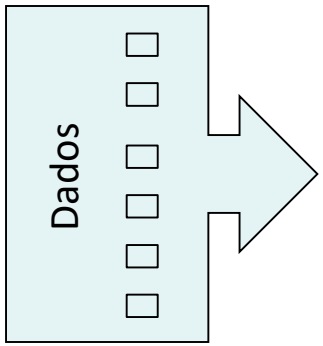


- **Por que os recursos de informação são valiosos para uma empresa?**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **As empresas diariamente produzem uma enorme quantidade de dados...**



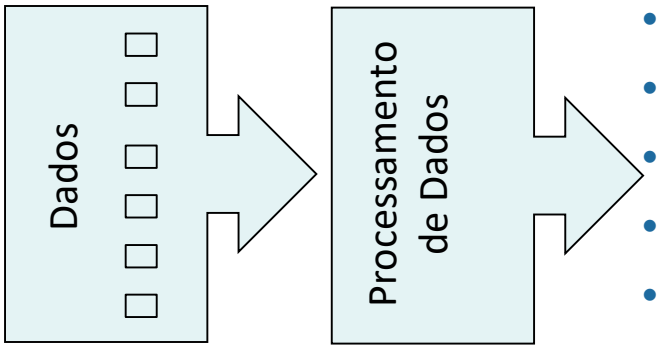
matéria-prima

- **Dados são elementos básicos, sem contexto ou significado específico, que podem ser quantificados, medidos ou observados.**
  - **Números: 55, 21, 3527, 1500, 225, 3, 15.000, ...**
  - **Palavras: Anderson, Silva, Marquês, São, Vicente, Brasil, Rio, Janeiro, PUC, INF, Gávea, Rua, ...**
  - **Símbolos: $, %, #, @, &, ...**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que servem como matéria-prima para o processamento de dados...**



matéria-prima

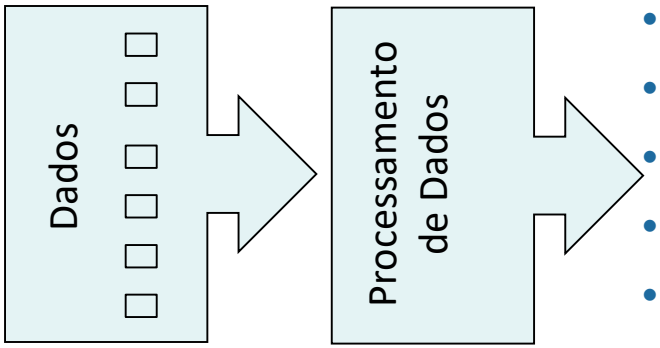
organização ou estruturação dos dados

- **Nome: Anderson da Silva**
- **Idade: 55**
- **Telefone: 21 3527-1500**
- **Local: Rua Marquês de São Vicente, 225**
- **Bairro: Gávea**
- **Cidade: Rio de Janeiro**
- **Empresa: PUC-Rio**
- **Departamento: INF**
- **E-mail: anderson@inf.puc-rio.br**
- **Salário-base: R$ 15.000,00**
- **Anuênio: 3,0%**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que servem como matéria-prima para o processamento de dados...**



matéria-prima

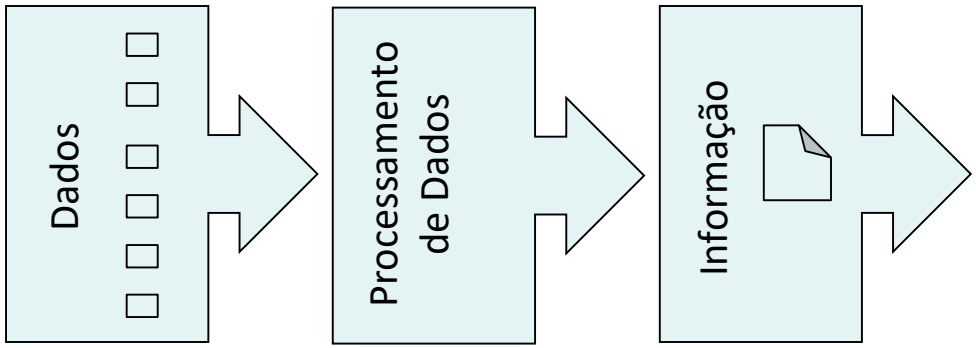
organização ou estruturação dos dados

- Exportador: Anderson & Silva
- Código do item: 55-21-3527
- Quantidade: 1500
- Destino: Rua Marquês de São Vicente, 225
- Bairro: Gávea
- Cidade: Rio de Janeiro
- Importador: PUC-Rio
- Departamento: INF
- E-mail: anderson@inf.puc-rio.br
- Valor do item: R$ 15.000,00
- Taxa de frete: 3,0%

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que produz informação (produto intermediário)...**



matéria-prima

organização ou estruturação dos dados

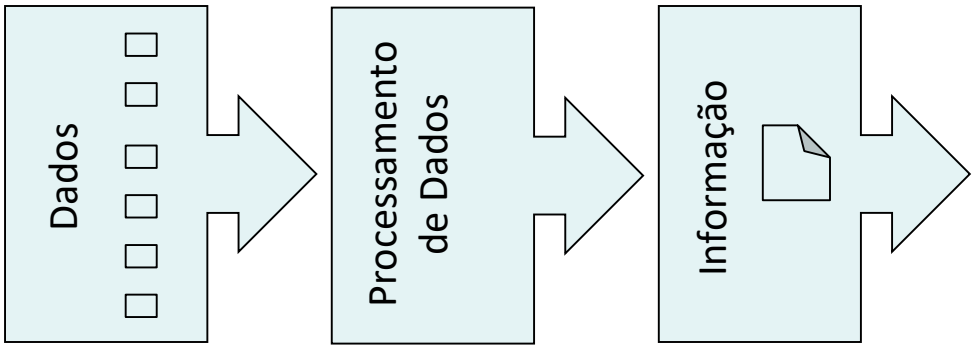
produto intermediário

- **Informação de identificação pessoal**
  - Nome: Anderson da Silva
  - Idade: 55
  - Telefone: 21 3527-1500
  - Local: Rua Marquês de São Vicente, 225
  - Bairro: Gávea
  - Cidade: Rio de Janeiro
  - Empresa: PUC-Rio
  - Departamento: INF
  - E-mail: anderson@inf.puc-rio.br
  - Salário-base: R$ 15.000,00
  - Anuênio: 3,0%

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...que produz informação (produto intermediário)...**



matéria-prima

organização ou estruturação dos dados

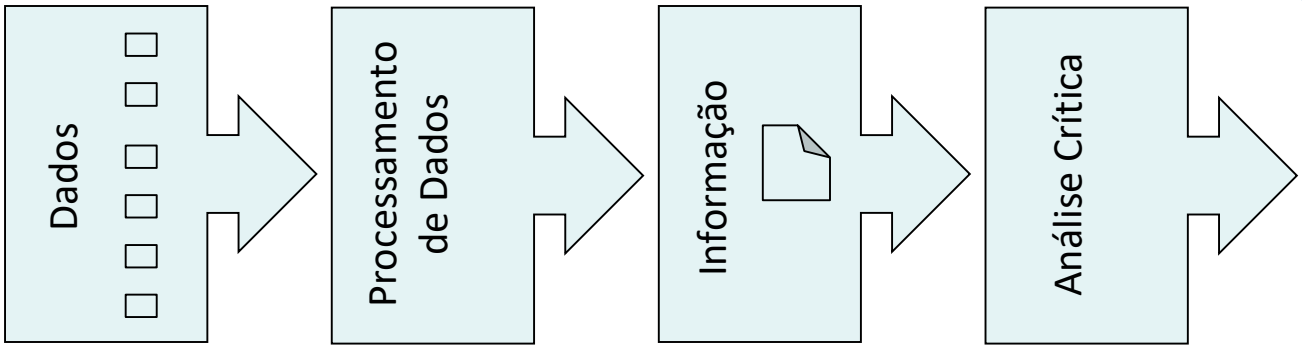
produto intermediário

- **Informação de importação de produto**
  - Exportador: Anderson & Silva
  - Código do item: 55-21-3527
  - Quantidade: 1500
  - Destino: Marquês de São Vicente, 225
  - Bairro: Gávea
  - Cidade: Rio de Janeiro
  - Empregador: PUC-Rio
  - Departamento: INF
  - Importador: anderson@inf.puc-rio.br
  - Valor do item: R$ 15.000,00
  - Taxa de frete: 3,0%

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **Quando realizamos a análise crítica da informação num determinado contexto...**



matéria-prima

organização ou estruturação dos dados

produto intermediário

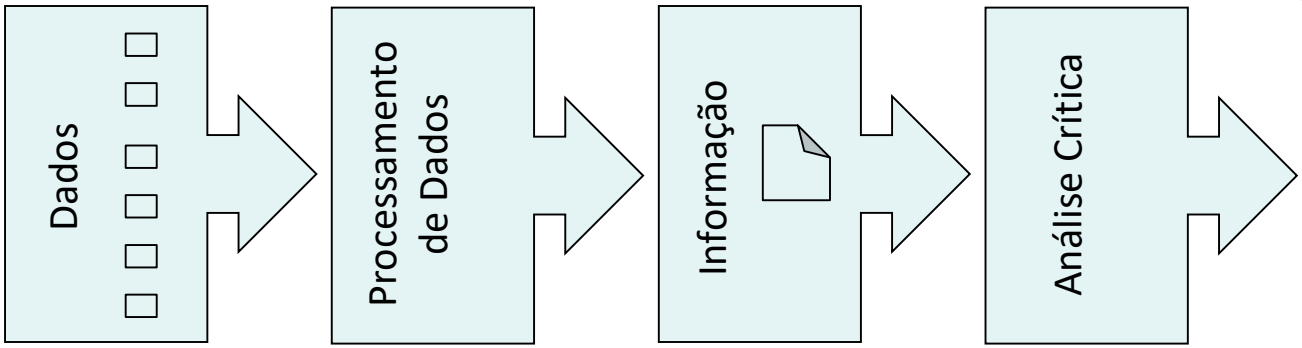
tratamento da informação em determinado contexto

- **Existem funcionários bem avaliados com salário inferior à média do mercado?**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **Quando realizamos a análise crítica da informação num determinado contexto...**



matéria-prima

organização ou estruturação dos dados

produto intermediário

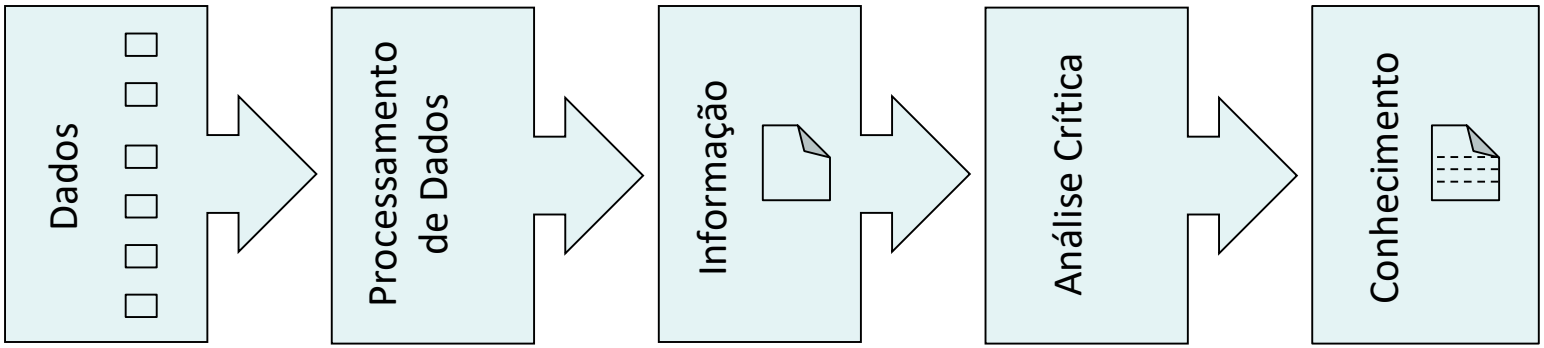
tratamento da informação em determinado contexto

- **Quais são as opções de importação que podem reduzir a taxa de frete para o cliente?**

Dados x Informação x Conhecimento

Precisamos entender a diferença e a relação entre dados, informação e conhecimento...

- **...produzimos conhecimento.**



matéria-prima

organização ou estruturação dos dados

produto intermediário

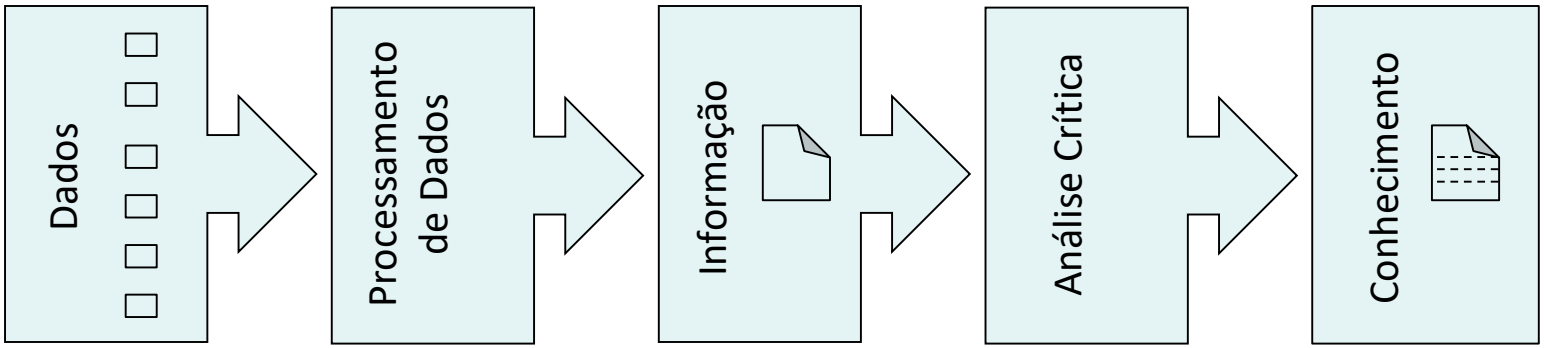
tratamento da informação em determinado contexto

produto final

Valor dos ativos de informação

Por que os ativos de informação são valiosos para uma empresa?

- **Informação e conhecimento são fundamentais para a tomada de decisão e resolução de problemas.**



matéria-prima

organização ou estruturação dos dados

produto intermediário

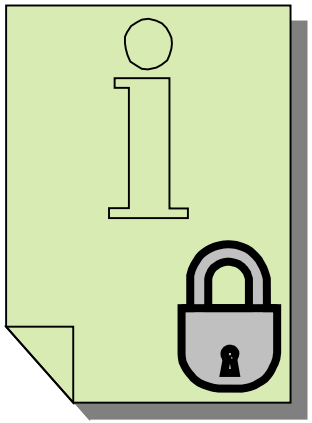
tratamento da informação em determinado contexto

produto final

Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

(Thomas R. Peltier, 2001)

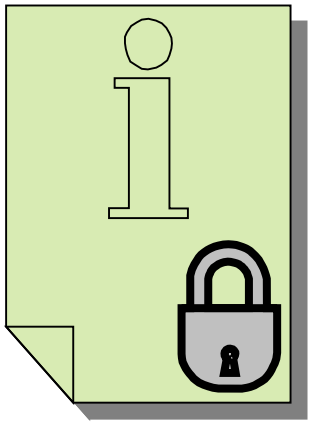


- **Por que os recursos de informação são valiosos para uma empresa?**
  - **Informação e conhecimento são fundamentais para a tomada de decisão e resolução de problemas.**

Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

(Thomas R. Peltier, 2001)

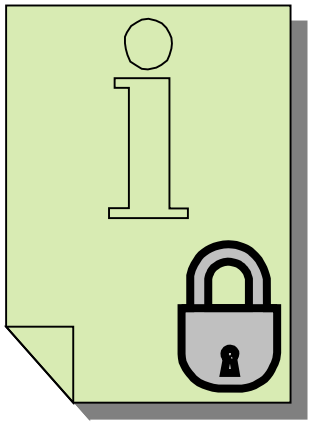


- **Como identificar os valiosos recursos de informação de uma empresa?**

Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

(Thomas R. Peltier, 2001)

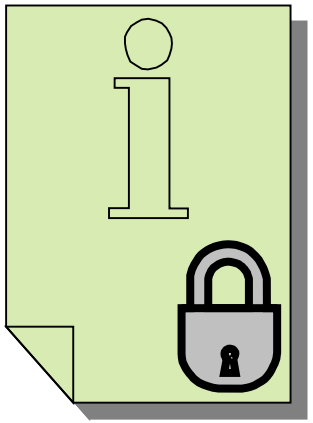


- **Como identificar os valiosos recursos de informação de uma empresa?**
- **Como assegurar a seleção e aplicação de salvaguardas apropriadas?**

Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

(Thomas R. Peltier, 2001)



- Como identificar os valiosos recursos de informação de uma empresa?
- Como assegurar a seleção e aplicação de salvaguardas apropriadas?
- Como assegurar que as decisões tomadas ajudarão a atingir o objetivo do negócio ou a sua missão?

Proteção da Informação

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou a sua missão.

- Como identificar os **informação** de uma
- Como assegurar a **seleção e aplicação de salvaguardas** apropriadas?
- Como assegurar que as decisões tomadas ajudarão a atingir o objetivo do negócio ou a sua missão?

Compliance

Compliance é o ato de estar em conformidade com leis, regulamentos, normas e padrões éticos, tanto internos quanto externos, de uma organização.

Compliance

Compliance é o ato de estar em conformidade com leis, regulamentos, normas e padrões éticos, tanto internos quanto externos, de uma organização.

- Segurança da Informação, Segurança Cibernética e Proteção à Privacidade
  - LGDP e Marco Civil da Internet
  - Família ISO 27000
  - ISO 29100 e ISO 29134
  - ISO 22301 e ISO 22313
  - Série NIST SP-800

Compliance

Compliance é o ato de estar em conformidade com leis, regulamentos, normas e padrões éticos, tanto internos quanto externos, de uma organização.

- **Segurança da Informação, Segurança Cibernética e Proteção à Privacidade**
  - **ABNT NBR ISO/IEC 29100**
  - **ABNT NBR ISO/IEC 27001**
  - **ABNT NBR ISO/IEC 27701**

Pontos-chaves

Ativos de informação estão sujeitos a ameaças de perda, roubo ou danos.

- **Os ativos de informação precisam ser protegidos para assegurar a confidencialidade, integridade e disponibilidade, evitando danos e prejuízos à organização.**

- **Quando entendemos o valor da informação para uma organização, compreendemos a necessidade da segurança da informação e da cibersegurança.**

Pontos-chaves

Ativos de informação estão sujeitos a ameaças de perda, roubo ou danos.

- **A segurança da informação visa garantir a proteção dos ativos através da seleção e aplicação de salvaguardas apropriadas e alinhadas com o objetivo do negócio e a missão da organização.**

- **A cibersegurança visa garantir a proteção dos ativos contra as ameaças cibernéticas mantendo um nível aceitável de estabilidade, continuidade e segurança.**

Pontos-chaves

Informações de identificação pessoal (dados pessoais) devem ser protegidos para assegurar a proteção da privacidade das pessoas.

- **A proteção da privacidade visa garantir a conformidade da organização com os direitos fundamentais de privacidade dos titulares de dados pessoais (DP), conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD).**

- **A violação da privacidade é a situação onde os dados pessoais são tratados em violação de um ou mais requisitos pertinentes de salvaguarda da privacidade.**

ABNT NBR ISO/IEC 29100:2024 – Estrutura de Privacidade

O objetivo é aprimorar as normas de segurança no que tange tratamento de dados pessoais (DP).

- Estabelece um framework internacional para proteção de privacidade e governança de dados pessoais.

- Fornece os princípios e os métodos para a proteção da privacidade em sistemas de Tecnologia da Informação (TI) e não se aprofunda nos detalhes operacionais.

- Fornece um arcabouço de princípios para a gestão da privacidade, enquanto a LGPD estabelece os direitos dos titulares e as obrigações dos controladores e operadores no tratamento dessas informações.

ABNT NBR ISO/IEC 29100:2024 – Estrutura de Privacidade

A norma é organizada em quatro partes principais:

- **Terminologia comum de privacidade;**
- **Atores e papéis no tratamento de dados pessoais;**
- **Salvaguarda de privacidade; e**
- **Princípios de privacidade.**

ABNT NBR ISO/IEC 29100:2024 – Terminologia

A norma é organizada em quatro partes principais:

- **Anonimização**
  - **Processo pelo qual os dados pessoais são irreversivelmente alterados, de tal modo que um titular de DP não mais possa ser identificado, direta ou indiretamente, seja por um controlador de DP individualmente ou em colaboração com qualquer outra parte.**

LGPD, Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

- **Pseudonimização**
  - **Processo aplicado aos dados pessoais que substitui informação identificável por um pseudônimo.**

ABNT NBR ISO/IEC 29100:2024 – Terminologia

A norma é organizada em quatro partes principais:

- **Anonimização (Exemplos)**

Paciente	CEP	Idade	Médico	Medicamento
Paulo	22775	66	Pedro	Tramol
Sônia	22775	24	Sara	Novalgina
Ana Lucia	22451	43	Robson	Novalgina
Simone	22451	32	Pedro	Flanax
Silvio	22654	26	Gustavo	Tramol
Luiz	22775	38	Sara	Flanax
José	22451	41	Sayão	Novalgina

supressão de atributos

CEP	Idade	Médico	Medicamento
22775	66	Pedro	Tramol
22775	24	Sara	Novalgina
23451	43	Robson	Novalgina
23451	32	Pedro	Flanax
22654	26	Gustavo	Tramol
22775	38	Sara	Flanax
23451	41	Sayão	Novalgina

CEP	Idade	Médico	Medicamento
22775	66	Pedro	Tramol
22775	24	Sara	Novalgina
23451	43	Robson	Novalgina
23451	32	Pedro	Flanax
22654	26	Gustavo	Tramol
22775	38	Sara	Flanax
23451	41	Sayão	Novalgina

encobrimento de caracteres

CEP	Idade	Médico	Medicamento
22XXX	66	Pedro	Tramol
22XXX	24	Sara	Novalgina
23XXX	43	Robson	Novalgina
23XXX	32	Pedro	Flanax
22XXX	26	Gustavo	Tramol
22XXX	38	Sara	Flanax
23XXX	41	Sayão	Novalgina

ABNT NBR ISO/IEC 29100:2024 – Terminologia

A norma é organizada em quatro partes principais:

- **Pseudonimização (Exemplo)**

Paciente	CEP	Idade	Médico	Medicamento
Paulo	22775	66	Pedro	Tramol
Sônia	22775	24	Sara	Novalgina
Ana Lucia	22451	43	Robson	Novalgina
Simone	22451	32	Pedro	Flanax
Silvio	22654	26	Gustavo	Tramol
Luiz	22775	38	Sara	Flanax
José	22451	41	Sayão	Novalgina

substituição por pseudônimos

Paciente	CEP	Idade	Médico	Medicamento
A0X1Z3D4	22775	66	Pedro	Tramol
A1P0Q0D1	22775	24	Sara	Novalgina
Y0B4C8T0	22451	43	Robson	Novalgina
U0B1G0D2	22451	32	Pedro	Flanax
P3Q0R1S5	22654	26	Gustavo	Tramol
H2K5E3F8	22775	38	Sara	Flanax
L0G3Q1M4	22451	41	Sayão	Novalgina

Pseudônimo	Paciente
A0X1Z3D4	Paulo
A1P0Q0D1	Sônia
Y0B4C8T0	Ana Lucia
U0B1G0D2	Simone
P3Q0R1S5	Silvio
H2K5E3F8	Luiz
L0G3Q1M4	José

A tabela de associação entre os pseudônimos irreversíveis e os dados originais é mantida de forma segura no controlador e não é compartilhada.

ABNT NBR ISO/IEC 29100:2024 – Atores e Papéis

A norma define 4 atores, seus respectivos papéis e os fluxos de dados pessoais entre eles.

- **Titular de DP**
  - **Fornecem seus dados para os controladores e operadores de DP e, quando não previsto pela legislação aplicável, dão consentimento e determinam suas preferências de privacidade sobre como seus dados devem ser tratados.**
  - **Exemplos:**
    - **funcionários em sistemas de recursos humanos;**
    - **consumidores em relatórios de crédito;**
    - **pacientes em prontuários de saúde.**

ABNT NBR ISO/IEC 29100:2024 – Atores e Papéis

A norma define 4 atores, seus respectivos papéis e os fluxos de dados pessoais entre eles.

- **Controlador de DP**
  - Determina os **propósitos** e os **meios** para o **tratamento de DP**, ou seja, decide por que e como os dados serão tratados.
  - Deve **garantir** que o **tratamento de DP** esteja em **conformidade** com os **princípios de privacidade** estabelecidos na norma.
  - Deve **implementar** os **controles de privacidade** para assegurar que as **operações de tratamento** sejam realizadas de maneira que **respeitem os direitos** dos titulares de DP.
  - Pode delegar a execução de **algumas operações** de tratamento a **operadores de DP**, mas a **responsabilidade pelo tratamento** permanece sendo sua.

ABNT NBR ISO/IEC 29100:2024 – Atores e Papéis

A norma define 4 atores, seus respectivos papéis e os fluxos de dados pessoais entre eles.

- **Operador de DP**
  - Realiza o tratamento de DP em nome do controlador de DP de acordo com as instruções do controlador.
  - Deve observar os requisitos de privacidade estabelecidos e implementar os controles de privacidade correspondentes.
  - Pode ser vinculado por um contrato que define suas obrigações e responsabilidades em relação ao tratamento dos dados.
  - Tipicamente, um operador de DP executa o processamento de dados, armazenamento e análise, sempre seguindo as diretrizes e instruções do controlador.

ABNT NBR ISO/IEC 29100:2024 – Atores e Papéis

A norma define 4 atores, seus respectivos papéis e os fluxos de dados pessoais entre eles.

- **Terceira Parte**
  - **Parte interessada na privacidade que não é o titular de dados pessoais (DP), o controlador de DP ou o operador de DP.**
  - **Quando recebe dados pessoais, não trata esses dados em nome do controlador de DP.**
  - **Em geral, se torna um controlador de DP por direito próprio assim que recebe os dados em questão.**
  - **Exemplo de cenário:**
    - **Quando um controlador de DP fornece dados a uma terceira parte para fins comerciais ou por ordem de uma autoridade.**

ABNT NBR ISO/IEC 29100:2024 – Atores e Papéis vs Fluxo de DP

A norma define 4 atores, seus respectivos papéis e os fluxos de dados pessoais entre eles.

Cenários	Titular de DP	Controlador de DP	Operador de DP	Terceira Parte
1	Fornecedor de DP	Recebedor de DP		
2		Fornecedor de DP	Recebedor de DP	
3	Fornecedor de DP		Recebedor de DP	
4	Recebedor de DP	Fornecedor de DP		
5	Recebedor de DP		Fornecedor de DP	
6		Recebedor de DP	Fornecedor de DP	
7		Fornecedor de DP		Recebedor de DP
8			Fornecedor de DP	Recebedor de DP

ABNT NBR ISO/IEC 29100:2024 – Identificadores de DP

Os identificadores de são elementos que podem ser usados para identificar uma pessoa natural.

- **Identificadores Comuns**
  - **As informações podem ser consideradas DP quando contêm ou estão associadas a um identificador que se refere a uma pessoa, como:**
    - **Número do Cadastro de Pessoa Física (CPF);**
    - **Número de passaporte;**
    - **Conta bancária;**
    - **Localização geográfica precisa;**
    - **Número de telefone.**

ABNT NBR ISO/IEC 29100:2024 – Identificadores de DP

Os identificadores de são elementos que podem ser usados para identificar uma pessoa natural.

- **Características Distintivas**
  - **As informações também podem ser consideradas DP se contiverem características que distinguem uma pessoa natural de outras, como dados biométricos.**
  - **A identificabilidade pode ser clara ou pode depender de uma combinação de atributos que, juntos, permitem identificar uma pessoa.**
    - **Ex: a combinação de "masculino", "52 anos" e "médico" pode ser suficiente para identificar uma pessoa em uma empresa específica, mas não fora dela.**

ABNT NBR ISO/IEC 29100:2024 – Identificadores de DP

Os identificadores de são elementos que podem ser usados para identificar uma pessoa natural.

- **Características Distintivas**
  - **Exemplos de atributos que podem ser usados para identificar pessoas:**
    - **Idade ou necessidades especiais de vulneráveis**
    - **Alegações de conduta criminosa**
    - **Informação coletada por serviços de saúde**
    - **Conta bancária ou número de cartão de crédito**
    - **Identificador biométrico**
    - **Extratos de cartão de crédito**
    - **Condenações criminais ou delitos cometidos**
    - **Número do cliente**
    - **Data de nascimento**

ABNT NBR ISO/IEC 29100:2024 – Identificadores de DP

Os identificadores de são elementos que podem ser usados para identificar uma pessoa natural.

- **Características Distintivas**
  - **Exemplos de atributos que podem ser usados para identificar pessoas:**
    - **Perfil financeiro**
    - **Gênero**
    - **Posição ou Trajetória no GPS**
    - **Endereço residencial**
    - **Endereço IP**
    - **Localização fornecida por sistemas de telecomunicação**
    - **Nome**
    - **Identificadores nacionais (ex: número do passaporte)**
    - **Endereço de e-mail pessoal**

ABNT NBR ISO/IEC 29100:2024 – Identificadores de DP

Os identificadores de são elementos que podem ser usados para identificar uma pessoa natural.

- **Metadados**
  - **Fornecem informações descritivas, estruturais e administrativas que ajudam a descrever, localizar, gerenciar e entender um ativo digital, como um documento, imagem ou vídeo.**
  - **Os sistemas de TIC podem eventualmente armazenar DP nos metadados de um ativo digital quando o titular de DP manipula o ativo.**
    - **Ex: O nome do titular de DP pode ser armazenado nos metadados de um documento quando esse titular cria um novo documento ou faz comentários ou altera documentos.**

ABNT NBR ISO/IEC 29100:2024 – Identificadores de DP

Os identificadores de são elementos que podem ser usados para identificar uma pessoa natural.

- **Dados Pessoais Sensíveis**
  - Categoria de **dados** cuja **natureza** é **considerada sensível,** pois se relacionam à **esfera mais íntima do titular** de dados pessoais (DP) ou podem ter um **impacto significativo** sobre ele.
  - Exemplos: **(Art. 5º , inciso II, da LGPD)**
    - Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

ABNT NBR ISO/IEC 29100:2024 – Salvaguarda de privacidade

Os requisitos de salvaguarda de privacidade são fundamentais para proteção de dados pessoais.

- **1 – Coleta e Retenção de DP:**
  - **As organizações devem estabelecer diretrizes claras sobre como os DP são coletados e por quanto tempo são retidos, garantindo que a coleta seja limitada ao necessário para os fins específicos.**

- **2 – Transferência de DP:**
  - **As regras para a transferência de DP para terceiras partes devem ser bem definidas, incluindo a necessidade de acordos contratuais que garantam a proteção adequada dos dados durante e após a transferência.**

ABNT NBR ISO/IEC 29100:2024 – Salvaguarda de privacidade

Os requisitos de salvaguarda de privacidade são fundamentais para proteção de dados pessoais.

- **3 – Avaliação de Riscos:**
  - As organizações devem **realizar avaliações de riscos** para **identificar** e **mitigar** potenciais **ameaças à privacidade** dos titulares de DP, incluindo a análise de como os dados são tratados e as vulnerabilidades associadas.

- **4 – Implementação de Controles de Privacidade:**
  - Implementar **controles específicos para proteger os DP**, que podem incluir **medidas organizacionais**, **técnicas** e **físicas**.
  - Esses controles devem ser **documentados** e **revisados** periodicamente.

ABNT NBR ISO/IEC 29100:2024 – Salvaguarda de privacidade

Os requisitos de salvaguarda de privacidade são fundamentais para proteção de dados pessoais.

- **5 – Conformidade Legal:**
  - As organizações devem estar **cientes das legislações aplicáveis** e garantir que suas práticas de tratamento de DP estejam em **conformidade com as leis** de proteção de dados e privacidade.

- **6 – Políticas de Privacidade:**
  - A alta direção deve **estabelecer** e **comunicar** uma **política de privacidade** que **reflita o compromisso** da organização com a **proteção dos DP** e que seja **acessível** a todas as partes interessadas.

ABNT NBR ISO/IEC 29100:2024 – Salvaguarda de privacidade

Os requisitos de salvaguarda de privacidade são fundamentais para proteção de dados pessoais.

- **7 – Monitoramento e Revisão:**
  - **As organizações devem monitorar continuamente os riscos e a eficácia dos controles implementados, realizando análises críticas e ajustes conforme necessário.**

ABNT NBR ISO/IEC 29100:2024 – Política de privacidade

A política estabelece diretrizes e compromissos da organização em relação ao tratamento de DP.

- **1 – Ser Apropriada ao Propósito da Organização:**
  - **A política deve refletir as atividades e os objetivos da organização em relação ao tratamento de DP.**

- **2 – Fornecer Estrutura para Determinação de Objetivos:**
  - **Deve servir como base para definir metas e objetivos relacionados à proteção da privacidade.**

- **3 – Compromisso com Requisitos de Salvaguarda da Privacidade:**
  - **A política deve incluir um compromisso explícito de atender aos requisitos legais e regulamentos aplicáveis à privacidade.**

ABNT NBR ISO/IEC 29100:2024 – Política de privacidade

A política estabelece diretrizes e compromissos da organização em relação ao tratamento de DP.

- **4 – Compromisso com a Melhoria Contínua:**
  - A política deve promover a melhoria contínua das práticas de privacidade dentro da organização.
- **5 – Comunicação Interna:**
  - A política deve ser comunicada a todos os níveis da organização, garantindo que todos os colaboradores estejam cientes das diretrizes e obrigações.
- **6 – Disponibilidade para Partes Interessadas:**
  - A política deve estar acessível para as partes interessadas, conforme apropriado, permitindo que os titulares de DP entendam como seus dados são tratados.

ABNT NBR ISO/IEC 29100:2024 – Princípios de privacidade

Os princípios de privacidade são fundamentais para orientar o tratamento de dados pessoais (DP).

- **1 – Consentimento e escolha:** **(LGPD, Art. 7º, hipóteses para o tratamento de DP)**
  - Os titulares de DP devem ter a opção de consentir ou não com o tratamento de seus dados, exceto em situações específicas previstas pela legislação.
- **2 – Legitimidade e especificação de propósito:** **(LGPD, Art. 6º , I – finalidade)**
  - O tratamento de DP deve ser realizado de forma legítima e para propósitos específicos, que devem ser claramente informados aos titulares.
- **3 – Limitação de coleta:** **(LGPD, Art. 6º , III – necessidade)**
  - A coleta de DP deve ser limitada ao que é necessário para os propósitos definidos, evitando a coleta excessiva.

ABNT NBR ISO/IEC 29100:2024 – Princípios de privacidade

Os princípios de privacidade são fundamentais para orientar o tratamento de dados pessoais (DP).

- **4 – Minimização de dados:** **(LGPD, Art. 6º , III – necessidade)**
  - Apenas os dados necessários para o propósito do tratamento devem ser coletados e mantidos.
- **5 – Uso, retenção e limitação da divulgação:** **(LGPD, Art. 6º , II – adequação)**
  - Os DP devem ser utilizados apenas para os fins para os quais foram coletados e não devem ser retidos por mais tempo do que o necessário.
- **6 – Exatidão e qualidade:** **(LGPD, Art. 6º , V – qualidade dos dados)**
  - Os DP devem ser precisos e atualizados, garantindo que a qualidade dos dados seja mantida.

ABNT NBR ISO/IEC 29100:2024 – Princípios de privacidade

Os princípios de privacidade são fundamentais para orientar o tratamento de dados pessoais (DP).

- **7 – Abertura, transparência e notificação: (LGPD, Art. 6º , VI - transparência)**
  - As organizações devem ser transparentes sobre suas práticas de tratamento de DP e notificar os titulares sobre como seus dados estão sendo utilizados.
- **8 – Participação individual e acesso: (LGPD, Art. 6º , IV – livre acesso)**
  - Os titulares de DP devem ter o direito de acessar seus dados e participar do processo de tratamento, podendo solicitar correções quando necessário.
- **9 – Responsabilização: (LGPD, Art. 6º , X - responsabilização)**
  - As organizações devem ser responsáveis pelo cumprimento dos princípios de privacidade e devem demonstrar conformidade.

ABNT NBR ISO/IEC 29100:2024 – Princípios de privacidade

Os princípios de privacidade são fundamentais para orientar o tratamento de dados pessoais (DP).

- **10 – Segurança da informação: (LGPD, Art. 6º , VII - segurança)**
  - **Medidas adequadas devem ser implementadas para proteger os DP contra acesso não autorizado, divulgação, alteração ou destruição.**

- **11 – Compliance com a privacidade: (LGPD, Art. 38º , RIPD)**
  - **As organizações devem garantir que suas práticas estejam em conformidade com as leis e regulamentos de privacidade aplicáveis.**

ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

A Gestão de Segurança da Informação (GSI) visa implantar um processo de gestão sistemática.

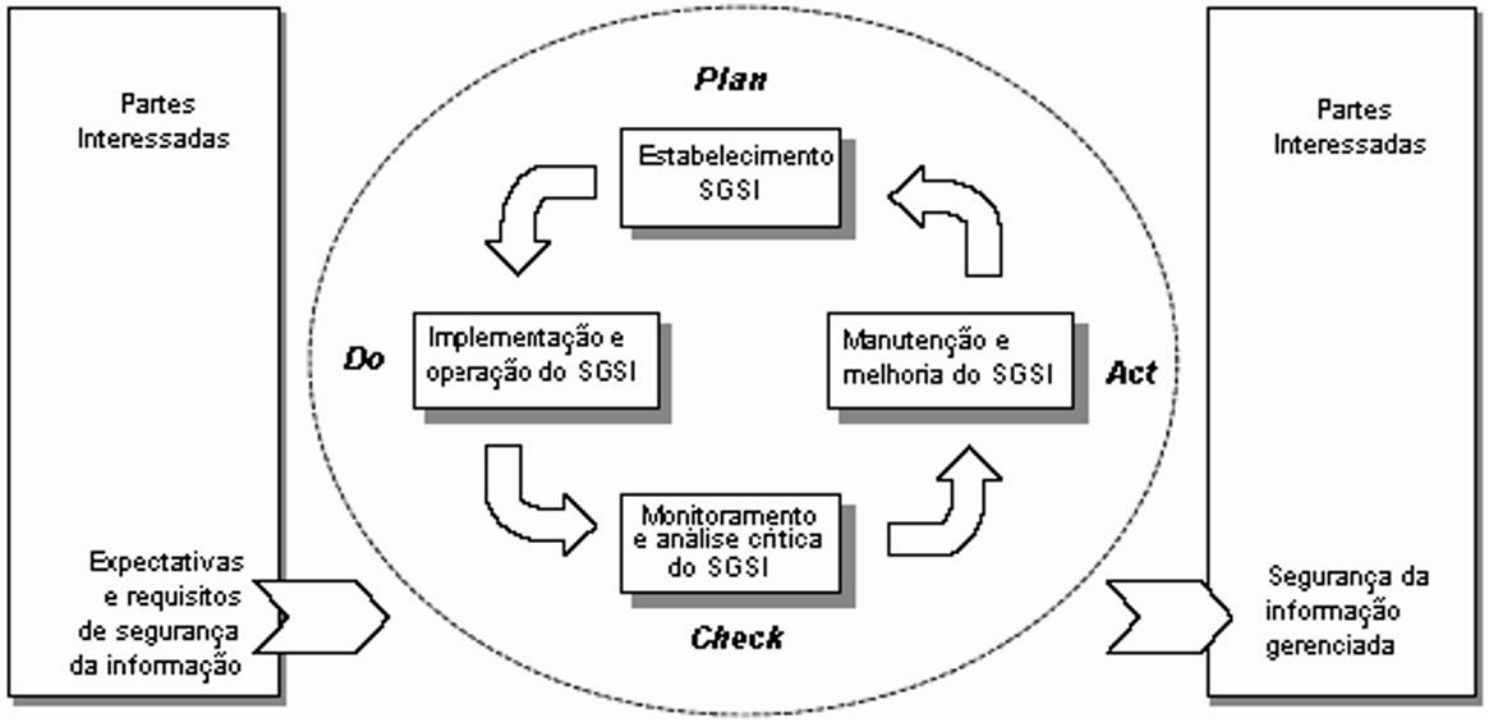
- **Principais Objetivos**

  - **1 – Assegurar a proteção dos ativos de informação da organização, garantindo a confidencialidade, a integridade e a disponibilidade desses ativos.**

  - **2 – Assegurar a conformidade da organização com leis e regulamentos, garantindo a reputação da organização e reduzindo prejuízos financeiros.**

ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

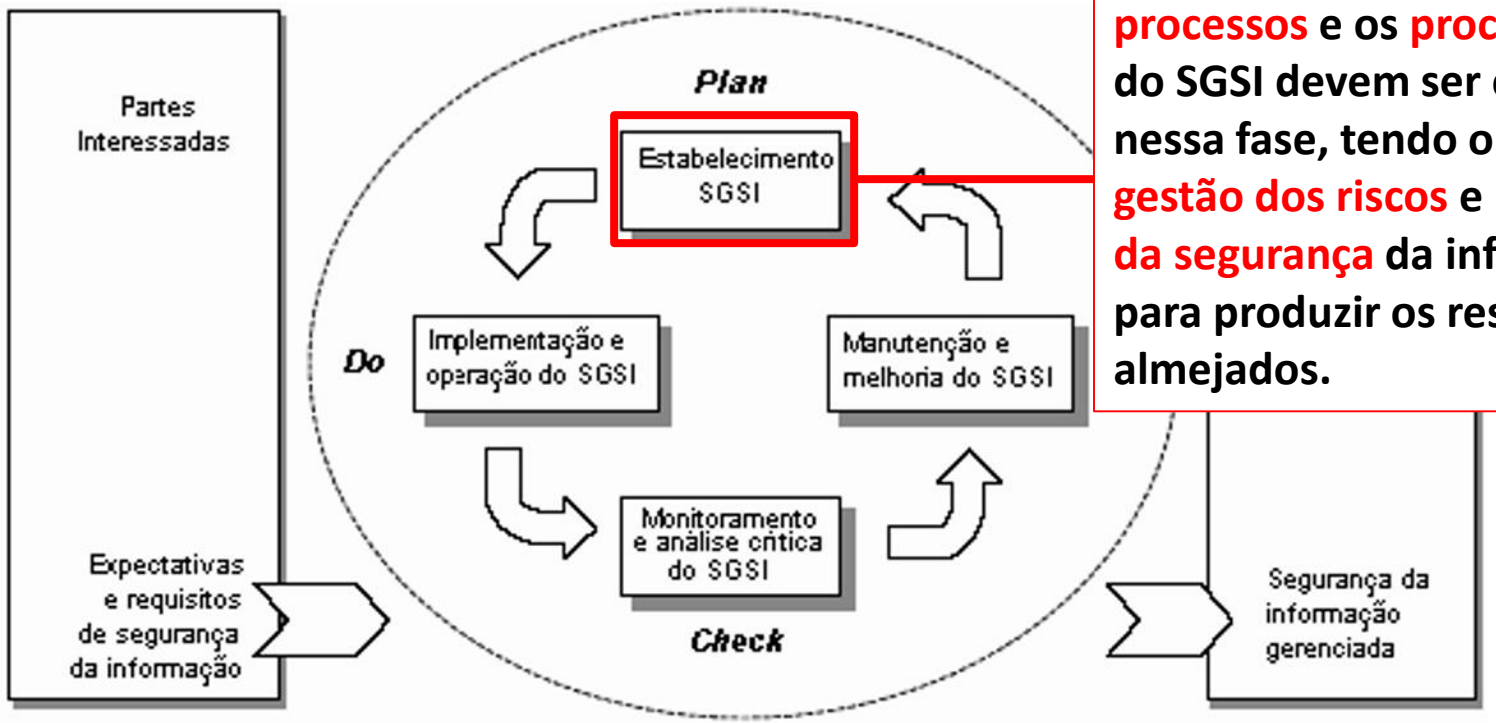
Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)



(ABNT NBR ISO/IEC 27001:2006, ABNT, p. vi)

ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)

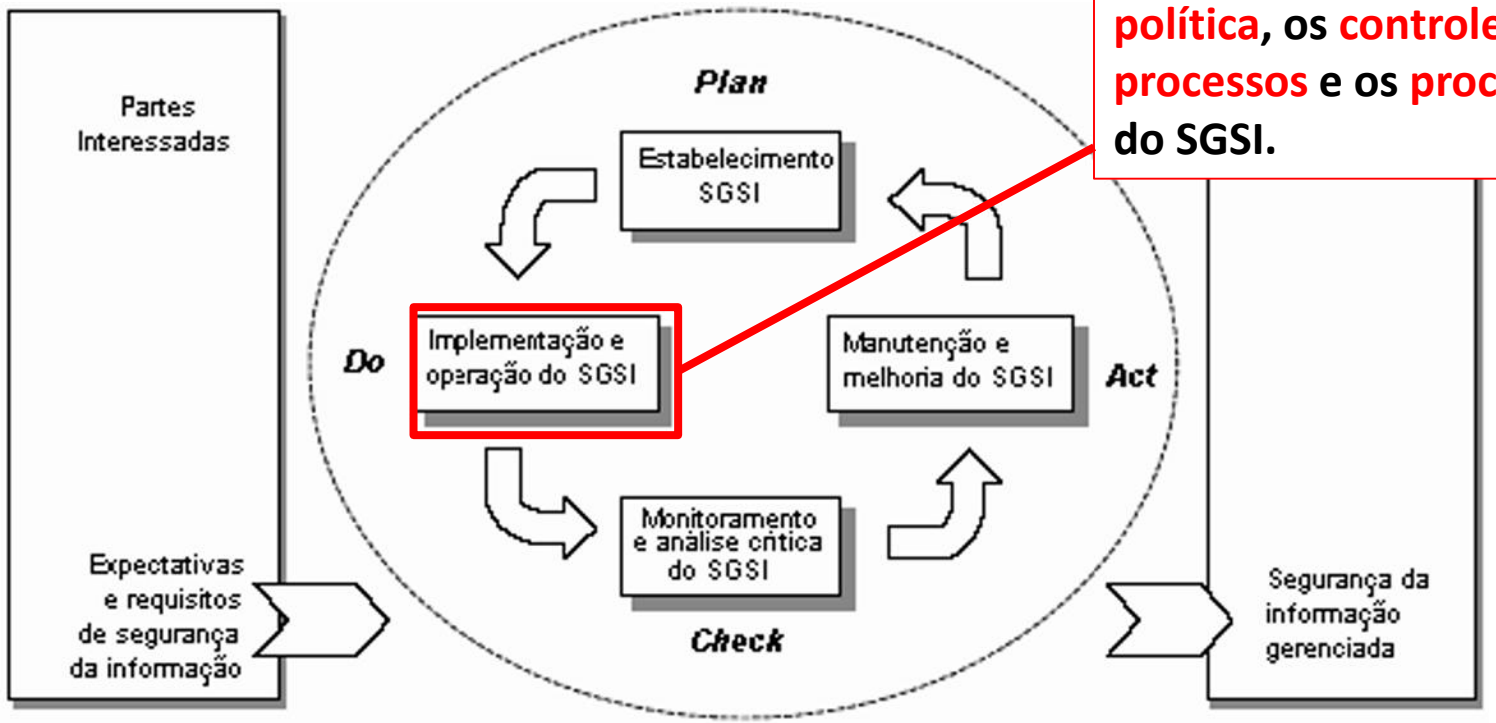


A **política**, os **objetivos**, os **processos** e os **procedimentos** do SGSI devem ser criados nessa fase, tendo o foco na **gestão dos riscos** e **melhoria da segurança** da informação para produzir os resultados almejados.

(ABNT NBR ISO/IEC 27001:2006, ABNT, p. vi)

ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)

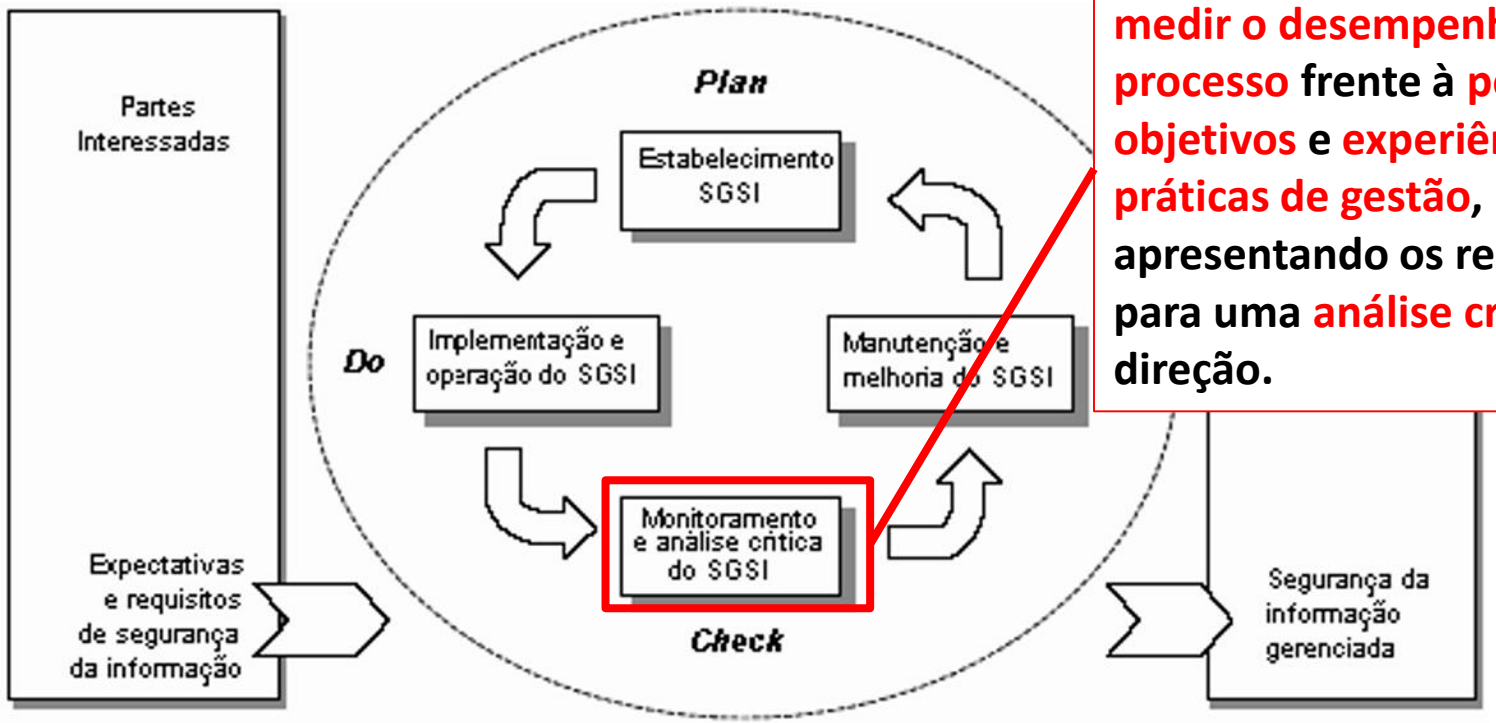


Implementar e operar a política, os controles, os processos e os procedimentos do SGSI.

(ABNT NBR ISO/IEC 27001:2006, ABNT, p. vi)

ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)

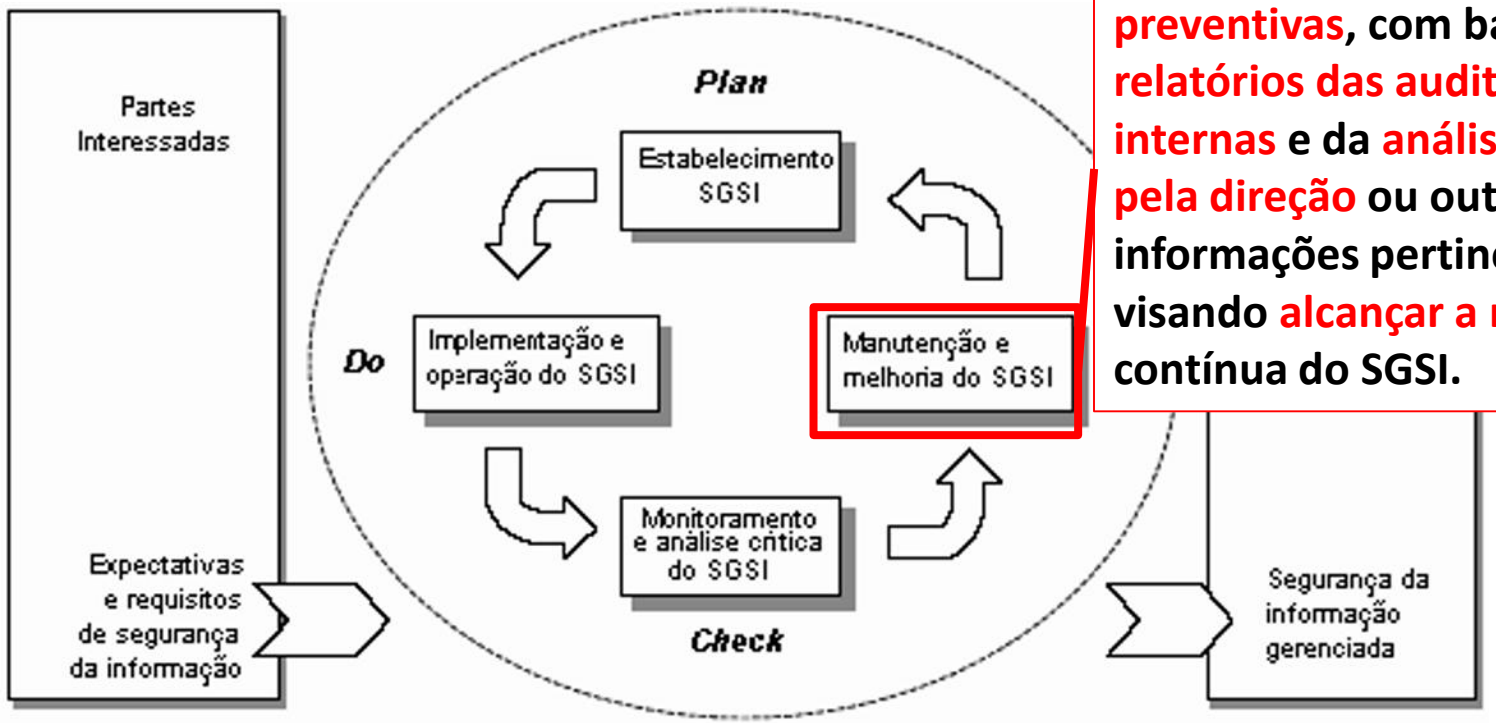


Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiências práticas de gestão, apresentando os resultados para uma análise crítica pela direção.

(ABNT NBR ISO/IEC 27001:2006, ABNT, p. vi)

ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)



Executar as **ações corretivas** e **preventivas**, com base nos **relatórios das auditorias internas** e da **análise crítica pela direção** ou outras informações pertinentes, visando **alcançar a melhoria contínua do SGSI.**

(ABNT NBR ISO/IEC 27001:2006, ABNT, p. vi)

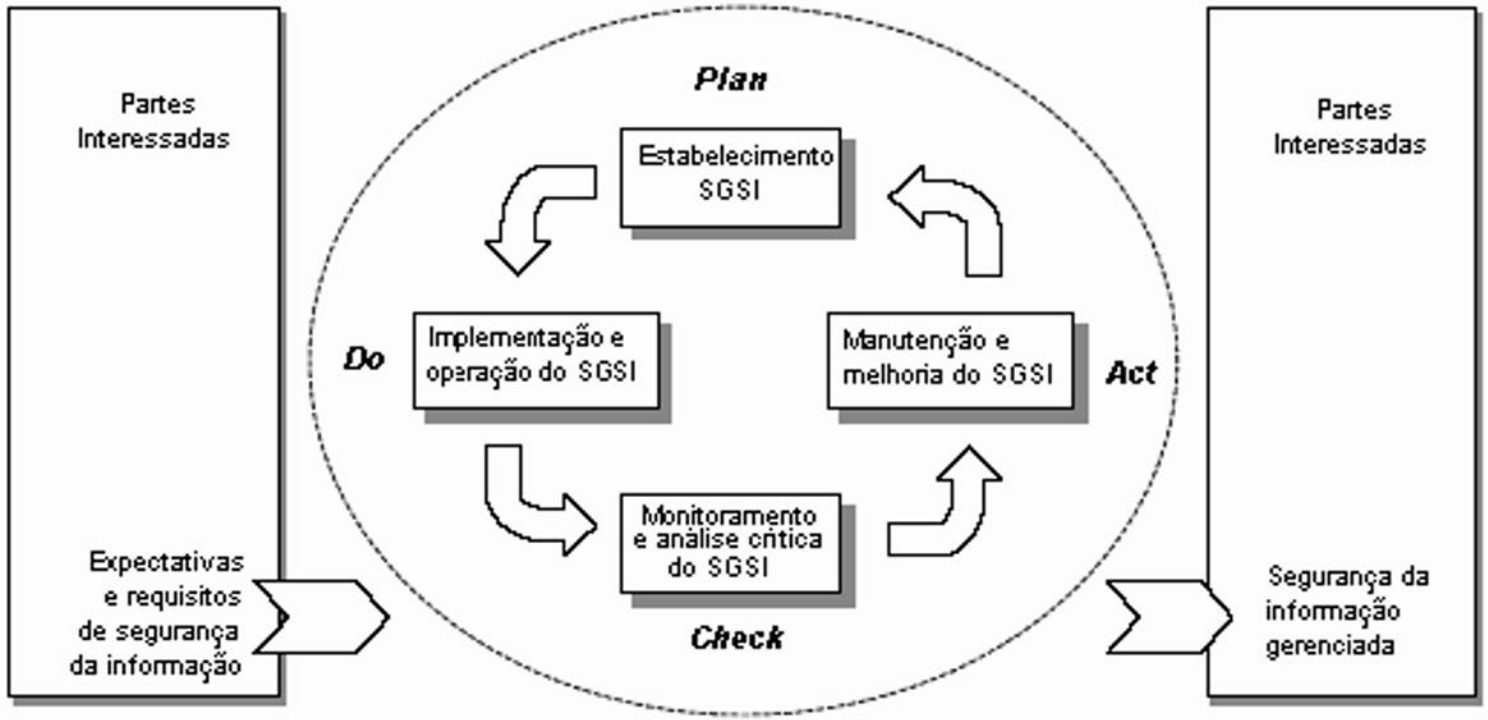
ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

A Gestão de Privacidade da Informação (GPI) visa implantar um processo de gestão sistemática.

- **Os requisitos da ABNT NBR ISO/IEC 27001 mencionando segurança da informação devem ser estendidos para a proteção da privacidade, caso esta seja potencialmente afetada pelo tratamento de DP.**
  - **1 – Assegurar a proteção dos ativos de informação da organização e a proteção dos dados pessoais, garantindo a confidencialidade, a integridade e a disponibilidade desses ativos e a proteção da privacidade.**
  - **2 – Assegurar a conformidade da organização com leis e regulamentos, garantindo a reputação da organização e reduzindo prejuízos financeiros.**

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)



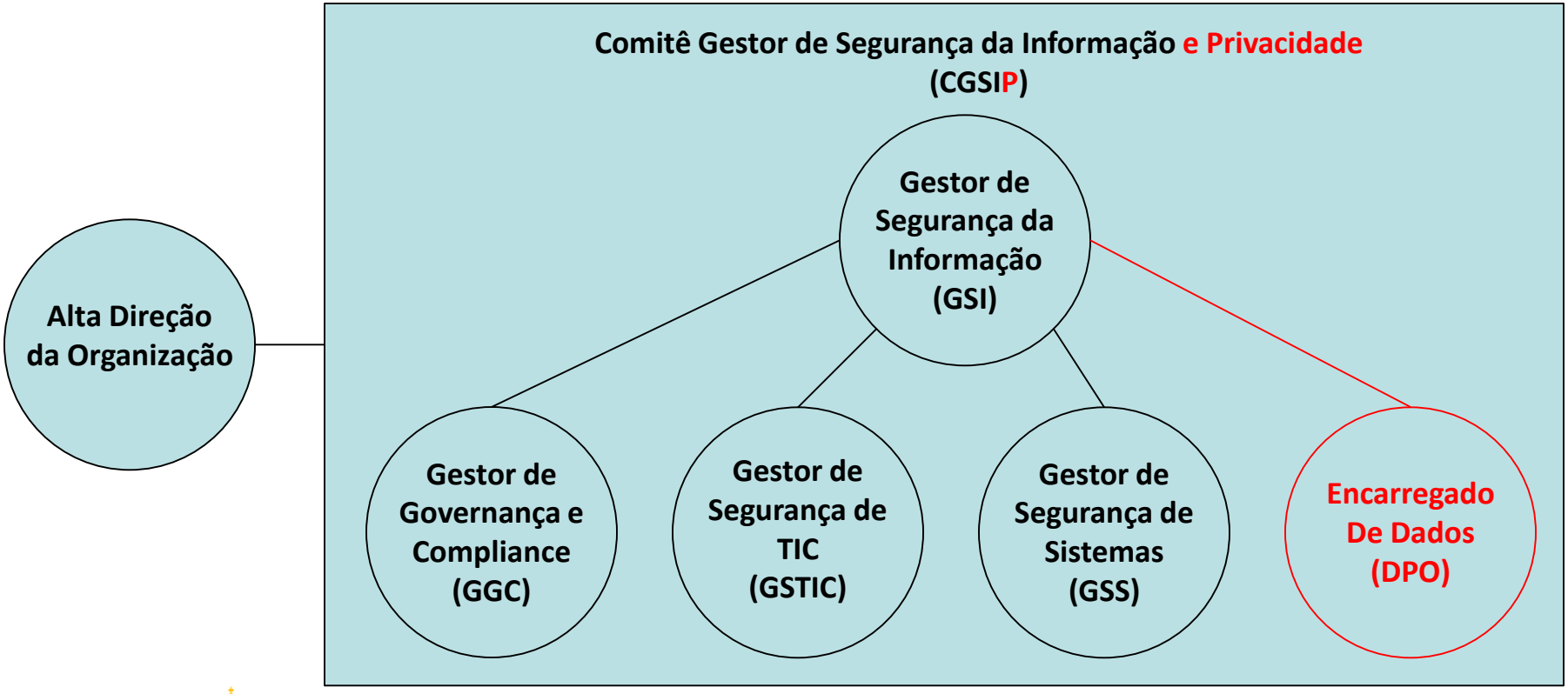
+ Privacidade da Informação

(ABNT NBR ISO/IEC 27001:2006, ABNT, p. vi)

Prof. Anderson Oliveira da Silva - anderson@inf.puc-rio.br

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Competências: Papéis e Responsabilidades



ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios de Valoração dos Ativos por Confidencialidade, Integridade, Disponibilidade e Privacidade:

Peso	Confidencialidade	Integridade	Disponibilidade	Privacidade
3 (Alto)	O ativo executa operações com informações sensíveis para o processo de negócio da organização	A integridade do ativo e/ou das informações tratados nele é crítica para o processo de negócio	A disponibilidade do ativo e/ou das informações tratadas nele é crítica para o processo de negócio	Violações da privacidade no ativo geram impactos negativos grandes para os titulares e para a organização
2 (Médio)	O ativo executa operações com informações não-sensíveis e não-públicas para o processo de negócio da organização	A falha de integridade do ativo e/ou das informações tratadas nele gera impactos negativos para o processo de negócios	A falha de disponibilidade do ativo e/ou das informações tratadas nele gera impactos negativos para o processo de negócios	Violações da privacidade no ativo geram impactos negativos medianos para os titulares e para a organização
1 (Baixo)	O ativo executa operações com informações públicas e sem prejuízo para o processo de negócio da organização	A falta de integridade do ativo e/ou das informações tratadas nele gera ineficiência, mas não tem impactos significativos sobre o processo de negócio	A falta de disponibilidade do ativo e/ou das informações tratadas nele gera ineficiência, mas não tem impactos significativos sobre o processo de negócios	Violações da privacidade no ativo geram impactos negativos pequenos para os titulares e para a organização

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios de Valoração dos Ativos por Confidencialidade, Integridade, Disponibilidade e Privacidade:

Ativo	Setor	Tipo	Confidencialidade	Integridade	Disponibilidade	Privacidade	Valor CIDP
Desktop	RH	Computador	3	3	3	3	**12**
Notebook	RH	Computador	3	3	1	3	**10**
Switch	RH	Rede	3	3	3	3	**12**
RHSystem	RH	Sistema	3	3	3	3	**12**
EduSystem	RH	Sistema	2	2	1	1	**6**

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios para o processo de avaliação de riscos: Consequência

Consequência	Valor	Descrição
Baixo	1	Se explorada, a ameaça não compromete de nenhuma maneira o funcionamento normal do sistema, nem oferece risco de vazamento de informações sensíveis e dados pessoais.
Médio	2	A ameaça não compromete informações sensíveis e dados pessoais, mas pode realizar ações não autorizadas que podem atrapalhar o sistema, aumentando levemente a chance de vazamentos ou inoperância.
Alto	3	A ameaça pode comprometer informações sensíveis e dados pessoais e realizar ações não autorizadas que podem atrapalhar o sistema, com chance de inoperância.
Muito alto	4	A ameaça compromete informações sensíveis e dados pessoais sensíveis e/ou o funcionamento total do sistema.

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios para o processo de avaliação de riscos: Probabilidade

Probabilidade	Valor	Descrição
Improvável	1	É esperado que a ameaça não se concretize na maioria dos casos (1 a 25% de chance de acontecer)
Possível	2	Existe uma possibilidade razoável de que a ameaça se concretize (26% a 50% de chance de acontecer)
Provável	3	Existe uma chance alta da ameaça se concretizar (51% a 75% de chance de acontecer)
Frequente	4	É esperado que a ameaça se concretize na maioria dos casos (76% a 100% de chance)

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios para o processo de avaliação de riscos: Matriz de Risco (Probabilidade x Consequência)

		Probabilidade			
Consequência		Improvável	Possível	Provável	Frequente
		1	2	3	4
Muito alto	4	4	8	12	16
Alto	3	3	6	9	12
Médio	2	2	4	6	8
Baixo	1	1	2	3	4

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios para o processo de avaliação de riscos: Nível de Risco

Risco	Valores	Descrição
Baixo	1, 2	Risco tolerável, sem necessidade de acompanhamento especial da ameaça.
Médio	3, 4	Risco tolerável, porém, com chances razoáveis de causar uma consequência significativa. Neste caso, a ameaça deve ser monitorada, sem urgência para a implementação de salvaguardas.
Alto	6, 8, 9	Risco não é tolerável, a consequência da ameaça e sua probabilidade não são ignoráveis. Neste caso, a ameaça deve ser monitorada e as salvaguardas devem ser implementadas rapidamente.
Muito alto	12, 16	Risco totalmente intolerável, a consequência da ameaça e sua probabilidade não são ignoráveis. Ameaças nesta faixa exigem a implementação de salvaguardas imediatamente.

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

Critérios para o processo de avaliação de riscos: Tratamento de Risco

Risco	Valores	Tratamento
Baixo	1, 2	Aceitar
Médio	3, 4	Aceitar
Alto	6, 8, 9	Mitigar (modificar, evitar, compartilhar)
Muito alto	12, 16	Mitigar (modificar, evitar, compartilhar)

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação

Domínios de Segurança dos Controles da Norma:

- Políticas de Segurança da Informação
- Organização da Segurança da Informação
- Segurança em Recursos Humanos
- Gestão de Ativos
- Controle de Acesso
- Criptografia
- Segurança Física e do Ambiente
- Segurança nas Operações
- Segurança nas Comunicações
- Aquisição, Desenvolvimento e Manutenção de Sistemas
- Relacionamento na Cadeia de Suprimento
- Gestão de Incidentes de Segurança da Informação
- Gestão da Continuidade do Negócio
- Conformidade

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação (Estendido – 27701)

Domínios de Segurança dos Controles da Norma:

- **Políticas de Segurança da Informação**
  - **+ Política de Privacidade (política interna).**
  - **+ Aviso de Privacidade (política externa).**
  - **+ Conformidade com as leis e regulamentações para o tratamento de DP.**
- **Organização da Segurança da Informação**
  - **+ Nomeação do Encarregado de Dados Pessoais (DPO).**
  - **+ Nomeação de um Comitê de Gestão de Privacidade.**
  - **+ Política para uso de dispositivo móvel com DP.**
- **Segurança em Recursos Humanos**
  - **+ Conscientização, educação e treinamento abordando as consequências da violação de privacidade ou de regras de segurança e procedimentos para a organização, seus membros e o titular de DP.**

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação (Estendido – 27701)

Domínios de Segurança dos Controles da Norma:

- **Gestão de Ativos**
  - **+ Incluir DP como uma das categorias de classificação de informação.**
  - **+ Conscientização sobre a definição de DP e como reconhecer DP.**
  - **+ Gerenciamento de mídias removíveis com DP:**
    - **Controle de transferência, armazenamento seguro e descarte.**

- **Controle de Acesso**
  - **+ Registro e cancelamento de usuários que administrem ou operem sistemas e serviços que tratam DP.**
  - **+ Registro preciso e atualizado dos perfis dos usuários criados em sistemas de informação que manipulam DP.**
  - **+ Procedimentos seguros de entrada para quaisquer contas de usuários sob o controle do cliente.**

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação (Estendido – 27701)

Domínios de Segurança dos Controles da Norma:

- **Criptografia**
  - **+ Política para o uso de controles criptográficos para proteger DP sensíveis.**
- **Segurança Física e do Ambiente**
  - **+ Reutilização ou descarte seguro de equipamentos com DP.**
  - **+ Restringir a criação de material físico que inclua DP ao mínimo necessário.**
- **Segurança nas Operações**
  - **+ Requisitos para cópia de segurança, recuperação e restauração de DP.**
  - **+ Registros de eventos (logs) que gravem o acesso ao DP (por quem, quando, qual titular de DP e quais mudanças).**
  - **+ Critério em relação a quando e como as informações de log podem se tornar disponíveis ou usáveis pelo cliente.**
  - **+ Proteção das informações dos registros de eventos (logs) com DP.**

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação (Estendido – 27701)

Domínios de Segurança dos Controles da Norma:

- **Segurança nas Comunicações**
  - **+ Assegurar que regras relativas ao tratamento de DP são mandatórias por todo o sistema e fora dele em transferências de informações.**
  - **+ Assegurar que os indivíduos que operam com acesso aos DP estejam sujeitos a um acordo obrigatório de confidencialidade.**

- **Aquisição, Desenvolvimento e Manutenção de Sistemas**
  - **+ Assegurar que os DP transmitidos por redes não confiáveis estejam criptografados para a transmissão.**
  - **+ Políticas para o projeto e desenvolvimento de sistemas incluam diretrizes para as necessidades de tratamento de DP da organização.**
  - **+ Projeto de sistemas e/ou componentes que tratam DP com os princípios de *privacy by design* e *privacy by default*, incluindo sistemas terceirizados.**
  - **+ Não usar DP para propósitos de teste. Usar DP falso ou sintético.**

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação (Estendido – 27701)

Domínios de Segurança dos Controles da Norma:

- **Relacionamento na Cadeia de Suprimento**
  - **+ Especificar as medidas mínimas técnicas e organizacionais que o fornecedor precisa atender nos acordos que tratam DP para que a organização cumpra com as suas as obrigações de proteção de DP e segurança da informação.**

- **Gestão de Incidentes de Segurança da Informação**
  - **+ Estabelecer as responsabilidades e procedimentos para a identificação e registro de violações de DP.**
  - **+ Resposta aos incidentes de segurança da informação com violação de DP devem ser tratadas e notificadas aos titulares de DP e autoridade de supervisão.**
  - **+ Incluir cláusulas que cobrem a notificação de uma violação envolvendo DP nos contratos com os operadores de DP.**

ABNT NBR ISO/IEC 27002 – Controles de Segurança da Informação (Estendido – 27701)

Domínios de Segurança dos Controles da Norma:

- **Gestão da Continuidade do Negócio**
  - **Sem especificação de novos controles.**

- **Conformidade**
  - **+ Identificar quaisquer sanções legais potenciais relativas ao tratamento de DP, incluindo multas substanciais oriundas diretamente da autoridade de supervisão local.**
  - **+ Reter cópias de seus procedimentos e políticas de privacidade associados, por um período conforme especificado na sua programação de retenção.**
  - **+ Prover evidências independentes de que a segurança da informação está implementada e é operada de acordo com os procedimentos e as políticas da organização (principalmente no caso de um operador de DP).**
  - **+ Incluir métodos de análise crítica das ferramentas e componentes relacionados ao tratamento de DP.**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Controladores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Controladores de DP:

- **Condições para coleta e tratamento**
  - **Determinar e documentar que o tratamento é lícito, com bases legais conforme as jurisdições aplicáveis, e com propósitos legítimos e claramente estabelecidos.**
    - **Identificação e documentação do propósito**
    - **Identificação de bases legais**
    - **Determinando quando e como o consentimento deve ser obtido**
    - **Obtendo e registrando o consentimento**
    - **Avaliação de impacto de privacidade**
    - **Contratos com operadores de DP**
    - **Controlador conjunto de DP**
    - **Registros relativos ao tratamento de DP**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Controladores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Controladores de DP:

- **Obrigações para os titulares de DP**
  - **Para assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP e para atender quaisquer outras obrigações aplicáveis aos titulares de DP, relativas ao tratamento dos seus DP.**

  - **Determinando e cumprindo as obrigações para os titulares de DP**
  - **Determinando as informações para os titulares de DP**
  - **Fornecendo informações aos titulares de DP**
  - **Fornecendo mecanismos para modificar ou cancelar o consentimento**
  - **Fornecendo mecanismos para negar o consentimento ao tratamento de DP**
  - **Acesso, correção e/ou exclusão**
  - **Obrigações dos controladores de DP para informar aos terceiros**
  - **Fornecendo cópia do DP tratado**
  - **Tratamento de solicitações**
  - **Tomada de decisão automatizada**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Controladores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Controladores de DP:

- **Privacy by design e Privacy by Default**
  - **Assegurar que processos e sistemas sejam projetados de tal forma que a coleta e o tratamento (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.**
    - **Limite de coleta**
    - **Limite de tratamento**
    - **Precisão e qualidade**
    - **Objetivos de minimização de DP**
    - **Anonimização e exclusão de DP ao final do tratamento**
    - **Arquivos temporários**
    - **Retenção**
    - **Descarte**
    - **Controles de transmissão de DP**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Controladores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Controladores de DP:

- **Compartilhamento, transferência e divulgação de DP**
  - **Determinar se e documentar quando o DP é compartilhado, transferido para outras jurisdições ou terceiros e/ou divulgado de acordo com as obrigações aplicáveis.**
    - **Identificando as bases para a transferência de DP entre jurisdições**
    - **Países e organizações internacionais para os quais DP podem ser transferidos**
    - **Registros de transferência de DP**
    - **Registro de divulgação de DP para terceiros**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Operadores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Operadores de DP:

- **Condições para coleta e tratamento**
  - **Documentar e determinar que o tratamento é lícito, com base legal, conforme as jurisdições aplicáveis e com propósitos legítimos e claramente definidos.**
    - **Acordos com o cliente**
    - **Propósitos da organização**
    - **Uso de marketing e propaganda**
    - **Violando instruções**
    - **Obrigações do cliente**
    - **Registros relativos ao tratamento de DP**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Operadores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Operadores de DP:

- **Obrigações para os titulares de DP**
  - **Assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP, e que estejam de acordo com quaisquer outras obrigações aplicáveis para os titulares de DP relativas ao tratamento de seus DP.**
    - **Obrigações para os titulares de DP**
      - **Ex: Incluir a correção ou exclusão dos DP em um tempo hábil.**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Operadores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Operadores de DP:

- **Privacy by design e Privacy by Default**
  - **Assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.**
    - **Arquivos temporários**
    - **Retorno, transferência ou descarte de DP**
    - **Controles de transmissão de DP**

ABNT NBR ISO/IEC 27701 – Controles Adicionais para Operadores de DP

Controles adicionados pela ABNT NBR ISO/IEC 27701 para Operadores de DP:

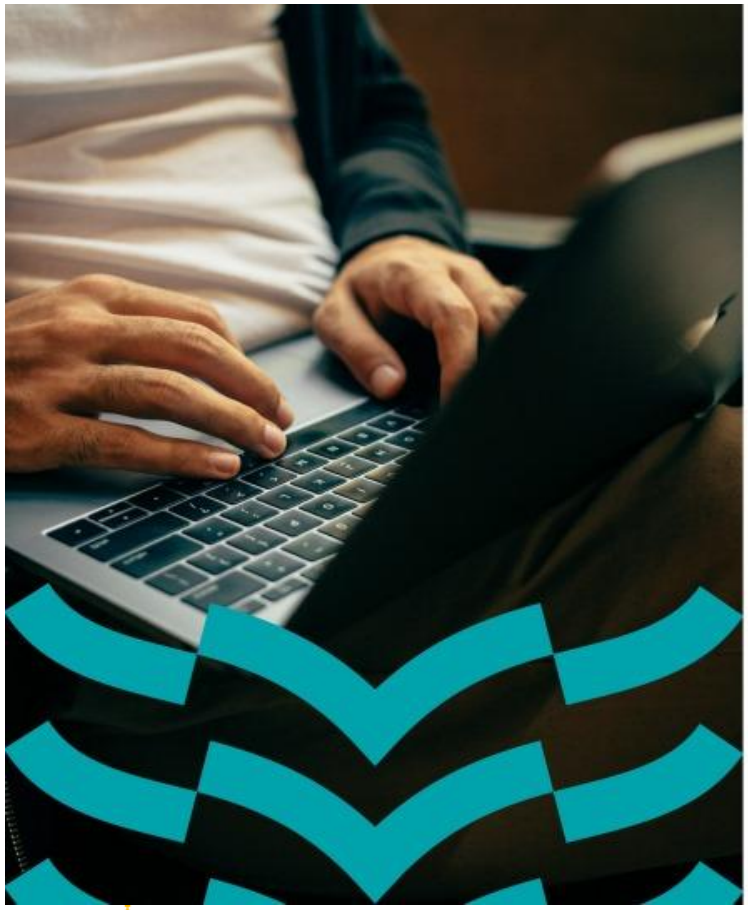
- **Compartilhamento, transferência e descarte de DP**
  - **Determinar se e documentar quando DP são compartilhados, transferidos para outras jurisdições ou terceiros e/ou divulgados, de acordo com as obrigações aplicáveis.**
    - **Bases para a transferência de DP entre jurisdições**
    - **Países e organizações internacionais para os quais o DP podem ser transferidos**
    - **Registros de DP divulgados para terceiros**
    - **Notificação de solicitações de divulgação de DP**
    - **Divulgações legalmente obrigatórias de DP**
    - **Divulgação de subcontratados usados para tratar DP**
    - **Contratação de um subcontratado para tratar DP**
    - **Mudança de subcontratado para tratar DP**

ABNT NBR ISO/IEC 27701 – Sistema de Gestão de Privacidade da Informação (SGPI)

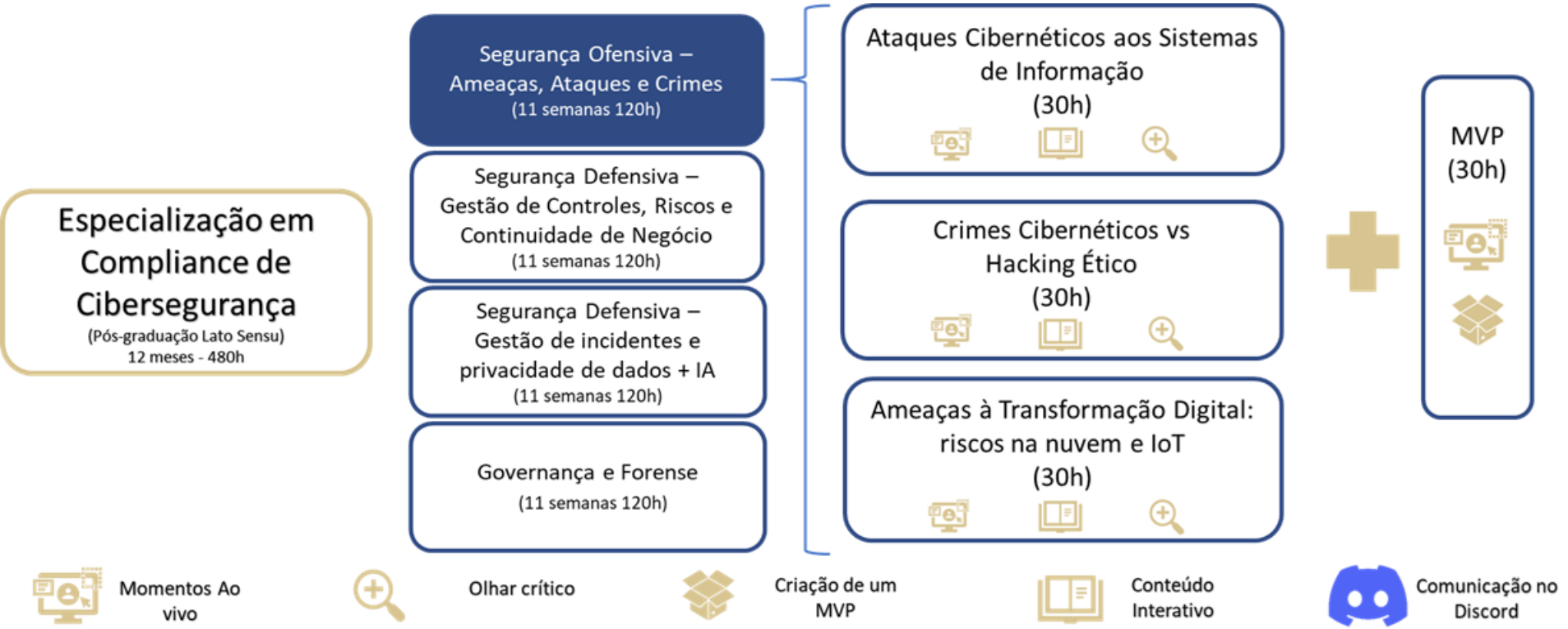
Manual de Gestão de Segurança da Informação e Privacidade (GSIP)

- Política de Segurança da Informação
- Política de Privacidade
- Abrangência, Papéis e Responsabilidades
- Processo de Avaliação de Risco
  - Critério para valoração de ativos
  - Critério de probabilidade e consequência
  - Critério de aceitação de risco
  - Identificação dos riscos
  - Análise de riscos
  - Avaliação de riscos
- Tratamento de riscos
  - Plano de Tratamento de Riscos
  - Declaração de Aplicabilidade
- Monitoramento e análise crítica

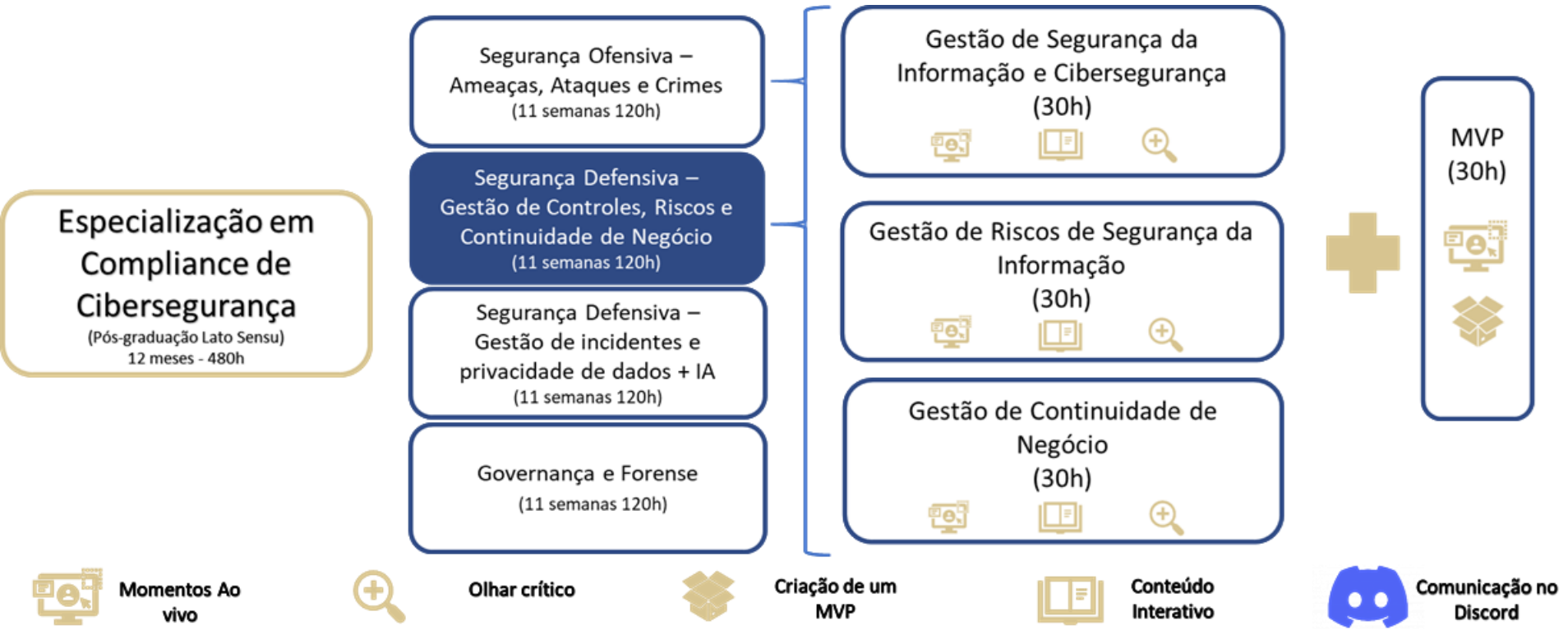
Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade



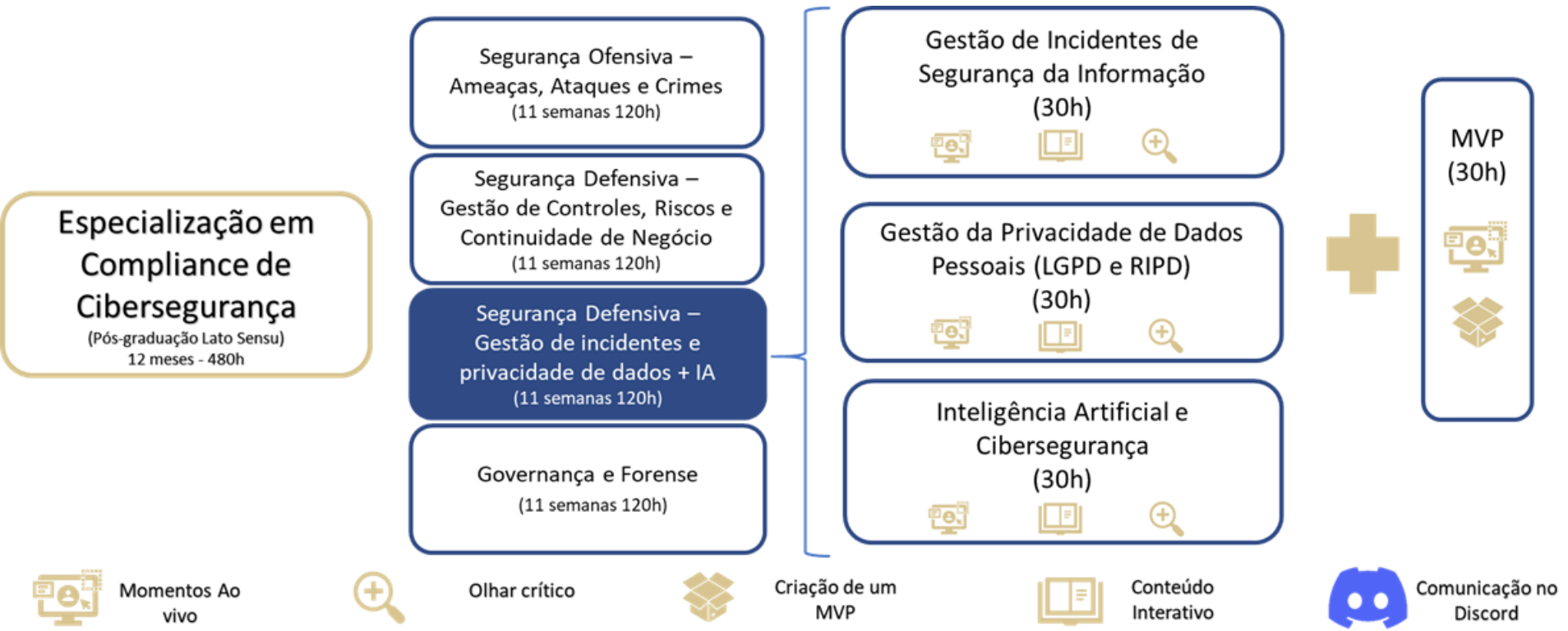
Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade



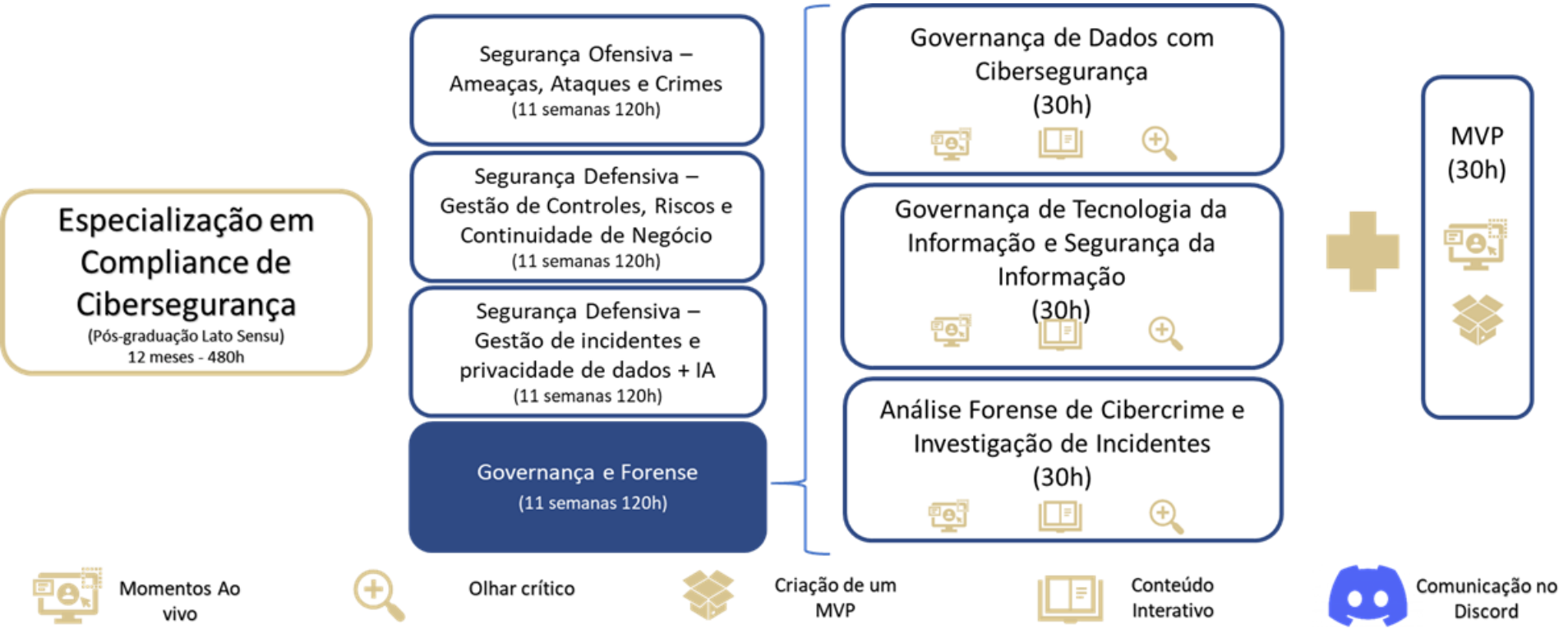
Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade



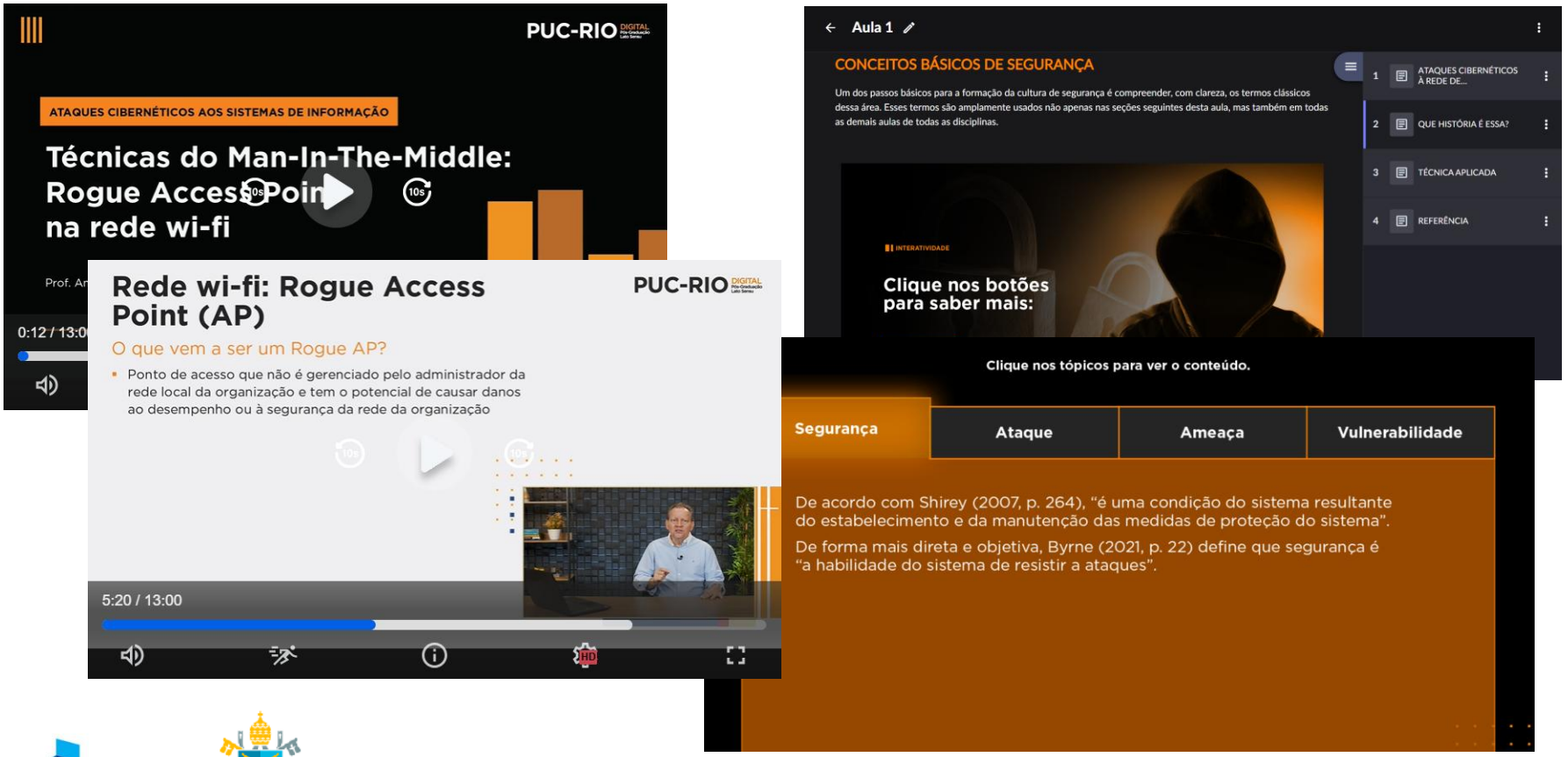
Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade



Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade

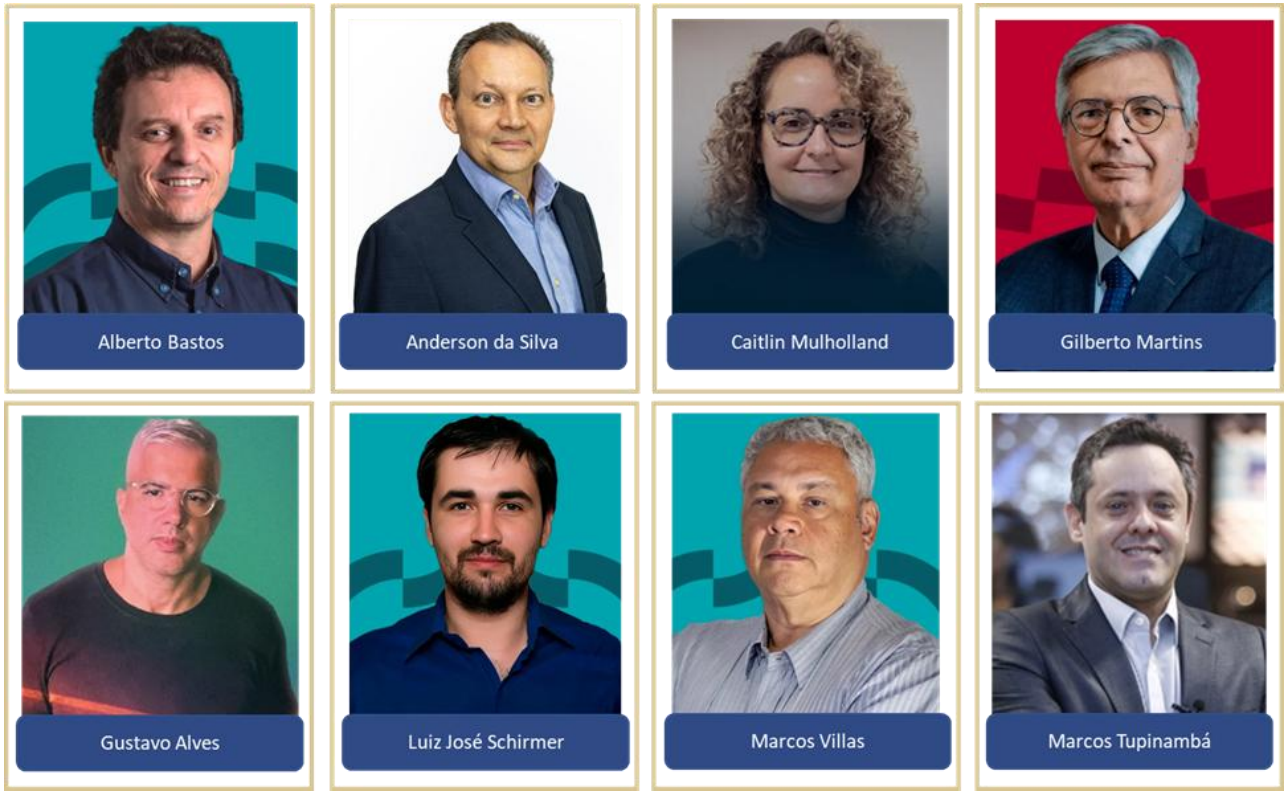


Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade

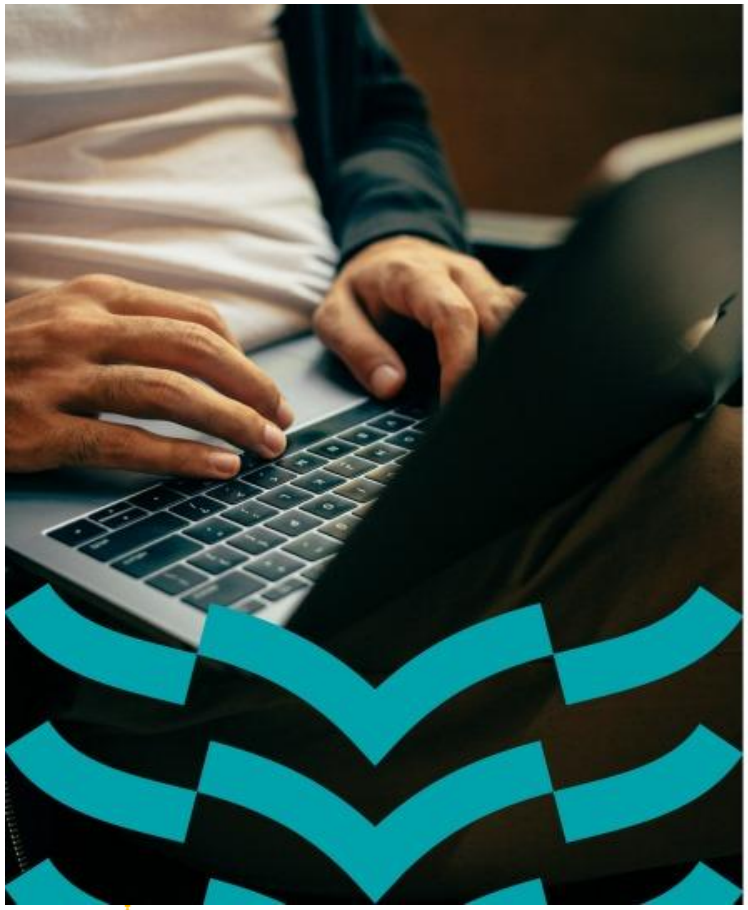


Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade

Pós-Graduação em Compliance de Cibersegurança – PUC-Rio Digital



Visão integrada de Segurança da Informação, Cibersegurança e Proteção da Privacidade



16º Seminário de Proteção à Privacidades e aos Dados Pessoais

Segurança e Privacidade da Informação – Conformidade com as Normas ISO e ABNT

Obrigado!

Prof. Anderson Oliveira da Silva

Gestor de Segurança da Informação
Encarregado de Dados Pessoais
anderson@inf.puc-rio.br

linkedin.com/in/anderson-oliveira-da-silva-58221680