Rio PREFEITURA | GOVERNO E INTEGRIDADE PÚBLICA | SUBSECRETARIA DE TRANSPARÊNCIA E GOVERNO DIGITAL

MODULO

A importância da Gestão de Riscos para a construção de um Governo Digital

Alberto Bastos

CEO & CTO NA MODULO SECURITY SOLUTIONS

abastos@modulo.com
@albastos

MODULO

Nossa história e a LGPD

36 anos

APPROVED COMPANY ISO 27001 Information Security Management Systems
QMS Certification Services

APPROVED COMPANY ISO 27701 Privacy Information Management
QMS Certification Services

CIS Center for Internet Security

MINISTÉRIO DA DEFESA EED EMPRESA ESTRATÉGICA DE DEFESA

MINISTÉRIO DA DEFESA PED PRODUTO ESTRATÉGICO DE DEFESA

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

The Open Group Open FAIR

iapp BRONZE MEMBER

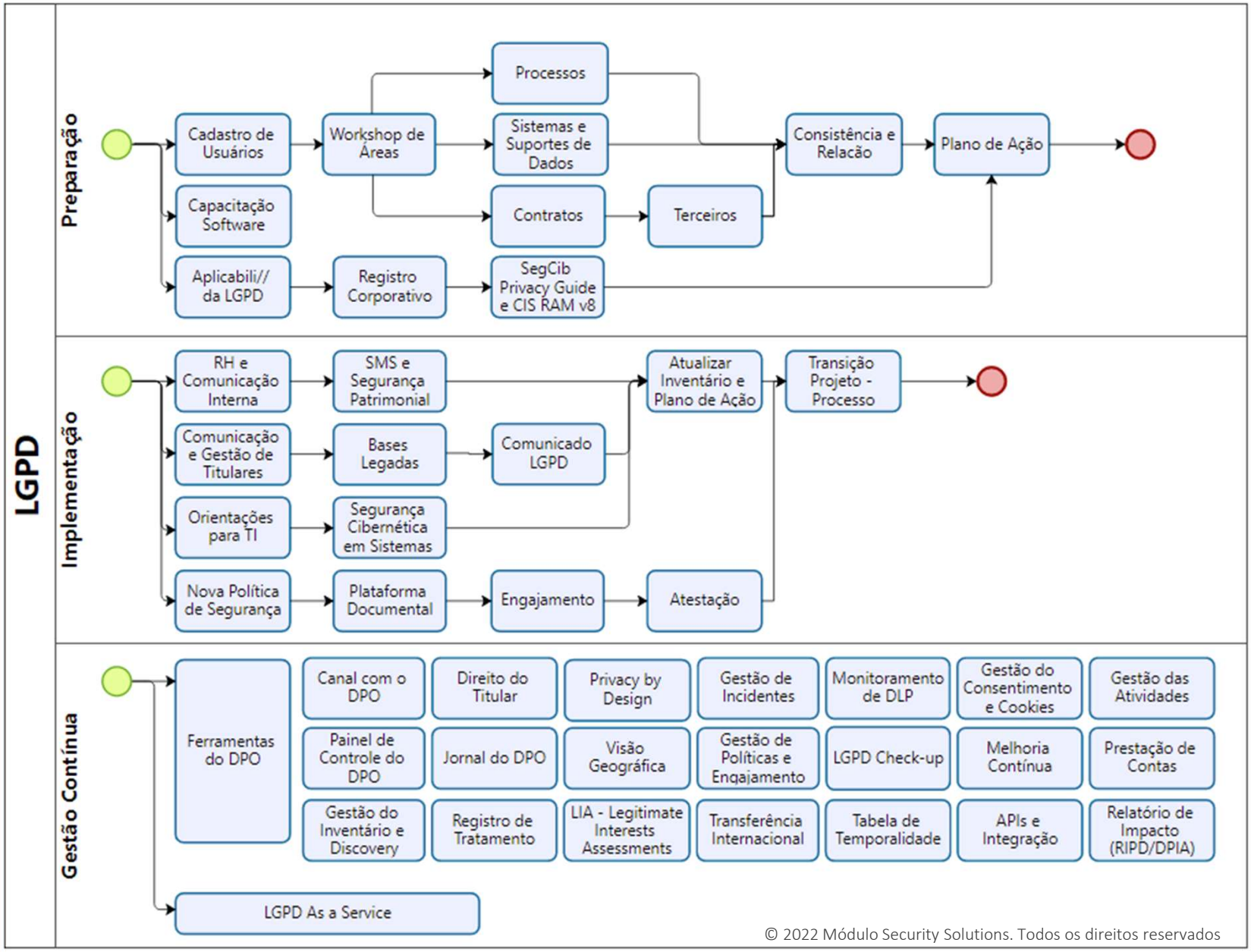
assespro RJ

MODULO

© 2022 Módulo Security Solutions. Todos os direitos reservados

© 2022 Módulo Security Solutions. Todos os direitos reservados

Roadmap LGPD



© 2022 Módulo Security Solutions. Todos os direitos reservados

MODULO

© 2022 Módulo Security Solutions. Todos os direitos reservados

Privacy Day no Cristo

27/01 - 19:00

transmissão ao vivo em:

youtube.com/CristoRedentorOficial

SANTUÁRIO CRISTO REDENTOR

MODULO

MARTINS DE ALMEIDA ADVOGADOS

iapp

MODULO

© 2022 Módulo Security Solutions. Todos os direitos reservados

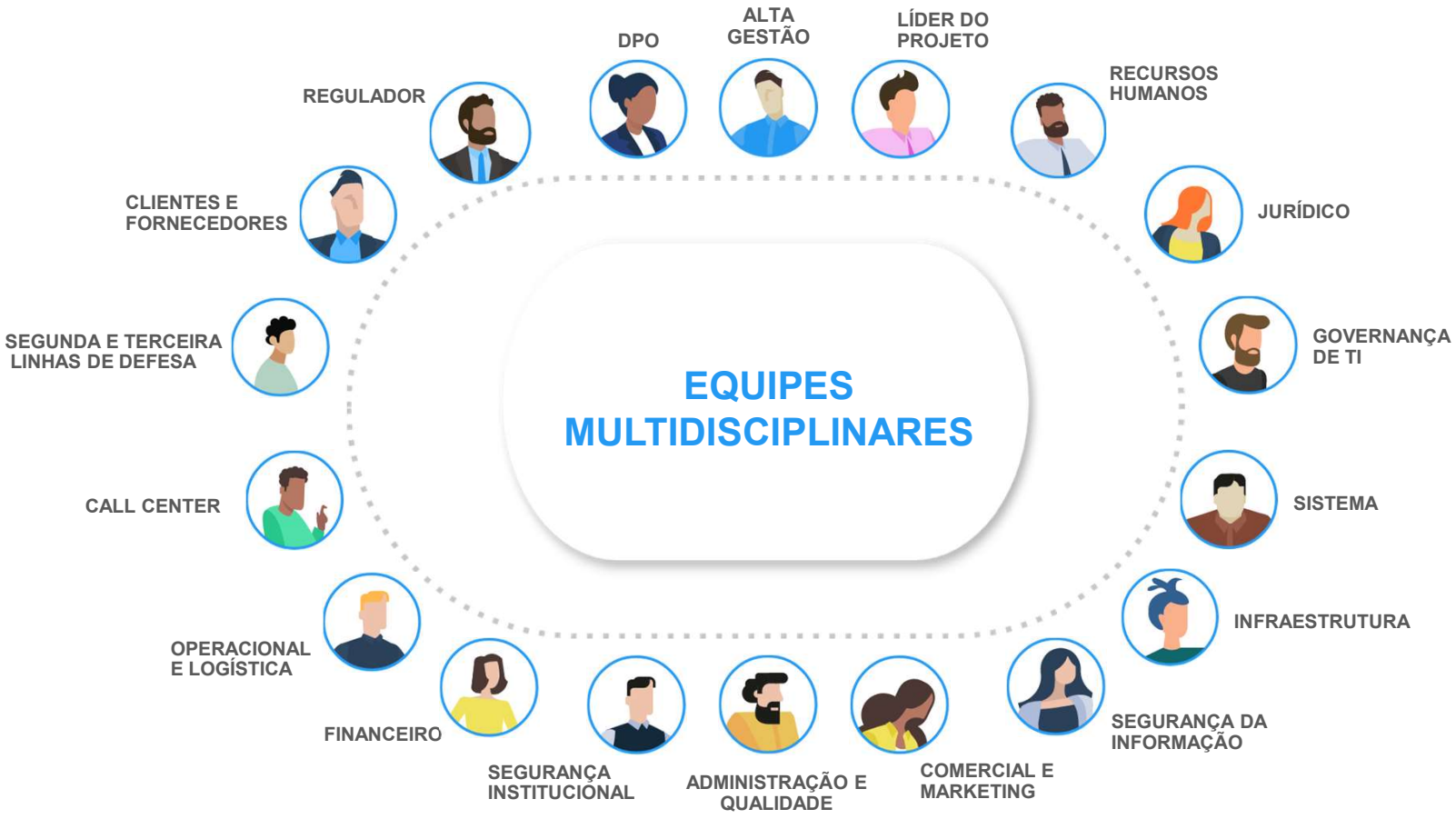
LGPD

Ameaça ou oportunidade?

© 2021 Módulo Security Solutions. Todos os direitos reservados

Pessoas

A LGPD envolve equipes multidisciplinares com profissionais das mais variadas áreas, sistemas e partes relacionadas críticas para o tratamento de dados pessoais.



reservados

© 2022 Módulo Security Solutions. Todos os direitos reservados

Inventário atualizado

Mapeamento do ambiente, sistemas e proteção de dados pessoais na organização, com correlacionamento das informações.

GERAR GRAFO
VISUALIZAÇÃO 3D

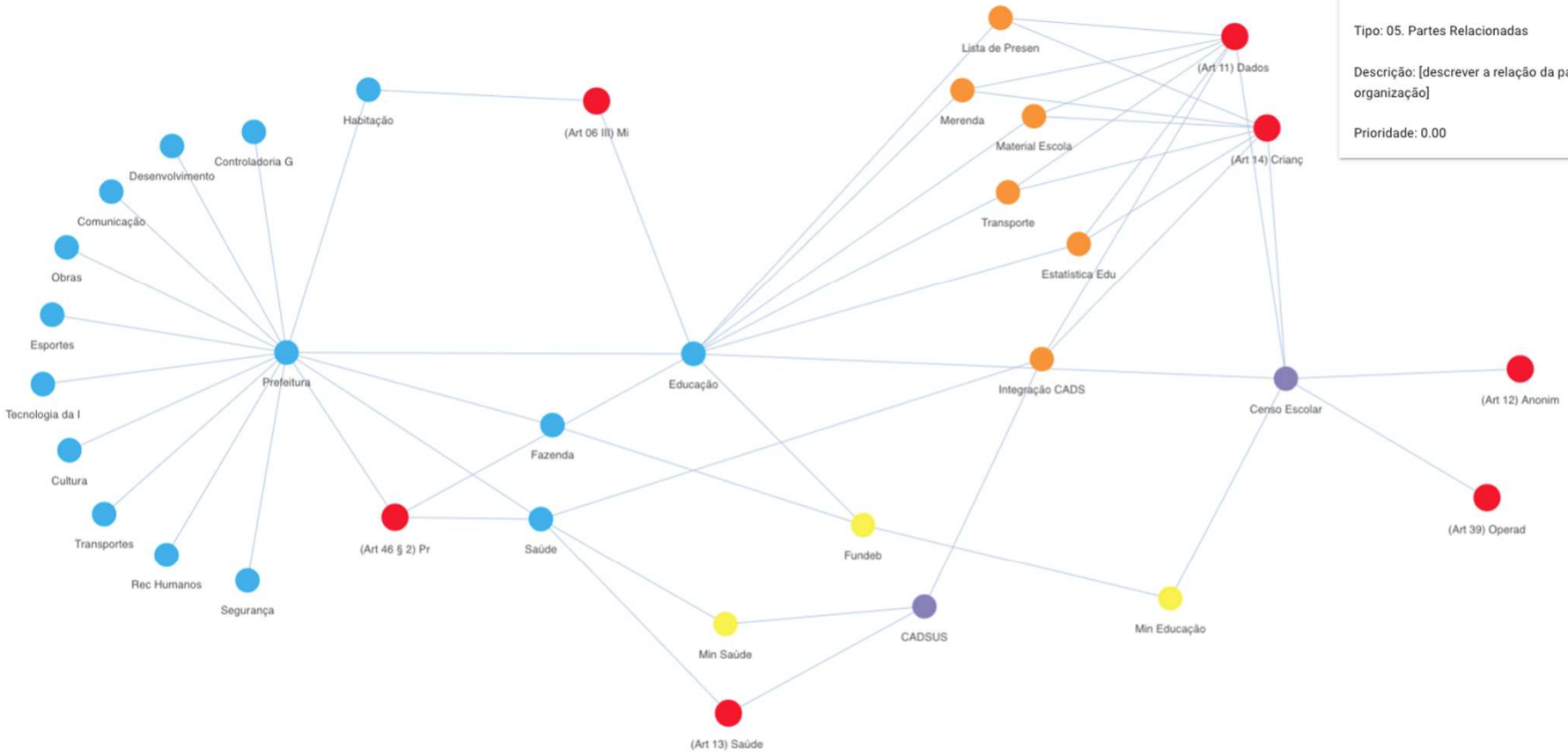
Código: EVTD202202149338

Título:

Tipo: 05. Partes Relacionadas

Descrição: [descrever a relação da parte relacionada com a organização]

Prioridade: 0.00



© 2022 Módulo Security Solutions. Todos os direitos reservados

Cockpit do DPO

Ambiente organizado com painéis de controles que podem ir de alertas no celular até salas de gestão, passando por workflow e dashboards.

reservados

© 2022 Módulo Security Solutions. Todos os direitos reservados

Gestão de riscos

Painel com as informações para apoio a decisão e priorização baseada em gestão de riscos com: os requisitos da Lei, o inventário do negócio e as aplicações necessárias para a gestão dos direitos dos titulares.

[9] Painel de Controle do DPO

Ocorrências e Incidentes

Incidente	Prior
Rule detected - Aviso Encarregado	16,0
Registro no reclameaqui.com - Exemplo	16,0
Notificação da ANPD a pedido de Titular - Exemplo	16,0
Jair Andando	16,0
Ana Liza	16,0
Gestor perdeu o seu token em local não sabido - Exemplo	12,8
Novo Sistema de Gestão de Clientes	12,0
Nova campanha MKT001	12,0
Juscelino Oliveira	12,0
Joaquim José da Silva	12,0
Ivete Eva	12,0
Carla Pires	12,0
Joaquim Manoel	9,6
Usuário solicitou retirada da base RH - Exemplo	9,0
Reunião de Instalação do Comitê da LGPD 04nov2020	9,0
Novo sistema Sys001	9,0
Novo sistema ERPRH	9,0

Direito do Titular

Nome	Prior
[illegible]	16,0
[illegible]	16,0
[illegible]	12,0
[illegible]	12,0
[illegible]	12,0
[illegible]	12,0
[illegible]	9,6

Privacy by Design/Default

Nova atividade	Prior
Novo Sistema de Gestão de Clientes	12,0
Nova campanha MKT001	12,0
Novo sistema Sys001	9,0
Novo serviço de diretório AD em nuvem	9,0
Novo Produto P001	9,0
Novo armazenamento de processos judiciais	9,0
Nova Filial	9,0

Prioridades

Responsável	Qtd	Área	Sistemas	Partes	Atividades	Incidente	Total
[illegible]	105	14,3	38,2	41,7	606,2		700,4
[illegible]	60				573,4		573,4
[illegible]	58				483,0		483,0
[illegible]	42			0,0	364,2	35,6	399,8
[illegible]	22				235,8		235,8
[illegible]	13				192,6	18,0	210,6
[illegible]	19				168,1		168,1
[illegible]	18				136,9		136,9
[illegible]	9				101,0	31,0	132,0
[illegible]	17				122,5		122,5
[illegible]	11					116,6	116,6
[illegible]	9				104,6		104,6
[illegible]	13				101,2		101,2
[illegible]	11				92,2		92,2
[illegible]	207					80,2	80,2
[illegible]	12				78,9		78,9
[illegible]	20	11,1	26,8	10,4	20,3		68,6

Assunto

Assunto	Qtd	Prior
(Art 01, 02, 05) Fundamentos e Definições	34	20,0
(Art 03, 04) Aplicação da Lei	9	0,0
(Art 06, 09, 17 .. 22, 51) Princípios e Direitos do Titular	57	33,2
(Art 06, 09, 17 .. 22, 51) Princípios e Direitos do Titular, (Art 0...	1	16,0
(Art 07) Base Legal, Hipóteses de Tratamento	56	457,1
(Art 08) Consentimento	25	17,0
(Art 10) Legítimo Interesse	15	0,0
(Art 11) Dados Sensíveis	73	493,1

3. Áreas de Negócio

Área	Prior
4.2 RH	14,3
4.3 FC	12,3
2.1 MKT	11,1
3.2 SB	10,8
2.4 NRJ	9,3
4.1 GP	7,5
4.4 TIS	6,5
2.2 NB	6,4

4. Sistemas e Suportes de Dados

Sistema/Suporte	Prior
MS Teams (Cyber)	9,3
Catho	8,0
Site Vagas.com	7,4
Site Nube	7,4
GRRF	7,1
Facebook	7,1
Protheus - Gestão de Pessoal	6,7
CON Social	6,5

5. Partes Relacionadas

Nome	Prior
[illegible]	13,8
[illegible]	8,3
[illegible]	6,3
[illegible]	6,3
[illegible]	6,3
[illegible]	6,3
[illegible]	4,2
[illegible]	4,2

6. Plano de Ação

Atividade	Descrição	Prior
Orientar a equipe de sistemas quanto ao tratamento de dados pessoais de crianças e adolescentes	Macro-atividade (Todos os sistemas que tratam...	20,5
Orientar a área quanto ao tratamento de dados pessoais sensíveis	Macro-atividade (Todas as áreas que tratem da...	20,5
Preencher o ciclo de vida do dado pessoal em cada sistema, suporte e site, incluindo a definição de temporalidade	Macro-atividade (Todos os sistemas)	20,0
Implementar os recursos para atendimento aos direitos do titular (Art 9, 17 a 22)	Macro-atividade (Corporativo)	20,0
Definir os requisitos, implementar e publicar a política de proteção de dados e privacidade	Macro-atividade (Corporativo)	20,0
Avaliar e justificar a base legal (hipótese de tratamento) dos sistemas e suportes de dados	Macro-atividade (Todos os sistemas)	20,0

DPOs

Título	Nome	Prior
[illegible]	[illegible]	0,0
[illegible]	[illegible]	0,0
[illegible]	[illegible]	0,0
[illegible]	[illegible]	0,0
[illegible]	[illegible]	0,0
[illegible]	[illegible]	0,0

© 2021 - Powered by Módulo Risk Manager

reservados

© 2022 Módulo Security Solutions. Todos os direitos reservados

Art. 5º Para os fins desta Lei, considera-se: (1 tópico)

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

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, e deverá mencionar, no mínimo:

IV - os riscos relacionados ao incidente;

© 2022 Módulo Security Solutions. Todos os direitos reservados

Gestão de Riscos

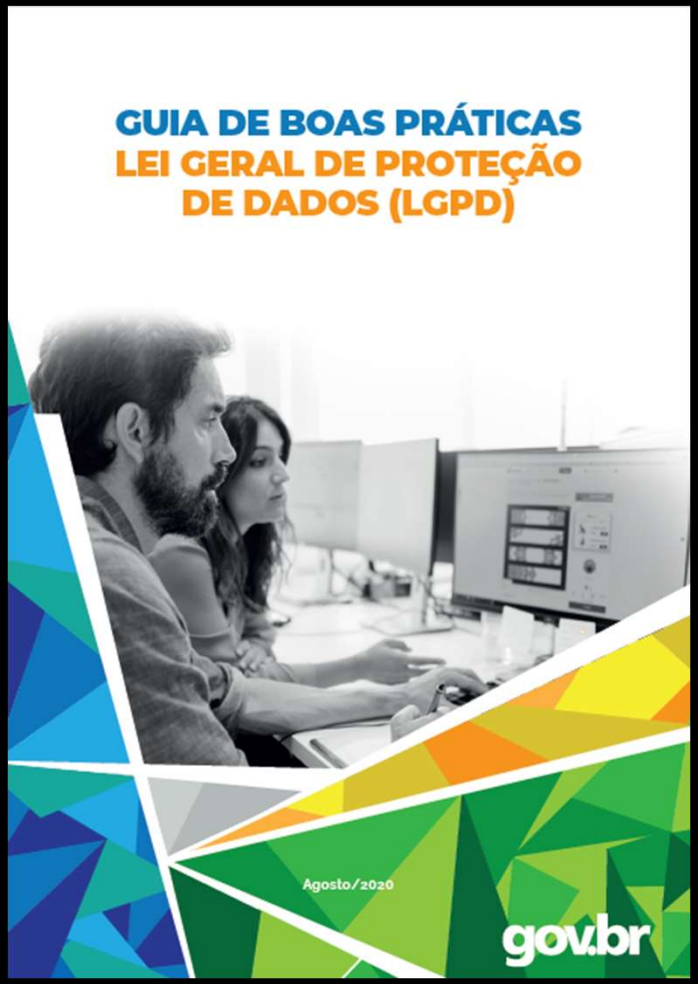


Tabela 5 Risco referente ao tratamento de dados pessoais

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[3]
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda	5	15	75
R04	Roubo	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

© 2022 Módulo Security Solutions. Todos os direitos reservados

[6] Plano de Ação LGPD - Estatística

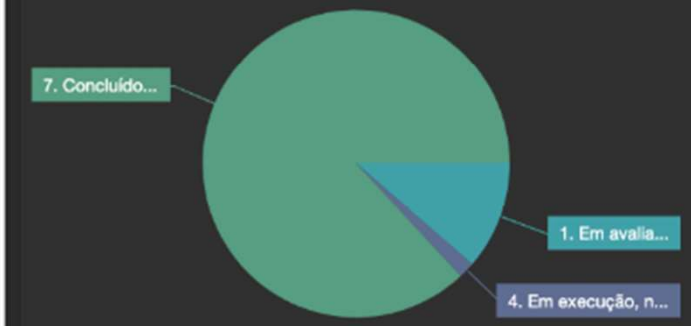
Macro Atividades

Atividade	Qtd	Prior	Média
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas	89	821,0	9,2
Preencher o ciclo de vida do dado pessoal em cada sistema, suporte e site, incluindo a definição de temporalidade	66	688,5	10,4
Preencher as abas de dados de segurança dos sistemas e suportes de dados, e avaliar as demandas de segurança	66	523,5	7,9
Avaliar e justificar a base legal (hipótese de tratamento) dos sistemas e suportes de dados	66	688,5	10,4
Orientar a equipe de sistemas quanto ao tratamento de dados pessoais sensíveis	26	261,3	10,0
Classificar as partes relacionadas	12	122,8	10,2
Orientar a equipe de sistemas quanto ao tratamento de dados pessoais de crianças e adolescentes	7	95,9	13,7
Avaliar com a área a real necessidade de utilizar dados pessoais sensíveis e a possibilidade de minimizar	7	67,3	9,6
Adequar os sites quanto às políticas e avisos a serem publicados	7	76,2	10,9
Adequar os sites quanto ao uso de cookies e sistemas analíticos	7	68,5	9,8

Visão das atividades

Título	Ativo	Prior	Média	Link
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas		18,5	18,5	
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas		16,2	16,2	
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas		15,4	15,4	
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas		15,2	15,2	
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas		15,0	15,0	
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de dados e partes relacionadas		13,9	13,9	
Preencher os pontos focais de proteção de dados para as áreas, sistemas, suportes de		13,7	13,7	

Qtd | Prior



Importância LGPD (lin) vs Facilidade LGPD (...

	2	3	4	Total geral
5	75	200	13	288
4	12	94	9	115
3	5	4	2	11
Total geral	92	298	24	414

Escopo da Atividade

Escopo da Atividade	Qtd	Prior
0. Corporativo	30	484
02. Registro Corporativo	89	821
03. Áreas de Negócio	52	569
04. Sistemas e Suportes de Dados	231	2258
05. Partes Relacionadas	12	123

Ações Consolidadas para Implementação

Ação para Implementação	Qtd	Prior
1. Template: Política de Proteção de Dados e Privacidade	1	20
1.1. Template: Cartilha de Proteção de Dados	1	16
1.1.1. Workshop: Conscientização LGPD	1	17
2. Template: Encarregado pelo Tratamento de Dados Pessoais	1	18
2.1. Software: Atendimento à solicitação de titular	1	20
2.2. Software: Gestão de Incidentes	1	19
2.2.1. Software: Privacy by design	1	16
2.3. Reunião: Publicações complementares	1	14
2.3.1. Reunião: Revisão de políticas corporativas	1	16
2.3.2. Template: Áreas de controle	1	16
2.4. Workshop: Alta Administração	1	16
3. Workshop: Áreas, Sistemas e Partes Relacionadas	89	821
3.1. Workshop: Áreas	27	337
3.1.1. Template: Benefícios para funcionários	1	14

Ponto Focal

Ponto Focal	Qtd	Prior
	90	864
	62	654
	51	477
	15	262
	20	215
	22	211

Assunto	Qtd
(Art 06, 09, 17 .. 22, 51) Princípios e Direitos do ...	1
(Art 07) Base Legal, Hipóteses de Tratamento	66
(Art 08) Consentimento	1
(Art 11) Dados Sensíveis	39
(Art 12) Anonimização	1
(Art 14) Crianças e Adolescentes	15
(Art 33 .. 36. 61) Transferência Internacional	3

Facilidade	Qtd
4. Pode ser realizada com pequeno acréscimo de recursos	2
3. Pode ser realizada com recursos existentes no orçame...	25
2. Exige recursos não previstos em orçamento	9

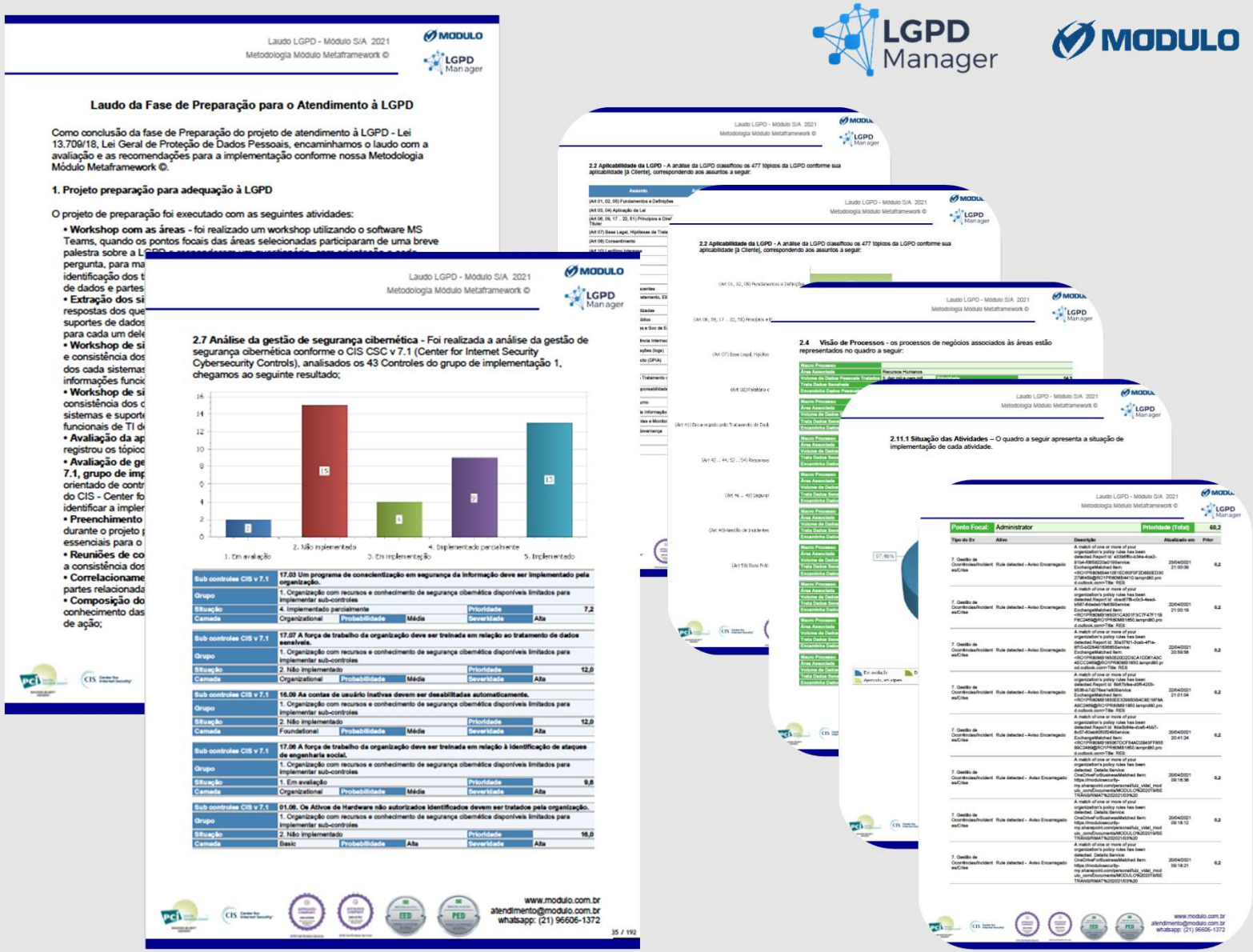
Urgência da Atividade	Qtd
5. Precisa ser realizado imediatamente	297
4. Precisa ser realizado o quanto antes por demandar t...	79
3. Precisa ser realizado até 31 de dezembro de 2020	34
2. Aguardar a definição da ANPD	4

Importância da Atividade	Qtd
5. Ação essencial para o atendimento à LGPD	28
4. Atendimento a requisito relevante da LGPD	11
3. Melhoria de processos com resultados relevantes, apoia...	1

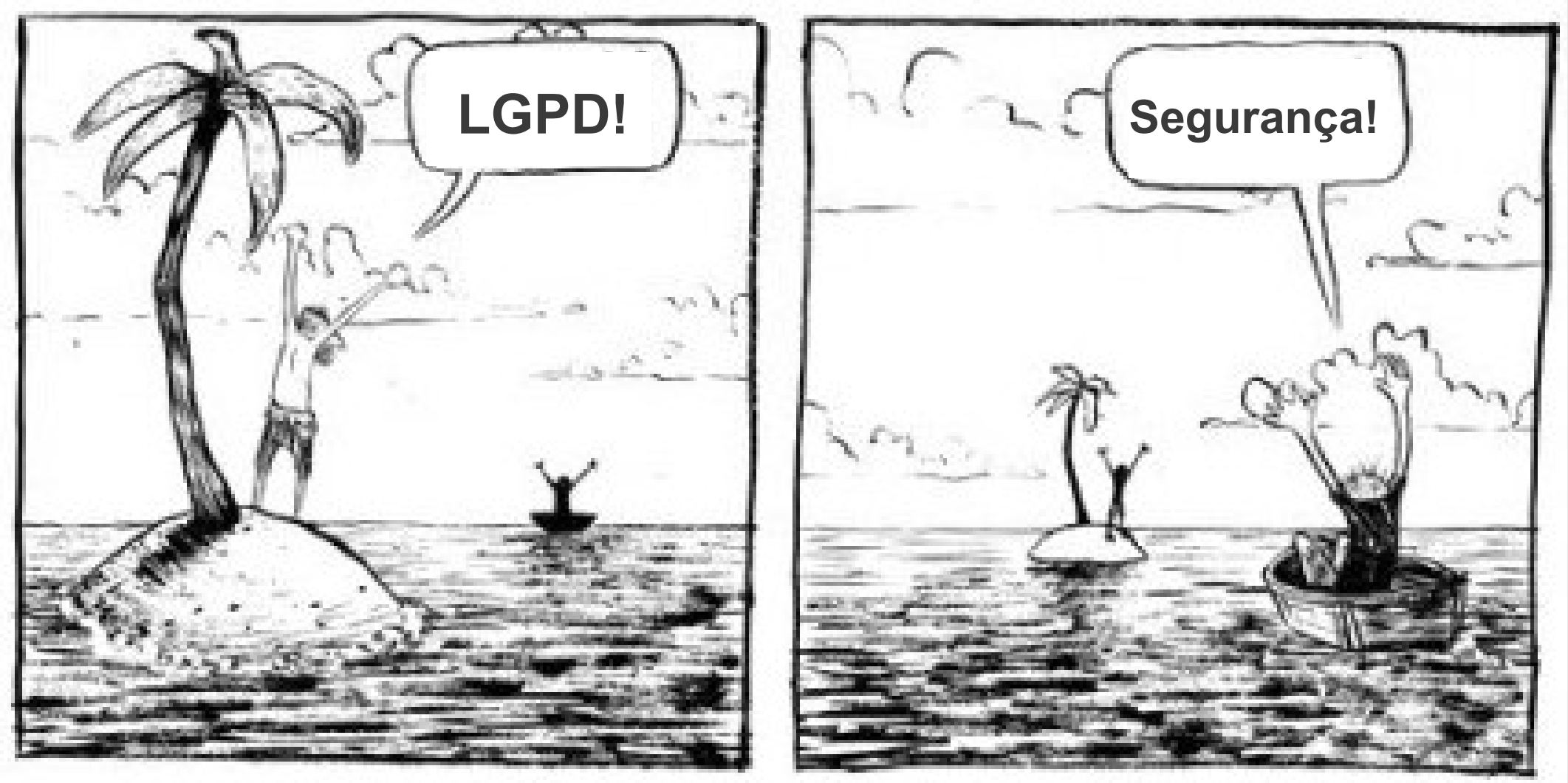
© 2022 - Powered by Módulo Risk Manager

Responsabilização

Prestação de Contas faz parte da LGPD, por isso é necessário gerar tanto relatórios analíticos como visões consolidadas.

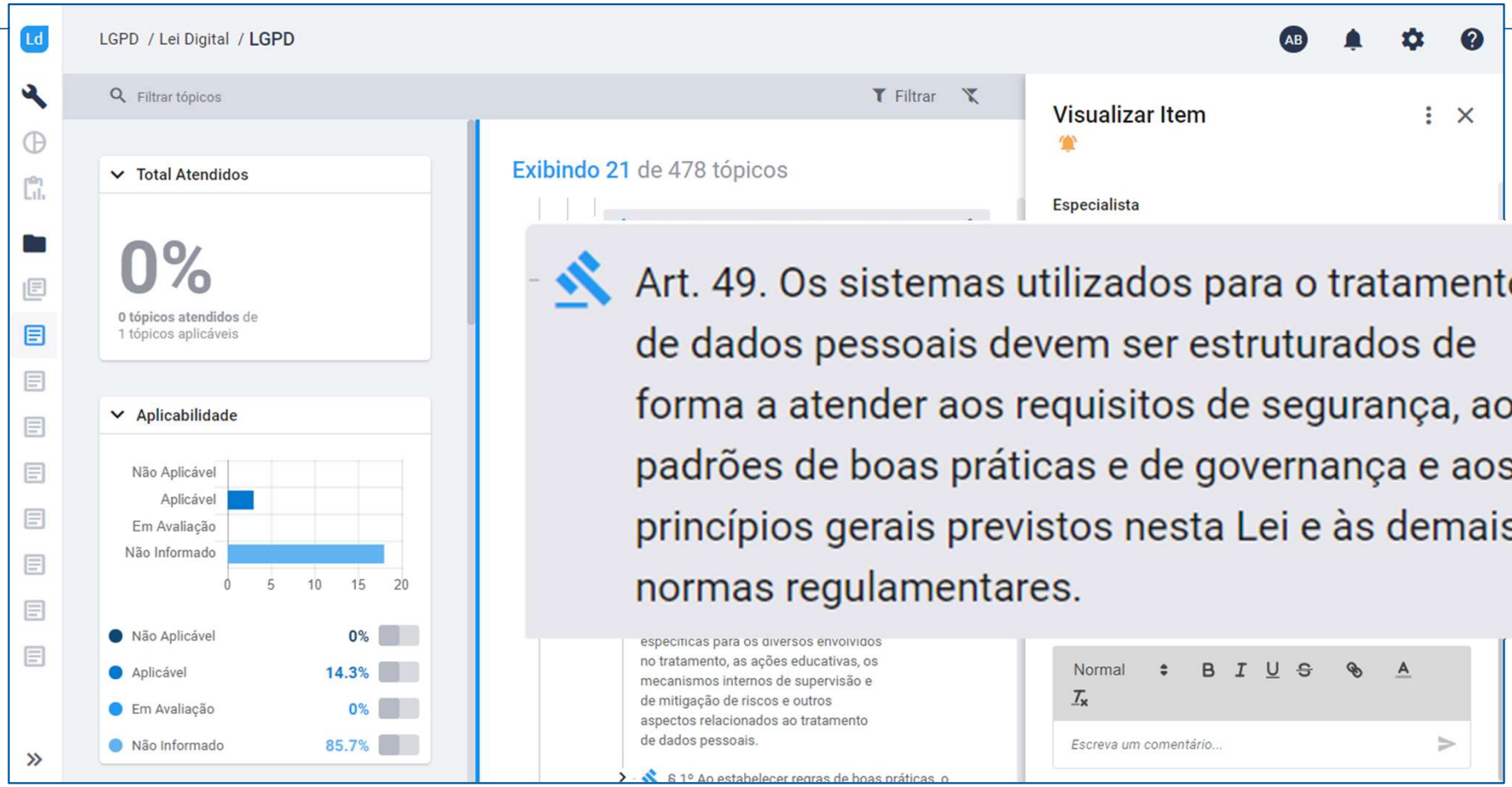


© 2022 Módulo Security Solutions. Todos os direitos reservados



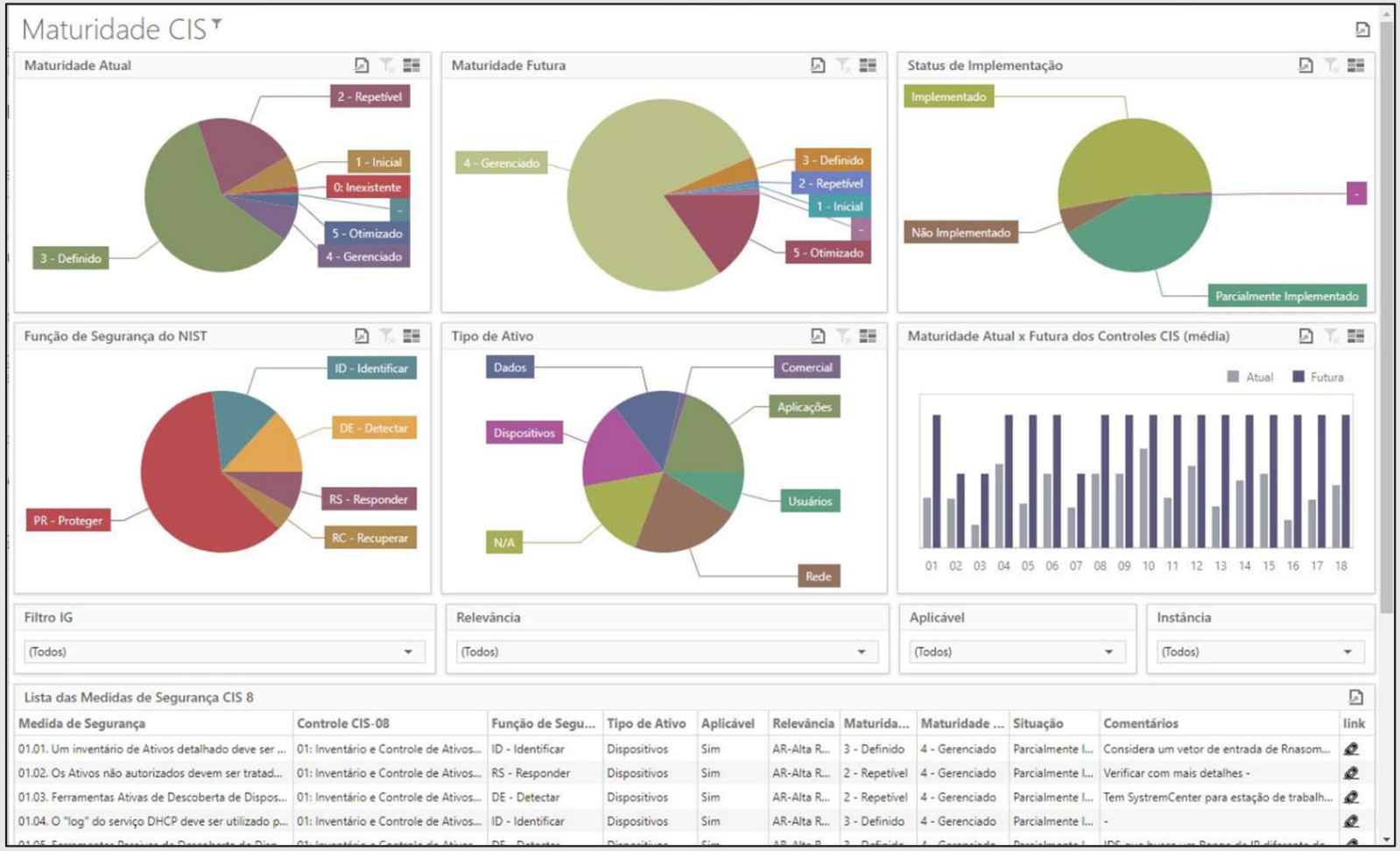
© © 2021 Módulo Security Solutions. Todos os direitos reservados

Padrões de boas práticas e de governança



© 2022 Módulo Security Solutions. Todos os direitos reservados

Painel de Maturidade de Cybersecurity - CIS v8



© 2022 Módulo Security Solutions. Todos os direitos reservados

CIS Center for Internet Security

CIS Controls

Guia Complementar de Privacidade

MODULO

© 2022 Módulo Security Solutions. Todos os direitos reservados

Rio PREFEITURA | GOVERNO E INTEGRIDADE PÚBLICA | SUBSECRETARIA DE TRANSPARÊNCIA E GOVERNO DIGITAL

MODULO

Obrigado!

A importância da Gestão de Riscos para a construção de um Governo Digital

Alberto Bastos

CEO & CTO NA MODULO SECURITY SOLUTIONS

abastos@modulo.com
@albastos

bit.ly/demolgpdmanager