

Segurança da Informação e LGPLD

MS Teams, 02fev2021

Carlos Affonso | caffonso@modulo.com.br

Wander Neto | wander.neto@modulo.com.br

Fernando Nery | fnery@modulo.com.br



Apresentação
para:



Governo Federal

Ministério da Saúde

Nossas Certificações



QMS Certification Services



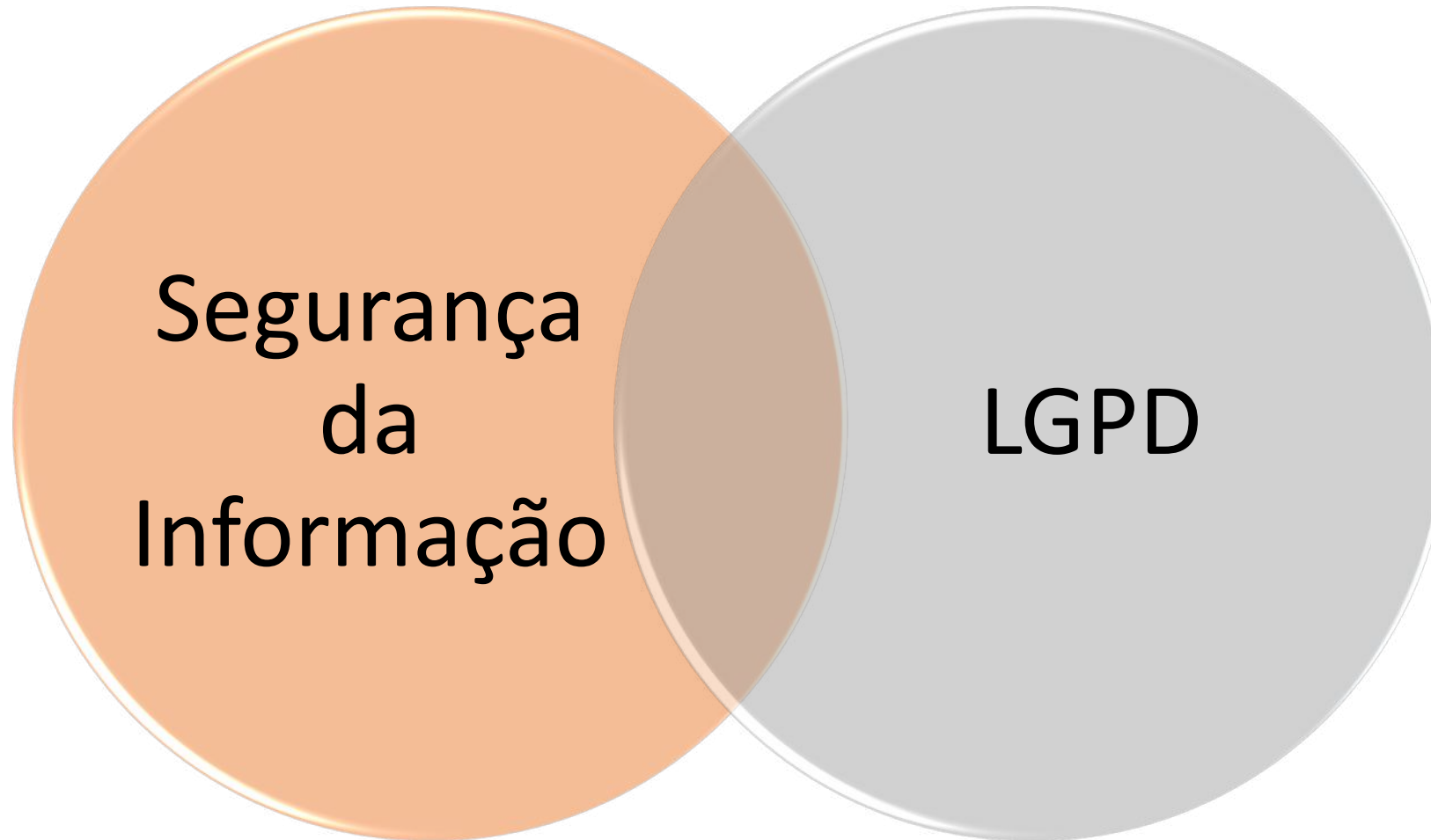
Certificações de Nosso Time



IPOF
International Product Owner
Foundation



O Escopo



Metodologia LGPD



Cockpit do DPO

Implementação

Atividades

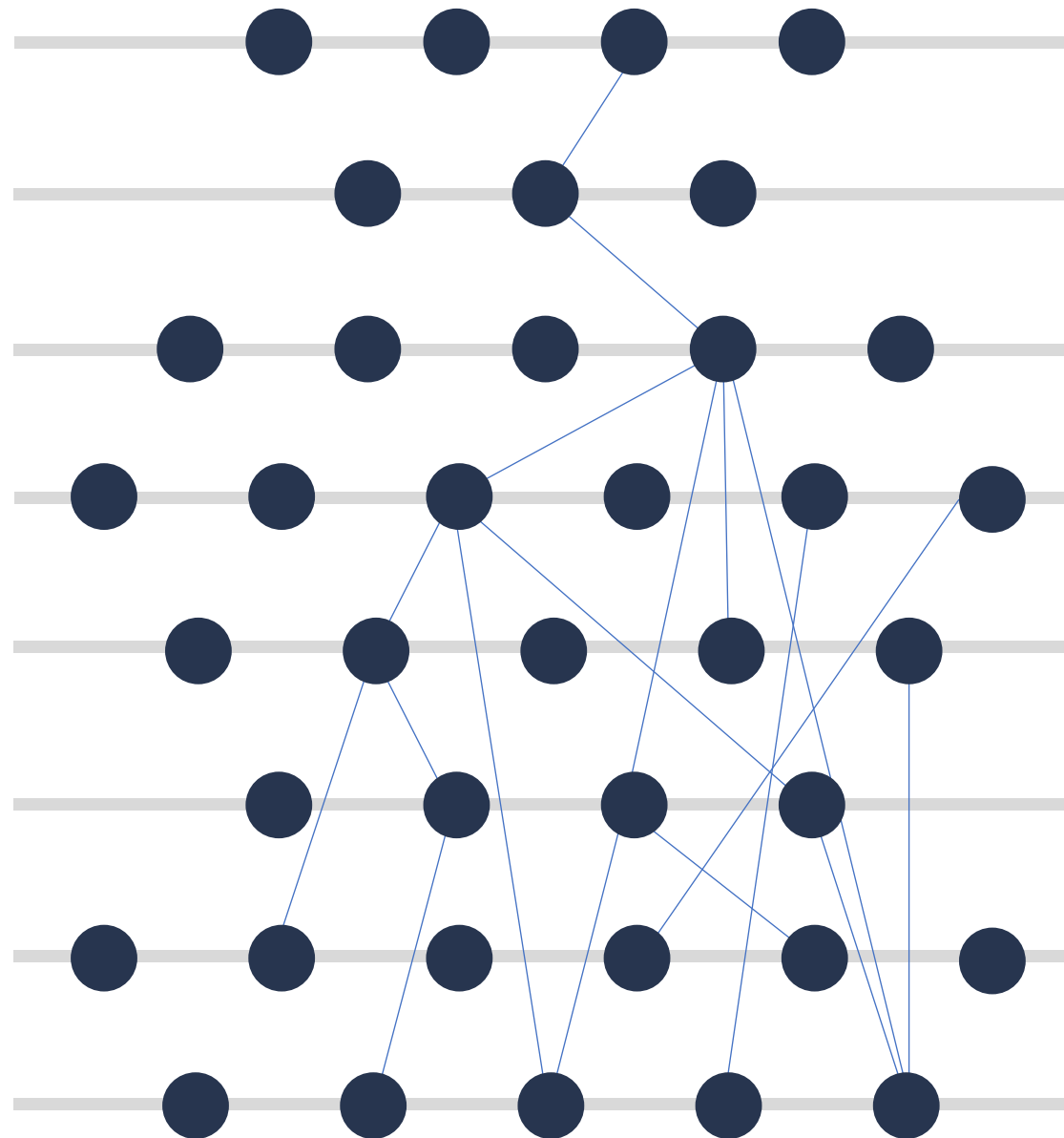
Partes Relacionadas

Sistema e Suporte de Dados

Áreas

Pessoas

LGPD





Projeto em Planilha



Automatização



Templates



Gestão de Incidentes



Direito do Titular



Privacy by Design



Cockpit do DPO



Relatório de Impacto (DPIA)



Segurança Cibernética



APIs: Registro, Cadastro de Dados Pessoais, Consentimento

CIS Controls®
Segurança Cibernética

Registro Corporativo



Macro-atividades



Gestão Contínua



Plano de Ação



Revisão de Documentos



Consistência



Implementação



Partes Relacionadas



Pessoas



Áreas



Sistemas



Lei 13.709 LGPD



Seq	Link	Situação do Requisito
1. Lei 13709		
c01a01pu	Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser ob...	4. Não implementado
c01a02	Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:	4. Não implementado
c01a0211	I - o respeito à privacidade;	4. Não implementado
c01a0212	II - a autodeterminação informativa;	4. Não implementado
c01a0213	III - a liberdade de expressão, de informação, de comunicação e de opinião;	4. Não implementado
c01a0214	IV - a inviolabilidade da intimidade, da honra e da imagem;	4. Não implementado
c01a0215	V - o desenvolvimento econômico e tecnológico e a inovação;	4. Não implementado
c01a0216	VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e	4. Não implementado
c01a0217	VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício d...	4. Não implementado
c01a03	Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por...	8. Monitoramento contínuo...
c01a0311	I - a operação de tratamento seja realizada no território nacional;	4. Não implementado
c01a0312	II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ...	4. Não implementado
c01a0313	III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.	4. Não implementado
c01a03p1	§1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se enco...	4. Não implementado

Assunto	Qtd	Prior
	194	627,7
(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais	37	28,8
(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais, (Art 39) Operador, (Art 50) B...	1	1,2
(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais, (Art 46 .. 49) Segurança da I...	1	9,0
(Art 04) Segurança e Defesa	9	0,0
(Art 07) Base Legal, Hipóteses de Tratamento	13	32,0
(Art 08) Consentimento	21	12,0

Responsável	Qtd	Área	Sistemas	Partes	Ativida...	Incidente	Total
Área-fim LGPD	13				127,2	30,0	157,2
Jurídico LGPD	15				106,8	31,0	137,8
Sistemas LGPD	22				117,4	18,0	135,4
RH LGPD	11					118,0	118,0
Governança de TI LGPD	12				106,8		106,8

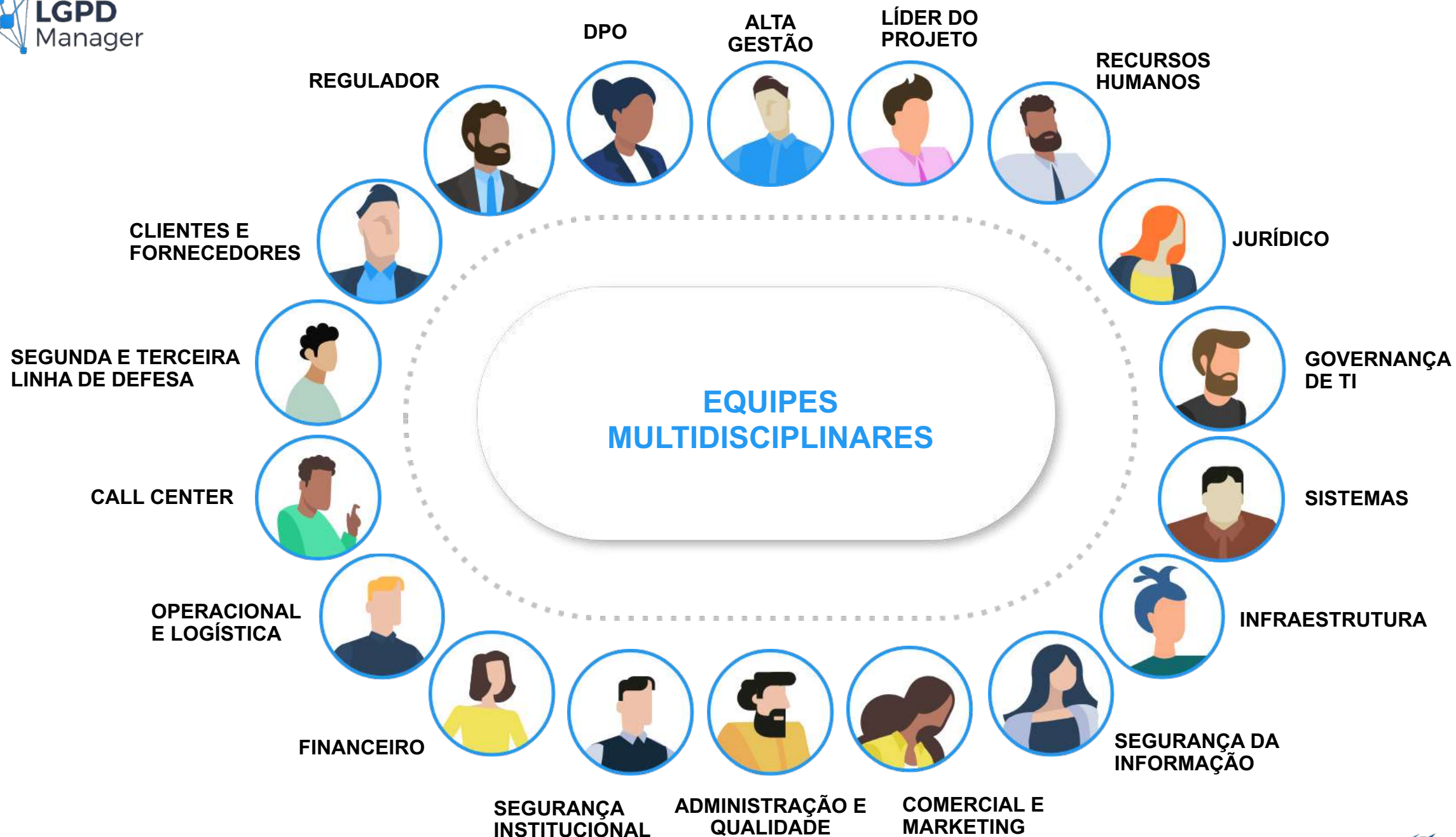
Área	Responsável	Prior
4.2 RH	Líder RH	11,8
2.2 U2	Líder NBSb	11,0
2.1 Mkt	Líder Comunicação	8,3
2.3 U3	Country Manager SP	6,8
1.3 UCM	Líder Comunicação	6,8
3.4 S4	Diretor Serviços I	5,3
2.2 S2	Líder SDR	5,3

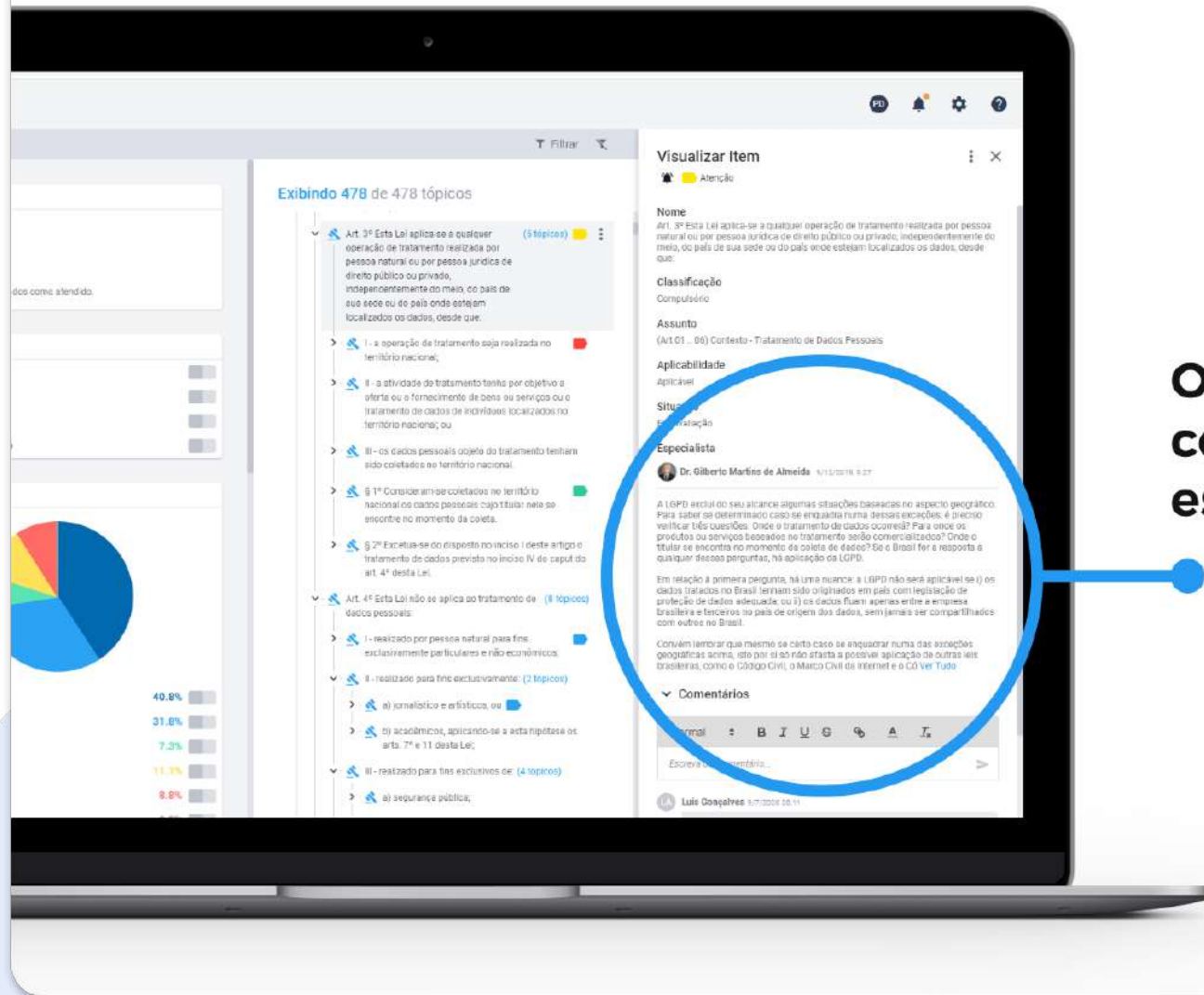
Sistema/Suporte	Responsável	Prior
Backup	Líder Infraestrutura	12,0
App Facebook, Instagram, Twitter	Líder MKT	9,2
Site GoToWebinar	Líder MKT	7,1
Site Broadcast	Líder MKT	7,1
MS LinkedIn	Líder RJN	7,1
LAG	Líder RJN	7,1
CFTV Câmeras	Líder RH	7,0

Nome	Responsável	Prior
Cliente	Líder NBSb	4,4
Cliente CI9	Líder NBSb	4,4
Cliente CI5	Líder NBSb	4,4
Cliente CI4	Líder NBSb	4,4
Cliente CI3	Líder NBSb	4,4
Cliente CI2	Líder NBSb	4,4
Cliente CI1	Líder NBSb	4,4

Atividade	Tipo	Prior
Orientar a área quanto ao tratamento de dados pessoais de...	Ação em área usuária	16,0
Orientar a área quanto ao tratamento de dados pessoais de...	Ação em área usuária	16,0
Avaliar e justificar a base legal (hipótese de tratamento) dos...	Base legal e hipóteses de tratamento	16,0
Avaliar e justificar a base legal (hipótese de tratamento) dos...	Base legal e hipóteses de tratamento	16,0
Avaliar e implementar cláusulas contratuais de tratamento ...	Contratos e relação com parceiros, operador...	16,0

Incidente	Tipo de Ocorrência	Prioridade ...
Registro no reclameaqui.com - Exemplo	Notícia na mídia / redes sociais	16,0
Notificação da ANPD a pedido de Titular - Exemplo	Notificação da ANPD	16,0
Jair Andando	Direito do titular	16,0
Ana Liza	Direito do titular	16,0
Lista de dados pessoais divulgadas no Pastebin - Exemplo	Vazamento de informações	15,0





The screenshot displays the LGPD Manager interface. On the left, there is a sidebar with a pie chart and a list of filters. The main area shows a list of articles under the heading "Exibindo 478 de 478 tópicos". A blue magnifying glass highlights a specific article. On the right, a "Visualizar Item" panel provides details for the selected article, including its name, classification, subject, and applicability. Below this, there is a section for "Comentários" (Comments) with a text input field and a submit button.

Visualizar Item

Atenção

Nome
Art. 3º Esta Lei aplica-se à qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

Classificação
Computacional

Assunto
(Art.01 - 06) Contexto - Tratamento de Dados Pessoais

Aplicabilidade
Aplicável

Situação
Instituições

Especialista
Dr. Gilberto Martins de Almeida 5/13/2018 9:27

A LGPD exclui do seu alcance algumas situações baseadas no aspecto geográfico. Para saber se determinado caso se enquadra numa dessas exceções, é preciso verificar três questões: Onde o tratamento de dados ocorreu? Para onde os produtos ou serviços baseados no tratamento serão comercializados? Onde o titular se encontra no momento da coleta de dados? Se o Brasil for a resposta a qualquer dessas perguntas, há aplicação da LGPD.

Em relação à primeira pergunta, há uma nuance: a LGPD não será aplicável se i) os dados tratados no Brasil tenham sido originados em país com legislação de proteção de dados adequada ou ii) os dados fluírem apenas entre a empresa brasileira e filiais no país de origem dos dados, sem jamais ser compartilhados com outros no Brasil.

Convém lembrar que mesmo se certo caso se enquadrar numa das exceções geográficas acima, isto por si só não obsta a possível aplicação de outras leis brasileiras, como o Código Civil, o Marco Civil da Internet e o CO-Ver Tudo.

Comentários

Formato: B I U G A J

Escreva um comentário...

Luiz Gonçalves 5/13/2018 10:11

Os artigos são
comentados por
especialistas



Obtenha o detalhamento que você precisa

Ld Lei Digital

Relatório

Everest Lei Digital - Relatório Geral

Assinatura: LGPLD v10 (design)
 Número: LD-c20295fc029f4835bcd8edd4c00be4de
 Data: 20 de agosto de 2020
 Gerado por: Patricia Duarte



4. Aplicabilidade

Em Avaliação	3 (6,38%)
Aplicável	18 (56,25%)
Não Aplicável	11 (34,38%)

5. Situação

Situação	%	Tópicos
Não Aplicável	40,63%	13
Em Avaliação	37,50%	12
Atendido Parcialmente	15,63%	5
Não Atendido	6,25%	2
Não Atendido	0,00%	0

3. Assunto

Regulação	0
(Art 48) Gestão de Incidentes e Monitoramento	0
(Art 20) Relação de Consumo	0
(Art 15) Exercício Jurídico e Contencioso	0

Ld Lei Digital 20 de agosto de 2020

6

7. Dados Consolidados

7.1. Consolidado por tópicos

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Assunto: (Art 01 - 06) Contexto - Tratamento de Dados Pessoais
Classificação: Compulsória
Aplicabilidade: Aplicável
Situação: Em Avaliação

Especialista: A privacidade e a liberdade são valores protegidos pela Constituição Federal, e os dados pessoais são informações essenciais para se cogitar tal valor e o desenvolvimento da personalidade humana. De fato, os indivíduos devem poder optar a cada instante sobre qual prioridade querem dar à liberdade ou à privacidade, por meio da autorização ou não de tratamento de seus dados pessoais.

A privacidade demarca um espaço particular na vida humana e por isso é reconhecida como constitutiva de personalidade do indivíduo. Efetivamente, o acesso público a certas informações particulares de uma pessoa tem potencial de favorecer ou coibir seus comportamentos, influenciando o seu agir natural e a construção de sua história pessoal.

Visto por outro ângulo, o deasseamento excessivo da vida privada por meio de aproveitamento indiscriminado dos dados pessoais inflige ao indivíduo e uma situação de vigilância invasiva e recorrente com o dano à dignidade.

Tal contexto é especialmente pertinente à sociedade contemporânea, em que os dados pessoais assumem acentuado valor moral, social, político e econômico, o que reforça a necessidade de dotar o indivíduo de capacidade de autodeterminação informativa.

A LGPD tem por objetivo proteger os dados pessoais, assim entendidos como os dados que identificam ou tornam identificável um indivíduo. Dados referentes a pessoas jurídicas são regulados por outras leis (como, por exemplo, as que disciplinam o nome comercial e o nome de estabelecimento).

A proteção conferida pela LGPD abrange dados pessoais em meio digital ou não. Portanto, dados pessoais que existam em uma das formas, ou em ambas, devem ser tratados de acordo com a LGPD independentemente do tipo de meio físico de suporte.

Como lei ordinária que é, a LGPD não é capaz de alterar a Constituição Federal, inclusive quanto a repartição de prerrogativas federativas para estados. Logo, a menção no parágrafo único do art. 1º, e que as normas da LGPD são de interesse nacional e vinculam União, Estados, Distrito Federal e Municípios, podem ser vistas principalmente como enunciação de uma agenda sensível e programática de buscar consistência de interpretação e aplicação.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Marcador: Excludente

Assunto: (Art 01 - 06) Contexto - Tratamento de Dados Pessoais
Classificação: Compulsória

Serena	Aadi	Ray	Rafa	Jessica	Kat	David
Babak	Charlotte	Danielle	Kelby	Maggie	Ty	Cynthia
Serena	Nathan	Krystal	Edwin	Lotia	Jacky	Yvette
Charlie	Jason	Samantha	Alice	Chris	Filip	April
Jon	Annie	David	Lola	Shawn	Kai	Jamie
Nell	Ryan	William	Deborah	Thomas	Dennis	Kevin
Mukesh	Kim	Julia	Windy	Isabelle	Jennifer	Ryan



Beth



Pete



MJ





Questionário LGPLD - Lei 13709

Lei Geral de Proteção de Dados Pessoais

Dados Pessoais

4. P01Art01..06 - Sua area trata dados pessoais?

- 1. Sim
- 2. Não
- 3. Não Sei

5. P01jArt01..06 - Que sistemas e suportes de dados tratam dados pessoais?

Questionário LGPLD Módulo - Lei 13.709/18
Lei Geral de Proteção de Dados Pessoais EXEMPLO

Sobre Tratamento de Dados Pessoais

4

P01Art01..06 - Sua área trata dados pessoais?

LGPLD Art 5, Inciso I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável. Ex: nome, email, telefone...



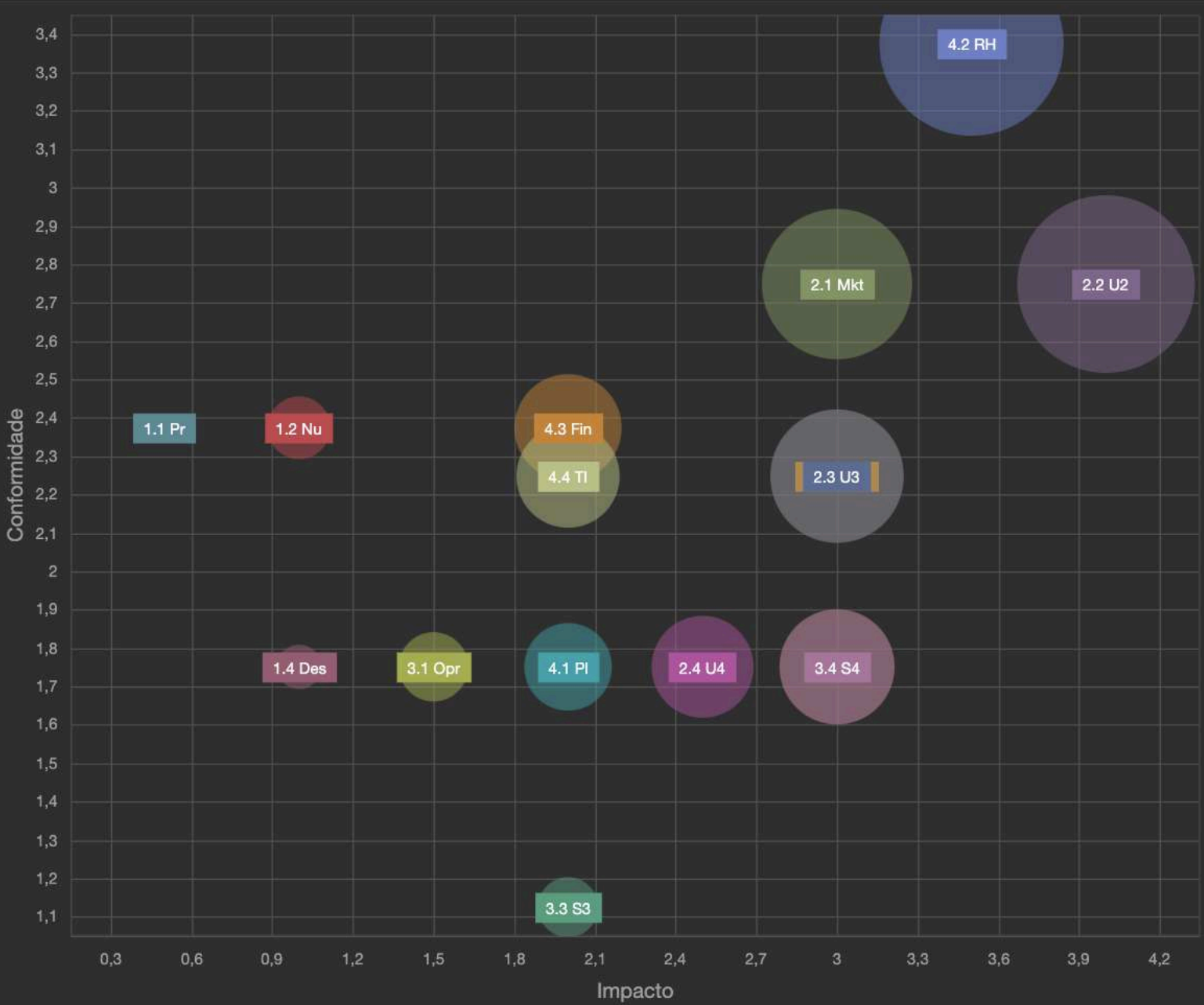
- 1. Sim
- 2. Não
- 3. Não Sei

5

P01jArt01..06 - Que sistemas e suportes de dados tratam dados pessoais? Fique à vontade para comentar.

Informe que sistemas e suportes de dados são utilizados por sua área para tratar dados pessoais. Se possível informe os sistemas e suportes de dados um por linha. Devem ser informados todos os sistemas e suportes de dados, como: sistemas internos e externos, planilhas, dados em papel, redes sociais (facebook, instagram) e mensagem instantânea (whatsapp, ...). Inclua comentários se for o caso.

Enter your answer



Área	Responsável	Conformidade	Impacto	Volume	Pri...
4.2 RH	Líder RH	3,4	3,5	3. dez mil a cem mil	11,8
2.2 U2	Líder NBSb	2,8	4,0	3. dez mil a cem mil	11,0
2.1 Mkt	Líder Comunicação	2,8	3,0	3. dez mil a cem mil	8,3
2.3 U3	Country Manager SP	2,3	3,0	2. mil a dez mil	6,8
1.3 UCM	Líder Comunicação	2,3	3,0	2. mil a dez mil	6,8
3.4 S4	Diretor Serviços I	1,8	3,0	1. menos de mil	5,3
3.2 S2	Líder SPB	1,8	3,0	1. menos de mil	5,3
4.3 Fin	Líder Adm & Fin	2,4	2,0	1. menos de mil	4,8
4.4 TI	Diretor Serviços I	2,3	2,0	2. mil a dez mil	4,5
2.4 U4	Líder RJN	1,8	2,5	1. menos de mil	4,4
4.1 PI	Líder Estratégia	1,8	2,0	1. menos de mil	3,5
3.1 Opr	Líder Software	1,8	1,5	1. menos de mil	2,6
1.2 Nu	Líder Produtos	2,4	1,0	1. menos de mil	2,4
3.3 S3	Country Manager SP	1,1	2,0	1. menos de mil	2,3
1.4 Des	Líder Desenvolvimento	1,8	1,0	1. menos de mil	1,8
1.1 Pr	Líder Produção	2,4	0,5	1. menos de mil	1,2



Qtd Áreas

23

Trata DP?	Qtd	Prior	DP sensíveis?	Qtd	Prior	Encaminha DP?	Qtd	Prior	Recebe DP?	Qtd	Prior
1. Sim	20	768,3	1. Sim	8	477,7	1. Sim	13	712,3	1. Sim	16	758,7
DP crianças?	Qtd	Prior	DP adolescentes?	Qtd	Prior	Transf. internacional?	Qtd	Prior	TXT, XLS, ...?	Qtd	Prior
1. Sim	7	502,4	1. Sim	10	578,4	1. Sim	9	155,3	1. Sim	18	756,2
DP Idosos?	Qtd	Prior	Imagem, voz, ...?	Qtd	Prior	R Sociais, Msg Inst?	Qtd	Pr...	Publica Sites?	Qtd	Prior
1. Sim	10	622,5	1. Sim	17	731,5	1. Sim	13	70...	1. Sim	12	343,2

Suporte Analógic...	Qtd	Pr...
1. Sim	9	60...

Responsável	Qtd	Prior
Administrator	3	0,0
Alberto Bastos	1	7,5
Alexandre Lyra	10	9,3
Artur Duarte Vidal	1	2,0
Carlos Affonso	8	6,4
Carolina Duarte	6	3,9
Cássio Ramos	1	3,5
Eduardo Poggi	3	2,0
Fábio Botelho	1	6,0
Fabio Lerke	1	16,0
Guilherme Poggi...	9	6,5
Isabella Igreja	8	11,1
Lucila Velloso	24	14,3
Marcio Cordeiro...	3	4,4
Rodrigo Brito	1	10,8
Rodrigo Morais	2	2,0
Ronald Marinho	1	12,3
Thiago Mendes ...	8	1,8
tiago (excluído)	1	5,5

Área	Responsável	Conform	Impacto	Volume Dados Pessoais	Prior
1.1 GPS	Eduardo Poggi	1,3	1,5	1. menos de mil	2,0
1.2 EVT	Carolina Duarte	2,6	1,5	1. menos de mil	3,9
1.3 UCM	Marcio Cordeiro Galvão	1,8	2,5	1. menos de mil	4,4
1.4 DRM	Fábio Botelho	2,4	2,5	4. cem mil a um milhão	6,0
2.1 MKT	Isabella Igreja	3,2	3,5	3. dez mil a cem mil	11,1
2.2 NB	Carlos Affonso	1,8	3,5	2. mil a dez mil	6,4
2.3 NSP	Vanessa Moreno	2,3	3,5	2. mil a dez mil	7,9
2.4 NRJ	Alexandre Lyra	2,3	4,0	3. dez mil a cem mil	9,3
3.1 ORM	Thiago Mendes Pereira	0,9	2,0	1. menos de mil	1,8
3.2 SB	Rodrigo Brito	3,1	3,5	2. mil a dez mil	10,8
3.3. SSP	tiago (excluído)	1,8	3,0	2. mil a dez mil	5,5
3.4 SRJ	Cássio Ramos	1,4	2,5	2. mil a dez mil	3,5
4.1 GP	Alberto Bastos	3,0	2,5	1. menos de mil	7,5
4.2 RH	Lucila Velloso	3,6	4,0	3. dez mil a cem mil	14,3
4.3 FC	Ronald Marinho	3,5	3,5	2. mil a dez mil	12,3
4.4 TIS	Guilherme Poggi de Arau...	2,2	3,0	1. menos de mil	6,5
[Requisição do T...	Administrator	0,0	0,0	0. Não respondido	0,0
[Requisição do T...	Administrator	0,0	0,0	0. Não respondido	0,0
[Requisição do T...	Administrator	0,0	0,0	0. Não respondido	0,0

Tipo de Dados Pessoais	Qtd	Prior
Nome	9	59,8
Endereço eletrônico (e-mail)	8	53,3
Fotos	7	54,0
Número de telefone	7	53,4
Cargo / função ou patente	6	49,5
Endereço funcional	5	32,6
Endereço residencial	3	31,9
Endereços em redes sociais	3	26,8
Endereços IP	3	12,2
Data de nascimento	2	16,2
Filiação	2	18,2
Formação escolar	2	11,2
Naturalidade ou nacionalidade	2	20,8
Número de documento de identida...	2	23,7
APPs ou programas de computado...	1	14,3
Assinatura	1	14,3
Biométricos (digital/ reconhecimen...	1	6,5
CNPJ vinculado a pessoa física	1	14,3
Dados sobre salário	1	14,3



Automatização de Relatórios



Relatório de Áreas para LGPLD

Emissão 17/06/2020

Instância mdl
Área 4.2 Gestão de Pessoas
Responsável Líder RH
Descrição 4.2 Gestão de Pessoas

Conformidade	Impacto	Volume Dados	Prioridade
3,38	3,5	3. dez mil a cem mil	11,81

Dados Cadastrais

Faz parte do escopo da LGPLD? 1. Sim

Processo de Negócio Aplicável

Coordenador Líder Estratégia

Envolvidos

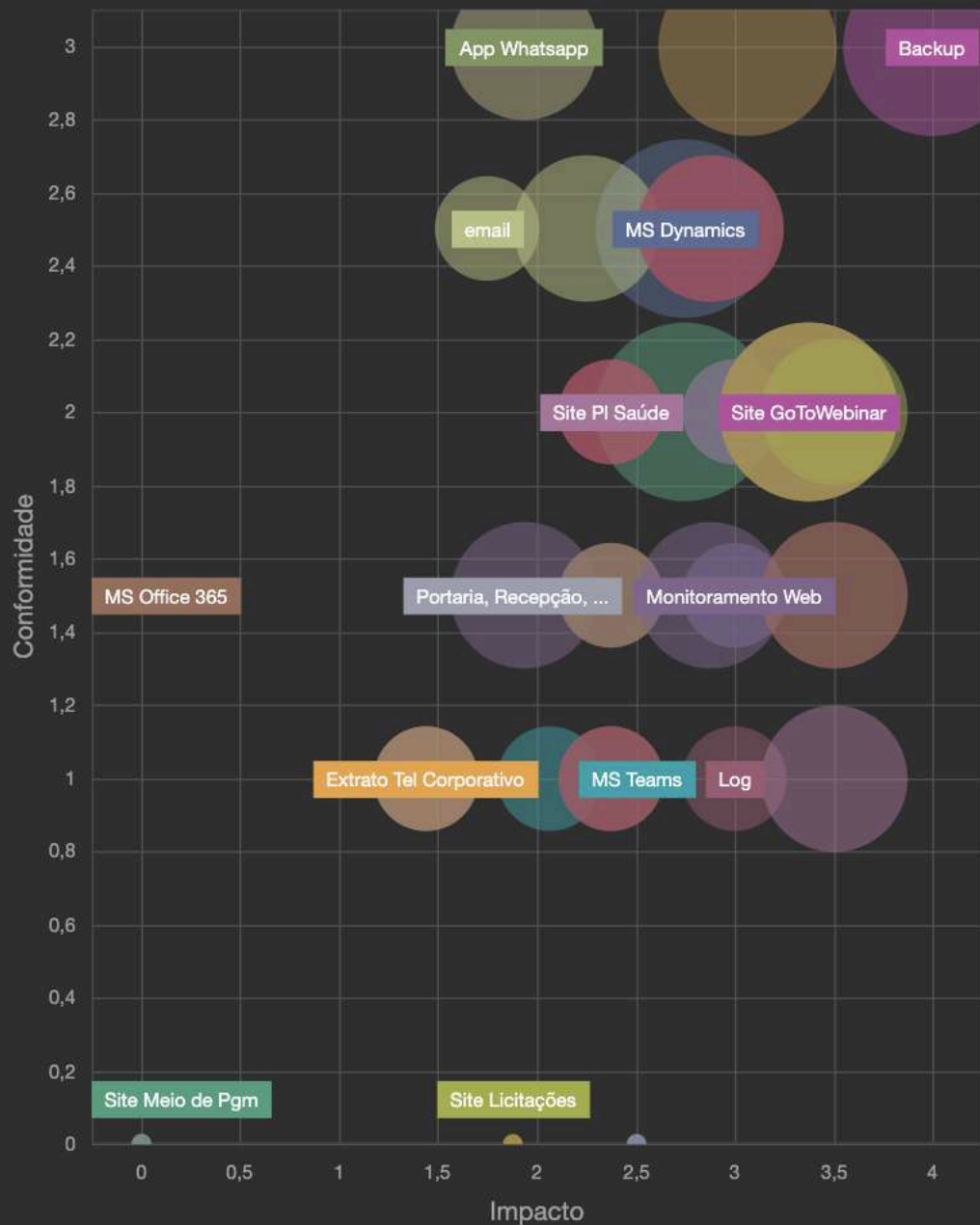
Atualizado em 19/05/2020 07:59:14

Dados Pessoais

Sua área realiza o tratamento de 1. Sim dados pessoais?

Quais sistemas tratam dados pessoais?

- email Corporativo - fatura de celular corporativo
- email Corporativo
- ERP
- Excel
- Linkedin
- MS Office 365
- Ponto Automatizado
- Site cartão refeição
- Site vale transporte
- Taxi: 99, Easy, Uber
- Triton
- Vagas.com
- Portal do plano de saúde, operado pela corretora SEFIP



Sistema e Suporte	Responsável	Pri...	Fornecedor/Operador	Qtd	Prioridade
Backup	Líder Infraestrutura	12,0	[definir o nome do prestador de serviço ou operador do sistema]	32	80,8
App Facebook, Instagram, Twitter	Líder MKT	9,2	Linkedin + Sales Navigator (contrato), Facebook (sem contrato)	1	9,2
Site GoToWebinar	Líder MKT	7,1	RD	1	7,1
Site Broadcast	Líder MKT	7,1	Linkedin/Microsoft	1	7,1
MS LinkedIn	Líder RJN	7,1	LAG	1	7,1
LAG	Líder RJN	7,1	GoToMeeting	1	7,1
CFTV, Câmeras	Líder RH	7,0	Vagas.com, LinkedIn	1	6,8
Site Currículuns/vagas	Líder RH	6,8	Totvs	1	6,8
MS Dynamics	Líder RJN	6,8	Docebo	1	6,0
IRenda Colab	Líder Adm & Fin	6,8			
ERP Proteus	Líder Adm & Fin	6,8			
Triton	PMO LGPD	6,0			
Site LMS	Líder RH	6,0			
App Whatsapp	Líder Infraestrutura	5,9			
App Telegram	Líder Infraestrutura	5,9			
Suportes Analógicos	Seg Empresarial LGPD	5,5			
MS OneDrive	Líder Infraestrutura	5,3			
DataLake/DW/BI	Líder Serviços	5,0			
Site Cartão Refeição	Líder RH	4,8			
Solic Despesas	Líder Adm & Fin	4,0			
MS Power BI	Líder Serviços	4,0			
Arq Planos (xls, txt, ...)	Líder Infraestrutura	4,0			

Responsável	Qtd	Prioridade
Líder RH	12	46,1
Líder Infraestrutura	13	44,8
Líder Adm & Fin	7	24,2
Líder MKT	5	23,4
Líder RJN	3	21,0
Líder Serviços	4	9,0
PMO LGPD	1	6,0
Seg Empresarial LGPD	1	5,5
Líder Estratégia	2	4,9
Projeto LGPD	4	0,0

Lista de sistemas	Qtd	Priori...	Suporte de DP	Qtd	Prio...	Tipo de tratamento	Q..	Pri...
0. Não respondido	33	70,6	0. Não respondido	9	0,0	0. Não Respondido	10	6,8
1. Sim	6	32,8	1. Ambiente interno (datacenter ou colocation sob responsabilidade do controlador)	11	51,3	1. Pelo próprio controlador	18	73,9
2. Não	18	81,5	2. Nuvem (IaaS - PaaS - SaaS - Storage - Colocation sob responsabilidade do operador)	25	78,1	2. Por um operador (verificar contratos e procedimentos)	22	86,5
			3. Microsoft 365, Google Suite e Aplicação do usuário	3	15,3	3. Responsabilidade dividida ou difusa	7	17,8
Citado por usuário?	30	75,9	4. Suporte Analógico (papel, microfilme, mídia externa)	6	19,4			
0. Não respondido	4	0,0	5. Mensagem Instantânea e Redes Sociais	3	20,9			
1. Sim	21	106,1						
2. Não	2	3,0						

Arquitetura da Solução Metodologia Modulo Metaframework



 **EXEMPLO Partes Relacionadas**
Avaliação LGPLD (Lei 13.709/18)

Bom dia,

Você recebeu este formulário por ser parte relacionada (cliente, fornecedor, parceiro, associado etc.) da Contoso. O preenchimento deste documento tem o objetivo de apoiar o atendimento da adequação à Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais - LGPLD. Muito obrigado pela participação!

Nosso objetivo, é obter um conjunto de informações preliminares sobre o tratamento de dados pessoais por sua organização, além de abordar os temas de proteção de dados presentes na LGPLD.

Não há respostas certas ou erradas, portanto fique à vontade e responda com a maior precisão que puder. Isso é muito importante.

No questionário, sua instituição é chamada de "Organização".

A equipe de suporte está à disposição para esclarecer dúvidas e receber sugestões.

Obrigado,

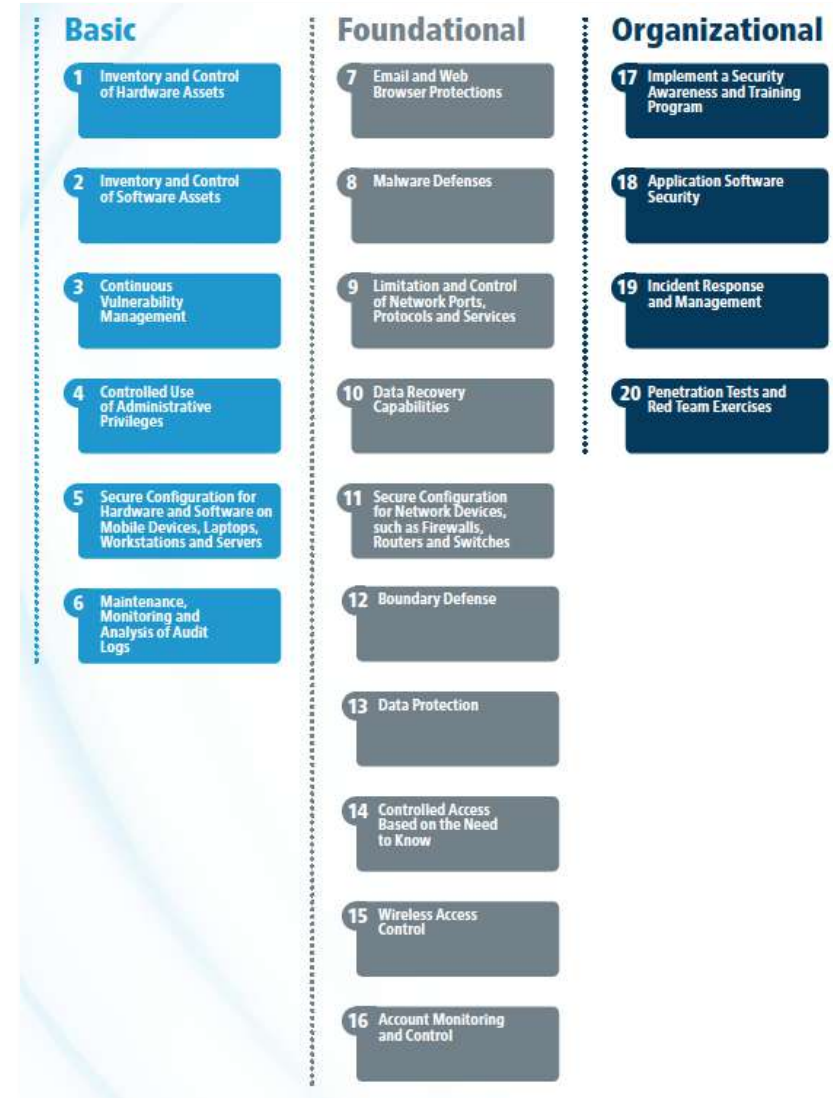
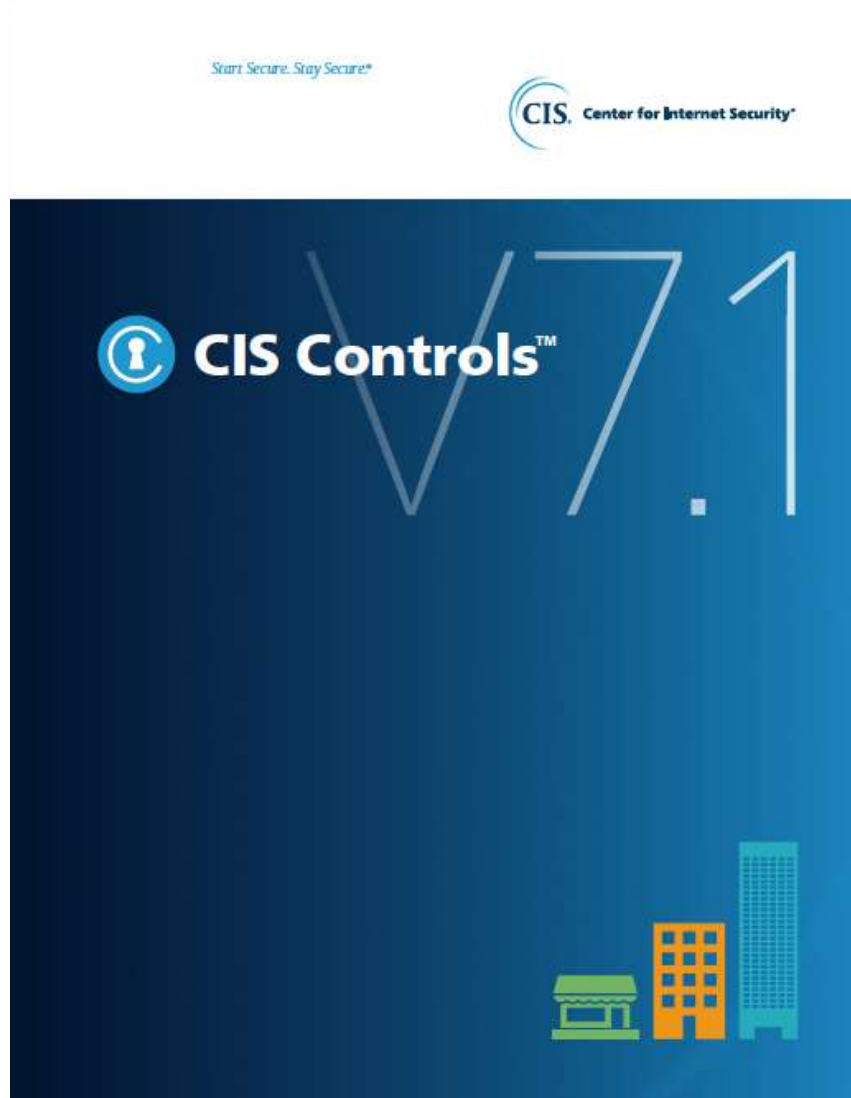
Zé Paça - Suprimentos
email@contoso.com.br

* Required

1. Qual o nome da sua organização? *
2. PR01Art50 Qual o CNPJ da Organização? *
3. Endereço, Cidade e Estado da Organização *
4. Responsável pela Resposta *
5. Cargo do Responsável pela Resposta *

1. Qual o nome da sua organização? *
2. PR01Art50 Qual o CNPJ da Organização? *
3. Endereço, Cidade e Estado da Organização *
4. Responsável pela Resposta *
5. Cargo do Responsável pela Resposta *

CyberSecurity Assessment – CIS CSF – Cybersecurity Controls

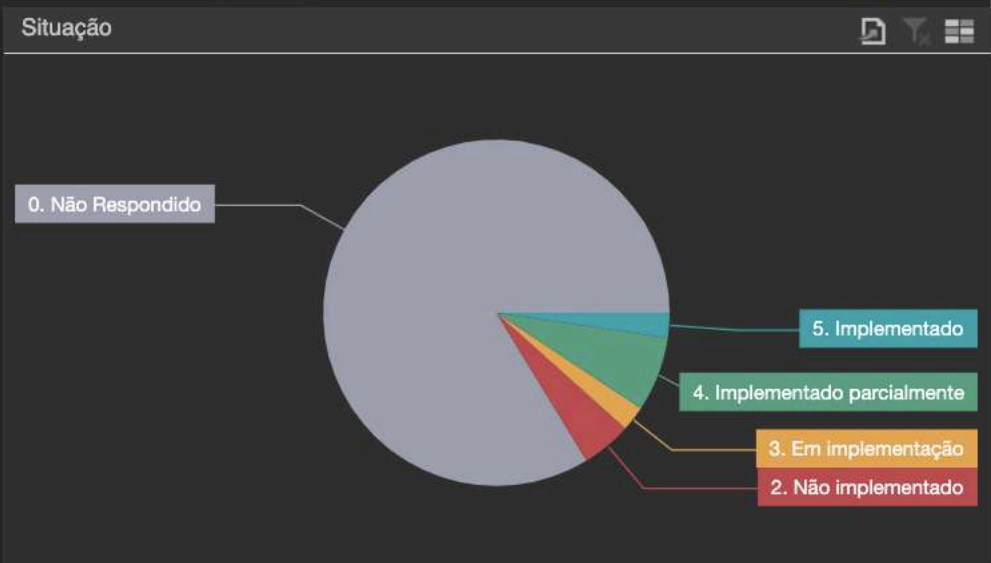


CIS Controls	Situação	Prob	Sever	Camada	G.I. CIS	Soluções Microsoft	Qtd
01.04. Um Inventário de Ativos de Hardware detalhado deve ser mantido pela organização.	5. Implementado	Alta	Alta	Basic	1.		1
01.06. Os Ativos de Hardware não autorizados identificados devem ser tratados pela organização.	4. Implementado parcialmente	Alta	Alta	Basic	1.		1
02.01. Um Inventário dos Softwares autorizados deve ser mantido pela organização.	0. Não Respondido	Alta	Alta	Basic	1.		
02.02. Todos os Softwares autorizados pela organização devem ser suportados por seus fornecedores.	4. Implementado parcialmente	Baixa	Média	Basic	1.		
02.06. Os Softwares não autorizados devem ser tratados pela organização.	0. Não Respondido	Alta	Alta	Basic	1.		
03.04. Ferramentas de gerenciamento de "patches" automatizadas devem ser implementadas pela organização para os sistemas operacionais.	4. Implementado parcialmente	Alta	Alta	Basic	1.		
03.05. Ferramentas de gerenciamento de "patches" automatizadas devem ser implementadas pela organização para os aplicativos de terceiros.	2. Não implementado	Alta	Alta	Basic	1.		
04.02. Senhas fortes devem ser utilizadas nos sistemas da organização.	3. Em implementação	Média	Alta	Basic	1.	Azure AD Conditional Access - gestão de identidade e acesso na nuvem, Azure AD Identity Protection - automatiza a detecção e remediação de riscos de identidade baseados em inteligência artificial, Azure AD Multi-Factor Authentication - gestão de identidade e acesso na nuvem, Azure AD Self-Service Password Reset (SSPR) - permite que os usuários redefinam suas senhas sem entrar em contato com a equipe de TI, Microsoft Intune (MDM & MAM) - gestão de estações de trabalho, dispositivos móveis e ap...	1
04.03. As contas administrativas devem ser dedicadas ao propósito de administração.	0. Não Respondido	Baixa	Alta	Basic	1.		
05.01. Configurações de segurança devem ser estabelecidas para sistemas operacionais e aplicativos da organização.	0. Não Respondido	Alta	Alta	Basic	1.		
06.02. O "log" de auditoria local deve ser habilitado em todos os sistemas e dispositivos de rede da organização.	0. Não Respondido	Alta	Alta	Basic	1.		
07.01 Apenas os navegadores web e clientes de e-mail totalmente suportados devem ser autorizados na organização.	0. Não Respondido	Média	Média	Found...	1.		
07.07 Serviços de filtragem DNS para ajudar a bloquear o acesso a domínios maliciosos conhecidos devem ser utilizados.	0. Não Respondido	Alta	Média	Found...	1.		
08.02 Os softwares "anti-malware" da organização devem ser atualizados regularmente quanto ao seu mecanismo de verificação e seu banco de dados de assinaturas.	0. Não Respondido	Alta	Média	Found...	1.		
08.04 Os dispositivos devem ser configurados de forma que eles realizem automaticamente uma verificação "anti-malware" nas mídias removíveis quando inseridas ou conectadas.	0. Não Respondido	Alta	Alta	Found...	1.	Azure AD Conditional Access - gestão de identidade e acesso na nuvem, Azure AD Identity Protection - automatiza a detecção e remediação de riscos de identidade baseados em inteligência artificial, Azure AD Privileged Identity Management - permite	1

Controle CIS v 7_1	Qtd
CIS CSC 01: Inventário e Controle de Ativos de Hardware	2
CIS CSC 02: Inventário e Controle de Ativos de Software	3
CIS CSC 03: Gerenciamento Contínuo de Vulnerabilidades	2
CIS CSC 04: Uso Controlado de Privilégios Administrativos	2
CIS CSC 05: Configurações de Segurança Para Hardware e Software em Dispositivos Móveis, Laptops, Estações de Trabalho e Servidores	1
CIS CSC 06: Manutenção, Monitoramento e Análise dos Registros de Auditoria	1
CIS CSC 07: Proteções para Navegador Web e E-mail	2
CIS CSC 08: Defesas Contra Malware	3
CIS CSC 09: Limitação e Controle de Portas de Rede	1
CIS CSC 10: Capacidade de Recuperação de Dados	4
CIS CSC 11: Configurações de Segurança para Dispositivos de Rede	1
CIS CSC 12: Defesa de Perímetros	2
CIS CSC 13: Proteção de Dados	3

Grupos de Implementação	Q.
1. Organização com recursos e conhecimento de segurança cibernética disponíveis limitados para implementar sub-controles	4.
2. Organização com recursos e conhecimento de segurança cibernética disponíveis moderados para implementar sub-controles	9.
3. Organização madura com recursos significantes e experiência em segurança cibernética disponíveis para implementar sub-controles	3.

Camada	Qtd
Basic	11
Foundational	22
Organizational	10



CIS Controls	Situação	Prob	Sever	Camada	G.I. C	Assunto LGPD	Qtd
01.04. Um Inventário de Ativos de Hardware detalhado deve ser mantido pela organização.	5. Implementado	Alta	Alta	Basic	1.	(Art 46 - 49) Segurança da Informação	32
01.06. Os Ativos de Hardware não autorizados identificados devem ser tratados pela organização.	4. Implementado parcialme...	Alta	Alta	Basic	1.	(Art 48) Gestão de Incidentes e Monitoramento	4
02.01. Um Inventário dos Softwares autorizados deve ser mantido pela organização.	5. Implementado	Alta	Alta	Basic	1.	(Art 50) Boas Práticas e Governança	7
02.02. Todos os Softwares autorizados pela organização devem ser suportados por seus fornecedores.	3. Em implementação	Baix					
02.06. Os Softwares não autorizados devem ser tratados pela organização.	5. Implementado	Alta	Alta	Basic	1.		
03.04. Ferramentas de gerenciamento de "patches" automatizadas devem ser implementadas pela organização para os sistemas operacionais.	5. Implementado	Alta	Alta	Basic	1.		
03.05. Ferramentas de gerenciamento de "patches" automatizadas devem ser implementadas pela organização para os aplicativos de tercelros.	5. Implementado	Alta	Alta	Basic	1.		
04.02. Senhas fortes devem ser utilizadas nos sistemas da organização.	4. Implementado parcialme...	Alta	Alta	Basic	1.		
04.03. As contas administrativas devem ser dedicadas ao propósito de administração.	2. Não implementado	Baixa	Alta	Basic	1.		
05.01. Configurações de segurança devem ser estabelecidas para sistemas operacionais e aplicativos da organização.	4. Implementado parcialme...	Alta	Alta	Basic	1.		
06.02. O "log" de auditoria local deve ser habilitado em todos os sistemas e dispositivos de rede da organização.	5. Implementado	Alta	Alta	Basic	1.		
07.01 Apenas os navegadores web e clientes de e-mail totalmente suportados devem ser autorizados na organização.	4. Implementado parcialme...	Média	Média	Foundational	1.		
07.07 Serviços de filtragem DNS para ajudar a bloquear o acesso a domínios maliciosos conhecidos devem ser utilizados.	5. Implementado	Alta	Média	Foundational	1.		
08.02 Os softwares "anti-malware" da organização devem ser atualizados regularmente quanto ao seu mecanismo de verificação e seu banco de dados de assinatur...	5. Implementado	Alta	Média	Foundational	1.		
08.04 Os dispositivos devem ser configurados de forma que eles realizem automaticamente uma verificação "anti-malware" nas mídias removíveis quando inseridas ...	5. Implementado	Alta	Alta	Foundational	1.		
08.05 Os dispositivos devem ser configurados de forma que eles não executem automaticamente o conteúdo armazenado nas mídias removíveis quando inseridas o...	5. Implementado	Alta	Alta	Foundational	1.		
09.04 "Firewalls" baseados em "host" ou ferramentas de filtragem de portas devem ser instalados nos sistemas dos usuários finais, com uma regra "default" para n...	5. Implementado	Alta	Alta	Foundational	1.		
10.01 Um " backup" automatizado deve ser realizado para cada sistema ao menos semanalmente e mais frequentemente em sistemas quem armazenam informaçãoe...	5. Implementado	Alta	Alta	Foundational	1.		
10.02 Todos os principais sistemas da organização devem possuir "backup" completo.	5. Implementado	Alta	Alta	Foundational	1.		
10.04 Os "backups" devem ser protegidos, através de segurança física ou criptografia, quando estiverem armazenados localmente, assim como quando forem movi...	4. Implementado parcialme...	Alta	Alta	Foundational	1.		
10.05 Todos os "backups" devem ter pelo menos um destino "offline".	4. Implementado parcialme...	Baixa	Alta	Foundational	1.		
11.04 A última versão estável de qualquer atualização de segurança deve ser instalada em todos os dispositivos de rede.	4. Implementado parcialme...	Média	Alta	Foundational	1.		
12.01 Um inventário atualizado de todos os perímetros da rede da organização deve ser mantido.	4. Implementado parcialme...	Alta	Alta	Foundational	1.		
12.04 Comunicações através de portas TCP, UDP, ou de aplicativos não autorizados, devem ser bloqueadas.	5. Implementado	Alta	Alta	Foundational	1.		
13.01 Um inventário de todas as informações confidenciais armazenadas, processadas ou transmitidas pelos sistemas da organização deve ser mantido.	2. Não implementado	Muito Alta	Muito Alta	Foundational	1.		
13.02 Dados ou sistemas confidenciais que não sejam acessados regularmente devem ser removidos pela organização.	2. Não implementado	Média	Alta	Foundational	1.		
13.06 Um software aprovado para criptografia de disco rígido deve ser implementado em dispositivos móveis que possuam dados confidenciais.	4. Implementado parcialme...	Média	Alta	Foundational	1.		
14.06 As informações devem ser protegidas através de listas de controle de acesso.	5. Implementado	Média	Alta	Foundational	1.		
15.07 A criptografia AES deve ser usada para proteger todo o tráfego sem fio da organização.	5. Implementado	Alta	Alta	Foundational	1.		
15.10 Redes locais virtuais (VLANs) específicas devem ser criadas para dispositivos pessoais ou outros dispositivos não confiáveis.	5. Implementado	Alta	Alta	Foundational	1.		
16.08 Todas as contas de usuário devem ser revisadas periodicamente, desabilitando aquelas que não sejam associadas a nenhum processo de negócio ou propriet...	5. Implementado	Baixa	Alta	Foundational	1.		
16.09 As contas de usuário inativas devem ser desabilitadas automaticamente.	1. Em avaliação	Média	Alta	Foundational	1.		
16.11 As sessões das estações de trabalho devem ser bloqueadas após um período de inatividade.	5. Implementado	Alta	Alta	Foundational	1.		
17.03 Um programa de conscientização em segurança da informação deve ser implementado pela organização.	5. Implementado	Média	Alta	Organizational	1.		
17.05 A força de trabalho da organização deve ser treinada em relação à autenticação segura.	5. Implementado	Alta	Alta	Organizational	1.		
17.06 A força de trabalho da organização deve ser treinada em relação à identificação de ataques de engenharia social	5. Implementado	Média	Alta	Organizational	1.		

Grupos de Implementação	Qtd	Camada	Qtd
1. Organização com recursos e conhecimento de segurança cibernética disponíveis limitados para implementar sub-controles	43	Basic	11
2. Organização com recursos e conhecimento de segurança cibernética disponíveis moderados para implementar sub-controles	94	Foundational	22
3. Organização madura com recursos significantes e experiência em segurança cibernética disponíveis para implementar sub-controles	34	Organizational	10

Controle CIS v 7_1	Qtd
CIS CSC 17: Avaliações de Competências em Segurança ...	6
CIS CSC 19: Gerenciamento e Resposta a Incidentes	4
CIS CSC 10: Capacidade de Recuperação de Dados	4
CIS CSC 16: Controle e Monitoramento de Contas	3
CIS CSC 13: Proteção de Dados	3
CIS CSC 08: Defesas Contra Malware	3
CIS CSC 02: Inventário e Controle de Ativos de Software	3
CIS CSC 15: Controle de Acesso Sem Fio	2
CIS CSC 12: Defesa de Perímetros	2
CIS CSC 07: Proteções para Navegador Web e E-mail	2

NIST CSF - CyberSecurity Framework	Qtd
DE.AE-3 - Event data are collected and correlated from...	1
DE.CM-1 - The network is monitored to detect potentia...	1
DE.CM-4 - Malicious code is detected	2
DE.CM-7 - O monitoramento de colaboradores não aut...	2
DE.DP-1 - Roles and responsibilities for detection are ...	1
DE.DP-4 - Event detection information is communicated	1
ID.AM-1 - Dispositivos físicos e sistemas dentro da org...	1
ID.AM-4 - External information systems are catalogued	1
ID.AM-5 - Resources (e.g., hardware, devices, data, tim...	1
ID.AM-6 - Cybersecurity roles and responsibilities for L...	1

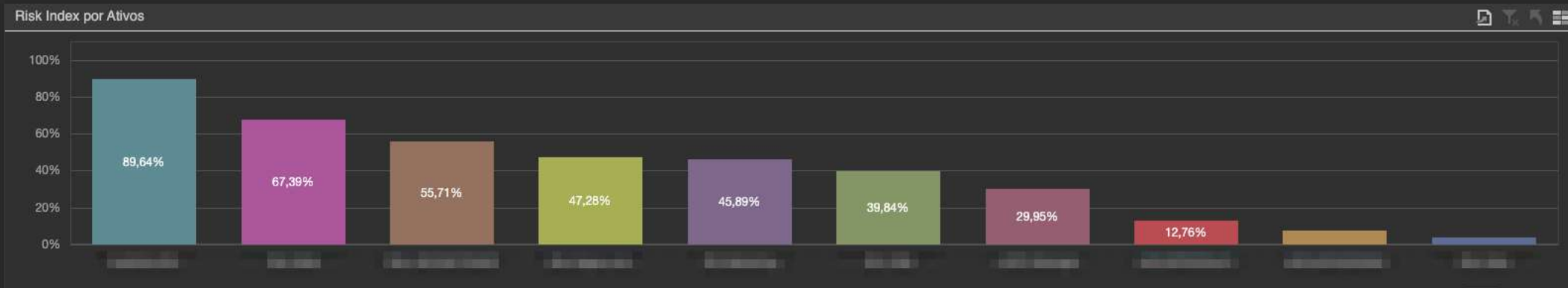
Soluções Microsoft	Qtd
Microsoft Intune (MDM & MAM) - gestão de estações de de...	25
Azure AD Conditional Access - gestão de identidade e a...	12
Microsoft Cloud App Security - visibilidade, controle e pr...	11
Microsoft Defender ATP - ajuda as redes corporativas a l...	9
Microsoft Sharepoint Online - armazena, organiza, comp...	7
Office 365 Advanced Threat Protection - detecta, investi...	6
Microsoft Yammer - rede social corporativa para comu...	6

Situação	Qtd
1. Em avaliação	5
2. Não implementado	23
3. Em implementação	3
4. Implementado parcialmente	24
5. Implementado	90

Filtro por Sistemas
(Todos)

Filtro por KBs
(Todos)

Filtro por Situação
(Todos)

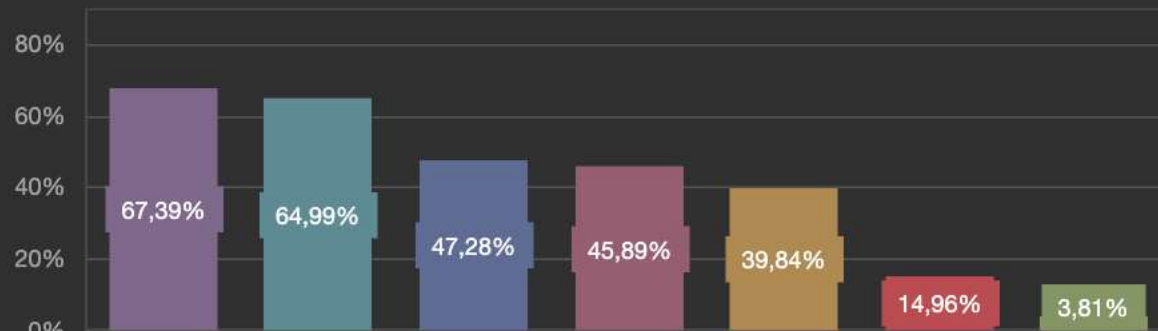


PSR	Ativo	Controle	Situação
60		O "login" de administração do servidor de banco de dados deve possuir uma senha de difícil dedução.	Implementado
60		O software antivírus em uso no Sistema Operacional deve ser atualizado com a base de assinaturas de vírus mais recente.	Implementado
60		Um software antivírus compatível com o Sistema Operacional deve ser instalado.	Implementado
60		O software antivírus em uso no Sistema Operacional deve ser atualizado com a base de assinaturas de vírus mais recente.	Implementado
60		Um software antivírus compatível com o Sistema Operacional deve ser instalado.	Implementado
60		O "login" de administração do servidor de banco de dados deve possuir uma senha de difícil dedução.	Implementado
60		O software antivírus em uso no Sistema Operacional deve ser atualizado com a base de assinaturas de vírus mais recente.	Implementado
60		Um software antivírus compatível com o Sistema Operacional deve ser instalado.	Implementado
48		A gestão de senhas de acesso ao sistema deve contemplar requisitos de segurança, tais como tamanho mínimo, complexidade, histórico de senhas e expiração.	Não Implementado
48		O acesso ao sistema por fora do perímetro da organização deve ser protegido por mecanismos de tunelamento ou acesso condicional em nuvem.	Não Implementado
48		O sistema deve possuir contas específicas para tarefas administrativas.	Implementado
48		O sistema deve possuir cópias de segurança criptografadas dos dados pessoais.	Não Implementado
48		O sistema deve possuir log das tentativas de acesso com êxito e falha.	Não Implementado
48		O sistema deve possuir segregação de privilégios de acesso através de perfis e funções, definindo regras e restrições de acordo com as necessidades específicas dos usuários (modelo RBAC).	Implementado
48		O sistema deve possuir um responsável para proteção de dados pessoais.	Não Implementado
48		O sistema deve prover mecanismos para proteger os dados pessoais.	Não Implementado
48		O sistema deve ter um mecanismo de proteção contra tentativas de acesso mal sucedidas.	Não Implementado
48		A concessão de direitos de acesso aos objetos dos bancos de dados do servidor deve ser monitorada, obedecendo ao "princípio do menor privilégio".	Implementado
48		A designação de grupos de usuários deve obedecer ao "princípio do menor privilégio".	Implementado
48		A versão dos componentes de acesso ao banco de dados deve ser a mais atual disponível, considerada estável pelo fabricante.	Não Implementado
48		As atualizações de software liberados para o banco de dados devem ser instalados.	Implementado
48		As permissões do diretório que contém os arquivos binários do banco de dados devem ser configuradas de forma a evitar acessos indevidos.	Implementado
48		O banco de dados deve ser protegido de acessos indevidos por um Firewall.	Implementado
48		O parâmetro "Account lockout threshold" deve ser definido como "5" ou menos tentativas mal sucedidas.	Implementado
48		O parâmetro "Allow log on locally" deve ser configurado como "Administrators, Users".	Implementado
48		O parâmetro "Minimum Password Length" deve ser configurado com um valor igual ou superior "14".	Não Aplicável
48		O parâmetro "Store passwords using reversible encryption" deve ser configurado como "Disabled".	Implementado
48		O parâmetro "Turn off Automatic Download and Install of updates" deve ser configurado como "Disabled".	Não Aplicável
48		O parâmetro "Windows Firewall: Domain: Firewall state" deve ser configurado como "On (recommended)".	Implementado
48		O parâmetro "Windows Firewall: Domain: Inbound connections" deve ser configurado como "Block (default)".	Implementado

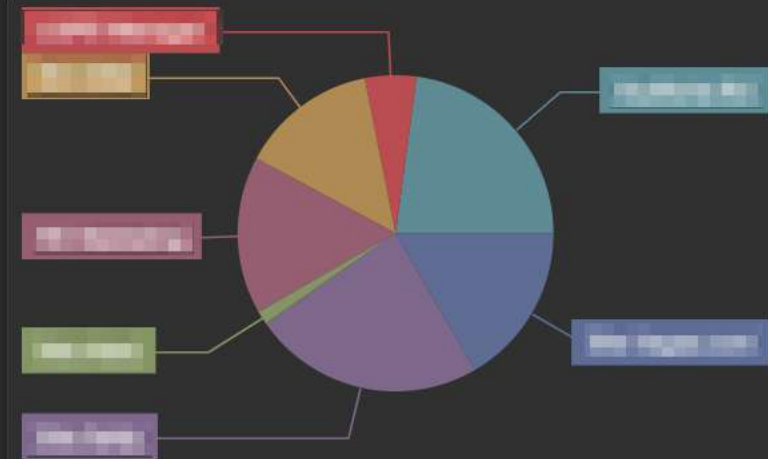
Risk Index Global



Risk Index por Sistemas



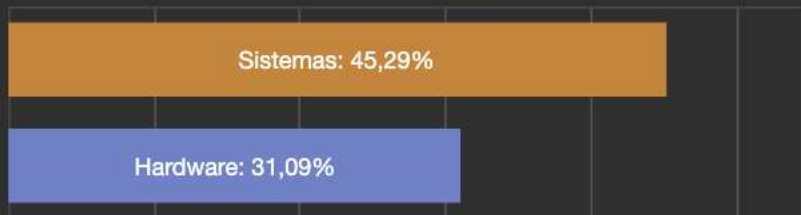
Percentual de Risco para a Organização



Risk Index por Tipificação



Hardware Sistemas



Nome do Ativo

PSR Identificado

PSR Aplicável

PSR Não Aplicável

Risk Index

Nome do Ativo	PSR Identificado	PSR Aplicável	PSR Não Aplicável	Risk Index
[Redacted]	1038	1158	27	89,64%
[Redacted]	279	414	771	67,39%
[Redacted]	1713	3075	48	55,71%
[Redacted]	339	717	468	47,28%
[Redacted]	519	1131	54	45,89%
[Redacted]	453	1137	66	39,84%
[Redacted]	336	1122	63	29,95%
[Redacted]	243	1905	294	12,76%
[Redacted]	135	1746	246	7,73%
[Redacted]	36	945	240	3,81%

Situação dos Controles

[Clique aqui para acessar a listagem de controles \(por situação\)](#)

Base de Conhecimento (KB)

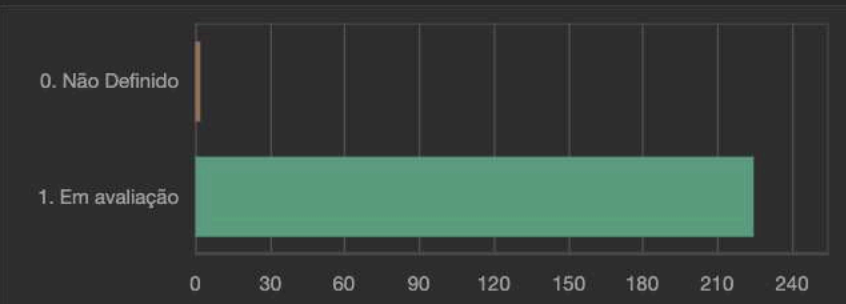
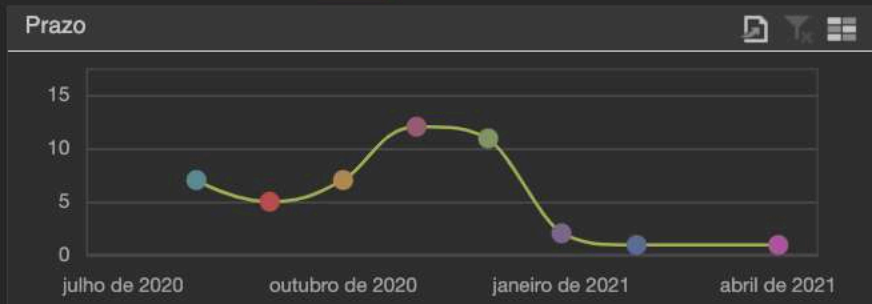
Risk Index

Base de Conhecimento (KB)	Risk Index
Gest Ident, Ctrl de Acesso e Prot Dados Pess em Sist	45,29%
Servidor Web	40,13%
Servidor de Banco de Dados	29,73%
Windows	26,11%

Atividade	Ativo	Prioridade	Assunto	Qtd	Escopo da aplicação	Qtd
Orientar a área quanto ao tratamento de dados pessoais de crianças e adolescentes	Atividade-guia	16,0	(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais	4	0. Não respondido	2
Orientar a área quanto ao tratamento de dados pessoais de crianças e adolescentes	Atividade-guia (todas as áreas que tratem dados pessoais de crianças e adolescentes)	16,0	(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais, (Art 39) Operador, (Art 50) Boas Práticas e Governança, Definição de Termos e Princípios	1	1. Lei 13.709	14
Avaliar e justificar a base legal (hipótese de tratamento) dos sistemas e suportes de dados	Atividade-guia (todos os sistemas e suportes de dados que tratem dados pessoais)	16,0	(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais, (Art 46 .. 49) Segurança da Informação, (Art 50) Boas Práticas e Governança	1	2. Registro Corporativo	51
Avaliar e justificar a base legal (hipótese de tratamento) dos sistema/repositório	Atividade-guia	16,0	(Art 07) Base Legal, Hipóteses de Tratamento	2	3. Negócio	13
Avaliar e implementar cláusulas contratuais de tratamento de dados pessoais dos sistemas e repositórios sob responsabilidade dos operadores e dos fornecedores	Atividade-guia	16,0	(Art 08) Consentimento	2	4. Sistemas e Suportes de Dados	145
Avaliar com a área a real necessidade de utilizar dados pessoais sensíveis e a possibilidade de minimizar	Atividade-guia	16,0	(Art 09, 17 .. 22) Direito do Titular	3	5. Partes Relacionadas	2
Avaliar com a área a real necessidade de utilizar dados pessoais sensíveis e a possibilidade de minimizar	Atividade-guia (todas as áreas que realizem o tratamento de dados pessoais sensíveis)	16,0	(Art 11) Dados Sensíveis	6	Responsável	Qtd
Avaliar com a área a real necessidade de utilizar dados pessoais de crianças e adolescentes e a possibilidade de minimizar	Atividade-guia	16,0	(Art 12) Anonimização	1	SEGTI	115
Avaliar com a área a real necessidade de utilizar dados pessoais de crianças e	Atividade-guia (todas as áreas que	16,0	(Art 14) Crianças e Adolescentes	7	Sistemas LGPD	20
			(Art 33 .. 36) Transferência	1	Seg Cibernética LGPD	14
					Jurídico LGPD	12
					Governança de TI LGPD	12
					Equipe Modulo LGPD	11
				

Âmbito	Qtd	Ativo	Qtd	Tipo da Atividade	Qtd	Facilidade	Qtd	Urgência da Atividade	Qtd	Importância da Atividade	Qtd
Sistemas e suportes de dados que tratam dados pessoais	123	Atividade-guia	66	Identificação de conjunto de dados e seu ciclo de vida	118	5. Pode ser realizada pela equip...	4	5. Precisa ser realizado imediata...	6	5. Ação essencial para o atendime...	39
Preparação do Plano de Ação para atendimento à LGPD	17	Atividade-guia (Corporativo)	27	Preparação do Plano de Ação	16	4. Pode ser realizada com pequ...	13	4. Precisa ser realizado o quanto...	39	4. Atendimento a requisito relevant...	148
Políticas, procedimentos, leis e regulamentos	12	SGIP	2	Adequação de sistemas	14	3. Pode ser realizada com frequ...	174	3. Precisa ser realizado o quanto...	103	3. Melhorias de processos não resolu...	32
Gestão do tratamento de dados pessoais	12	SGARQ	2	Segurança cibernética / Demonstrar Segurança	12	2. Exige recursos não previstos...	32	2. Pode ser realizado até 16 de a...	23	2. Melhorias de processo aprovellan...	1
Sistemas e suportes de dados específicos	10	Zoom	1	Adequação e criação de políticas	9	1. Complexidade alta para a qu...	3	1. Pode ser realizado após 16 de...	5	0. Não definido	1
Sites publicados externamente e internamente	8	WhatsApp	1	Adequação de Sites	6	0. Não definido	1	0. Não definido	1		
Infraestrutura tecnológica (dispositivos móveis, computadores do usuário, servidores, nuvem)	8										
Sistemas e suportes de dados do usuário	6										
Áreas que tratam dados	6										

Escopo da Atividade	Qtd
Sistemas e Suportes de Dados	143
Corporativo (toda a organização)	23
Preparação do Plano de Ação para atendimento à LGPD	19
Numero de Atividades	227





Ação para Implementação							
Ação Implementação	Sem	Escopo da aplicação	Predecessores	Tipo de Ação	Escopo da Atividade	Qtd	Prior
1.10. Política de Proteção de Dados e Privacidade	S01	0. Corporativo	0. Sem Predecessor	Template	Preparação do Plano de Ação para atendimento à LGPD	1	20,0
1.20. Encarregado pelo Tratamento de Dados Pessoais	S01	0. Corporativo	0. Sem Predecessor	Template	Encarregado de Tratamento de Dados Pessoais	1	17,5
1.30. Workshop Áreas, Sistemas e Partes Relacionadas	S01	2. Registro Corporativo	0. Sem Predecessor	Workshop com coleta de informações	Corporativo (toda a organização)	2	37,0
2.10.100. Cartilha de Proteção de Dados	S03	0. Corporativo	1.10. Política de Proteção de Dados e Privacidade	Template	Corporativo (toda a organização)	1	15,7
2.20.100. Atendimento à solicitação de titular	S02	0. Corporativo	1.10. Política de Proteção de Dados e Privacidade, 1.20. Encarregado pelo Tratamento de Dados Pess...	Implementação em Software	Sistemas e Suportes de Dados	1	20,0
2.20.200. Gestão de Incidentes	S03	0. Corporativo	1.10. Política de Proteção de Dados e Privacidade, 1.20. Encarregado pelo Tratamento de Dados Pess...	Implementação em Software	Corporativo (toda a organização)	1	18,5
2.20.300. Publicações complementares	S06	0. Corporativo	1.10. Política de Proteção de Dados e Privacidade, 1.20. Encarregado pelo Tratamento de Dados Pess...	Reunião de orientação	Corporativo (toda a organização)	1	14,3
2.20.400. Workshop Alta Administração	S03	0. Corporativo	1.20. Encarregado pelo Tratamento de Dados Pessoais	Workshop com coleta de informações	Áreas (departamentos, processos de negócios, ...)	1	15,7
2.30.100. Workshop Áreas	S02	3. Áreas de Negócio	1.30. Workshop Áreas, Sistemas e Partes Relacionadas	Workshop com coleta de informações	Áreas (departamentos, processos de negócios, ...)	48	578,3
2.30.200. Workshop Sistemas	S03	4. Sistemas e Suportes de Dados	1.30. Workshop Áreas, Sistemas e Partes Relacionadas	Workshop com coleta de informações	Infraestrutura de TI	1	17,5
2.30.200. Workshop Sistemas	S03	4. Sistemas e Suportes de Dados	1.30. Workshop Áreas, Sistemas e Partes Relacionadas	Workshop com coleta de informações	Sistemas e Suportes de Dados	14	280,0
2.30.300. Cláusulas para partes relacionadas	S02	0. Corporativo	1.30. Workshop Áreas, Sistemas e Partes Relacionadas	Template	Terceiros (clientes, fornecedores, ...)	1	14,9
3.10.100.1000. Conscientização LGPD	S04	0. Corporativo	1.10. Política de Proteção de Dados e Privacidade, 1.20. Encarregado pelo Tratamento de Dados Pess...	Workshop com coleta de informações	Corporativo (toda a organização)	1	16,5
3.20.200.1000. Privacy by design	S05	0. Corporativo	2.20.200. Gestão de Incidentes, 2.30.200. Workshop Sistemas	Implementação em Software	Corporativo (toda a organização)	1	16,1
3.20.300.1000. Revisão de políticas corporativas	S04	0. Corporativo	2.20.300. Publicações complementares	Reunião de orientação	Corporativo (toda a organização)	1	17,3
3.20.300.2000. Áreas de controle	S06	0. Corporativo	2.20.300. Publicações complementares	Template	Áreas (departamentos, processos de negócios, ...)	1	16,1
3.30.100.1000. Benefícios para funcionários	S04	0. Corporativo	2.30.100. Workshop Áreas, 2.30.200. Workshop Sistemas	Reunião de orientação	Terceiros (clientes, fornecedores, ...)	1	14,3
3.30.100.2000. Workshop Transferência Internacional	S07	3. Áreas de Negócio	2.30.100. Workshop Áreas	Workshop com coleta de informações	Sistemas e Suportes de Dados	2	12,3
3.30.100.2000. Workshop Transferência Internacional	S07	3. Áreas de Negócio	2.30.100. Workshop Áreas, 2.30.200. Workshop Sistemas	Workshop com coleta de informações	Sistemas e Suportes de Dados	1	15,5
3.30.100.3000. Redes Sociais	S04	3. Áreas de Negócio	2.30.100. Workshop Áreas	Template	Redes Sociais e Serviços de Nuvem	1	14,9
3.30.200.1000. Ajuste em Sistemas - Sensíveis	S05	4. Sistemas e Suportes de Dados	2.30.100. Workshop Áreas	Projeto	Sistemas e Suportes de Dados	5	92,5
3.30.200.1000. Ajuste em Sistemas - Sensíveis	S05	4. Sistemas e Suportes de Dados	2.30.100. Workshop Áreas, 2.30.200. Workshop Sistemas	Projeto	Sistemas e Suportes de Dados	1	18,5
3.30.200.2000. Ajuste em Sistemas - Crianças e Adolescentes	S06	4. Sistemas e Suportes de Dados	2.30.100. Workshop Áreas	Projeto	Áreas (departamentos, processos de negócios, ...)	17	348,5
3.30.200.2000. Ajuste em Sistemas - Crianças e Adolescentes	S06	4. Sistemas e Suportes de Dados	2.30.100. Workshop Áreas, 2.30.200. Workshop Sistemas	Projeto	Áreas (departamentos, processos de negócios, ...)	1	20,5
3.30.200.3000. Gestão de Inventários	S05	0. Corporativo	2.30.100. Workshop Áreas, 2.30.200. Workshop Sistemas	Implementação em Software	Infraestrutura de TI	1	14,9
3.30.200.4000. Segurança cibernética	S05	0. Corporativo	2.30.100. Workshop Áreas, 2.30.200. Workshop Sistemas	Projeto	Infraestrutura de TI	1	17,0
3.30.200.5000. Anonimização	S07	0. Corporativo	2.30.200. Workshop Sistemas	Projeto	Sistemas e Suportes de Dados	1	16,1
3.30.200.6000. Ajustes em Sites	S04	3. Áreas de Negócio	1.10. Política de Proteção de Dados e Privacidade	Projeto	Sistemas e Suportes de Dados	7	36,7

Ação para Implementação			
Tipo de Ação	Qtd	Pr...	M...
Implementação em Software	6	10...	17,3
Projeto	43	70...	16,3
Reunião de orientação	13	15...	12,1
Template	16	21...	13,7
Workshop com coleta de informações	70	97...	13,9

Responsável	Qtd	Prior Total	Prior Média
Auditoria LGPD	1	16,1	16,1
Comunicação e Marketing LGPD	1	14,9	14,9
Country Manager SP	6	61,3	10,2
Diretor Serviços I	11	106,5	9,7
Encarregado/DPO LGPD	16	280,7	17,5
Governança de TI LGPD	3	46,5	15,5
Infra TI LGPD	1	15,2	15,2
Jurídico LGPD	6	102,2	17,0
Líder Adm & Fin	10	151,5	15,2
Líder Comunicação	9	73,9	8,2

Situação da Atividade	Q..	P..	P...
0. Não Definido	3	2...	9,3
1. Em avaliação	1...	2...	1...

Assunto LGPD	Qtd	Prior Total	Prior Média
(Art 11) Dados Sensíveis	21	414,5	19,7
(Art 14) Crianças e Adolescentes	20	406,0	20,3
(Art 46 .. 49) Segurança da Informação	24	323,0	13,5
	44	316,3	7,2
(Art 07) Base Legal, Hipóteses de Tratamento	13	260,0	20,0
(Art 50) Boas Práticas e Governança	11	187,9	17,1
(Art 38) Relatório de Impacto (DPIA), (Art 50) Boas Práticas e Governança	2	34,0	17,0
(Art 42 .. 45, 52 .. 54) Responsabilidade e Sanções	2	30,0	15,0
(Art 12) Anonimização, (Art 46 .. 49) Segurança da Informação	2	29,5	14,8

Semana da Implementação	Qtd	Prior Total	Prior Média
S01	4	74,5	18,6
S02	50	613,2	12,3
S03	18	347,4	19,3
S04	28	280,1	10,0
S05	11	192,1	17,5
S06	28	525,6	18,8
S07	8	106,8	13,3
S08	1	15,2	15,2



Ação para Implementação									
	S01	S02	S03	S04	S05	S06	S07	S08	Total geral
1.10. Política de Proteção de Dados e Privacidade	20								20
1.20. Encarregado pelo Tratamento de Dados Pessoais	18								18
1.30. Workshop Áreas, Sistemas e Partes Relacionadas	37								37
2.10.100. Cartilha de Proteção de Dados			16						16
2.20.100. Atendimento à solicitação de titular		20							20
2.20.200. Gestão de Incidentes			19						19
2.20.300. Publicações complementares						14			14
2.20.400. Workshop Alta Administração			16						16
2.30.100. Workshop Áreas		578							578
2.30.200. Workshop Sistemas			298						298
2.30.300. Cláusulas para partes relacionadas		15							15
3.10.100.1000. Conscientização LGPD				17					17
3.20.200.1000. Privacy by design					16				16
3.20.300.1000. Revisão de políticas				17					17

Ação para Implementação			
Tipo de Ação	Qtd	Prior	Média
Implementação em Software	6	103,5	17,3
Projeto	43	702,1	16,3
Reunião de orientação	13	157,3	12,1
Template	16	219,3	13,7
Workshop com coleta de informações	70	972,7	13,9

Situação da Atividade	Qtd	Prior Total	Prior Média
0. Não Definido	3	27,8	9,3
1. Em avaliação	145	2127,1	14,7

Qtd Atividades	148
Total Atividades	148

Assunto LGPD	Qtd	Prior Total	Prior Média
(Art 11) Dados Sensíveis	21	414,5	19,7
(Art 14) Crianças e Adolescentes	20	406,0	20,3
(Art 46 .. 49) Segurança da Informação	24	323,0	13,5
	44	316,3	7,2
(Art 07) Base Legal, Hipóteses de Tratamento	13	260,0	20,0
(Art 50) Boas Práticas e Governança	11	187,9	17,1
(Art 20) Políticas de Privacidade (PPV)	6	84,0	14,0

Assunto LGPD	Qtd	Prior Total	Prior Média
S01	4	74,5	18,6
S02	50	613,2	12,3
S03	18	347,4	19,3
S04	28	280,1	10,0
S05	11	192,1	17,5
S06	28	525,6	18,8
S07	8	106,8	13,3
S08	1	15,2	15,2



Projeto em Planilha



Automatização

CIS Controls®
Segurança Cibernética

Registro Corporativo



Macro-atividades



Gestão Contínua

Lei 13.709 LGPD

Revisão de Documentos

Consistência

Plano de Ação

- Templates
- Gestão de Incidentes
- Direito do Titular
- Privacy by Design
- Cockpit do DPO
- Relatório de Impacto (DPIA)
- Segurança Cibernética
- APIs: Registro, Cadastro de Dados Pessoais, Consentimento

Pessoas

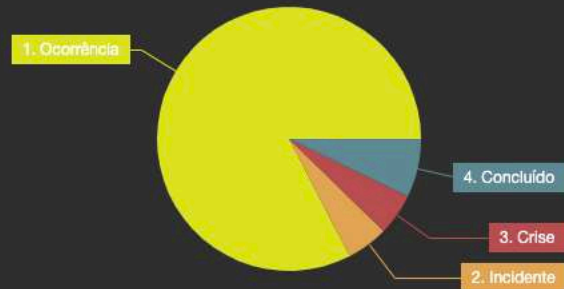
Áreas

Implementação

Partes Relacionadas

Sistemas

Classificação	Título	Tipo	Origem	Prior	Responsável	Prazo		Responsável	Qtd	Prior
1. Ocorrência	Ana Liza	Direito do titular	Portal do Titular	16	RH LGPD	12/11/2020		RH LGPD	11	118
1. Ocorrência	Carla Pires	Direito do titular	Portal do Titular	12	RH LGPD	17/07/2020	●	Jurídico LGPD	3	31
1. Ocorrência	Convíte para apresentação em evento - Exemplo	Ações de mercado e marketing	Mercado e eventos	2	Encarregado/DPO LGPD	14/01/2021	●	Comunicação e Marketing LGPD	3	30
1. Ocorrência	Criação de novo departamento	Gestão de mudanças, privacy by design, privacy by default	Área fim	6	Área-fim LGPD	11/09/2020	🚩	Área-fim LGPD	4	30
1. Ocorrência	Criação de novo Processo P001	Gestão de mudanças, privacy by design, privacy by default	Área fim	6	Área-fim LGPD	04/11/2020		Sistemas LGPD	2	18
1. Ocorrência	Jair Andando	Direito do titular	Portal do Titular	16	RH LGPD	08/10/2020		Encarregado/DPO LGPD	2	18
1. Ocorrência	João Ponês	Direito do titular	Ouvidoria	7	RH LGPD	15/09/2020		TIC LGPD	1	15
1. Ocorrência	Joaquim Campineiro	Direito do titular	Portal do Titular	4	RH LGPD	25/09/2020		Seg Cibernética LGPD	1	15
1. Ocorrência	Joaquim José da Silva	Direito do titular	Canal Fale Conosco - Site	12	RH LGPD	17/07/2020	●	Marcelo Lopes	1	9
1. Ocorrência	Joaquim Manoel	Direito do titular	Ação Judicial	9	RH LGPD	03/09/2020	🚩	Infra TI LGPD	1	9
1. Ocorrência	Juscelino Oliveira	Direito do titular	Portal do Titular	12	RH LGPD	17/09/2020				
1. Ocorrência	Neymar Neto	Direito do titular	Auditoria, Ouvidoria, estrutura de controles	9	RH LGPD	09/10/2020				
1. Ocorrência	Notificação da ANPD a pedido de Titular - Exemplo	Notificação da ANPD	ANPD	16	Encarregado/DPO LGPD	23/07/2019	●			
1. Ocorrência	Nova campanha MKT001	Gestão de mudanças, privacy by design, privacy by default	TI - Tecnologia da Informação	12	Comunicação e Marketing LGPD	20/08/2020	●	Origem	Qtd	Prior
1. Ocorrência	Nova campanha MKT010	Gestão de mudanças, privacy by design, privacy by default	TI - Tecnologia da Informação	9	Comunicação e Marketing LGPD	02/10/2020		Portal do Titular	6	69
1. Ocorrência	Nova Filial	Gestão de mudanças, privacy by design, privacy by default	Área fim	9	Área-fim LGPD	18/05/2021	●	Área fim	7	64
1. Ocorrência	Novo armazenamento de processos judiciais	Gestão de mudanças, privacy by design, privacy by default	Jurídico	9	Jurídico LGPD	20/10/2020		Ouvidoria	3	28
1. Ocorrência	Novo ponto de venda	Gestão de mudanças, privacy by design, privacy by default	Área fim	9	Comunicação e Marketing LGPD	05/11/2020		SI - Segurança da Informação	2	24
1. Ocorrência	Novo Produto P001	Gestão de mudanças, privacy by design, privacy by default	Área fim	9	Área-fim LGPD	17/09/2020		TI - Tecnologia da Informação	2	21
1. Ocorrência	Novo serviço de diretório AD em nuvem	Gestão de mudanças, privacy by design, privacy by default	SI - Segurança da Informação	9	Infra TI LGPD	04/11/2020		ANPD	1	16
1. Ocorrência	Novo sistema ERPRH	Gestão de mudanças, privacy by design, privacy by default	Área fim	9	Sistemas LGPD	07/08/2020	●	Mídia Aberta	1	15
1. Ocorrência	Novo sistema Sys001	Gestão de mudanças, privacy by design, privacy by default	Ouvidoria	9	Sistemas LGPD	07/08/2020	●	Jurídico	2	15
1. Ocorrência	Registro no reclameaqui.com - Exemplo	Notícia na mídia / redes sociais	Área fim	16	Jurídico LGPD	23/07/2019	●	Canal Fale Conosco - Site	1	12
1. Ocorrência	Solicitação do Titular	Direito do titular	Jurídico	6	Jurídico LGPD	26/06/2020	●	SAC - Atendimento ao Consumidor	1	9
1. Ocorrência	Usuário solicitou retirada da base RH - Exemplo	Direito do titular	Portal do Titular	9	Marcelo Lopes	17/04/2020	●	Auditoria, Ouvidoria, estrutura de controles	1	9
4. Concluído	Arlindo Madureira	Direito do titular	SAC - Atendimento ao Consumidor	9	RH LGPD	28/10/2020		Ação Judicial	1	9
4. Concluído	Ivete Eva	Direito do titular	Ouvidoria	12	RH LGPD	08/10/2020		Mercado e eventos	1	2
3. Crise	Lista de dados pessoais divulgadas no Pastebin - Exemplo	Vazamento de informações	Mídia Aberta	15	TIC LGPD	09/07/2019	●			
2. Incidente	Gestor perdeu o seu token em local não sabido -	Cibernético	SI - Segurança da Informação	15	Seg Cibernética LGPD	19/07/2019	●			



Tipo	Qtd	Prior
Direito do titular	13	133
Gestão de mudanças, privacy by design, privacy by default	11	96
Notificação da ANPD	1	16
Notícia na mídia / redes sociais	1	16
Vazamento de informações	1	15
Cibernético	1	15
Ações de mercado e marketing	1	2



Filtrar itens

Dashboard Filtrar

Definir Conteúdos

Política Corporativa de Proteção de Dados Pessoais X Política Website de Proteção de Dados Pessoais X Termo Aditivo de Proteção de Dados Pessoais X Termo de Consentimento X Carta de Convivência com Contratos-Padrão de Terceiros X

Inira uma ou mais opções

Política Corporativa de Proteção de Dados Pessoais Política Website de Proteção de Dados Pessoais Termo Aditivo de Proteção de Dados Pessoais Termo de Consentimento

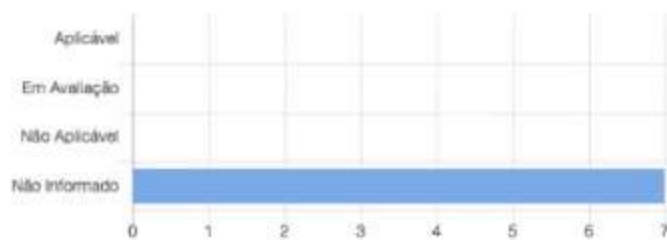
Carta de Convivência com Contratos-Padrão de Terceiros

Aplicar

Aplicabilidade



Aplicabilidade por conteúdo



	Geral	Política Corpor...	Política Websit...	Termo Aditivo ...	Termo de Cons...	Carta de Convi...
Aplicável	0%	0	0	0	0	0
Em Avaliação	0%	0	0	0	0	0
Não Aplicável	0%	0	0	0	0	0
Não informado	100%	4	2	0	1	0

Conteúdos

Política Corporativa de Proteção de Dados Pessoais

Política Corporativa de Proteção de Dados Pessoais (2 Tópicos)

6. DIREITOS DO TITULAR (1 Tópicos)

6.1. A XYZ zela para que o Titular do dado pessoal possa usufruir dos direitos assegurados pelos artigos 18 e 19 da LGPD, aos quais a presente Política se reporta, por remissão.

5. TRATAMENTO DE DADOS PESSOAIS (2 Tópicos)

5.3. Os dados pessoais coletados pela XYZ contam com consentimento dos visitantes do seu web site, obtidos na ocasião da primeira visita, por meio de procedimento de opt-in. Tal consentimento pode ser revogado pelo próprio interessado, a qualquer momento, mediante solicitação por e-mail dirigido a encarregado@XYZ.com.br. A XYZ procurará atualizar periodicamente a base de dados de consentimentos enviando e-mail para os endereços eletrônicos informados anteriormente pelos interessados.

5.5. Os dados pessoais tratados pela XYZ são: (1 Tópicos)

II - Mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante informação ou constatação de impropriedade respectiva ou face a solicitação de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de prazos de retenção de dados;

Política Website de Proteção de Dados Pessoais

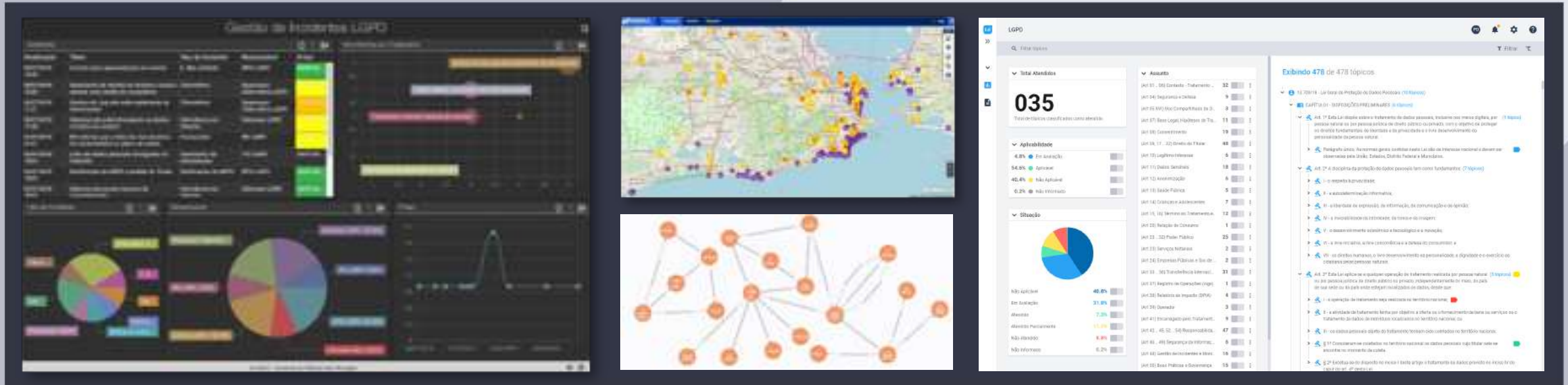
Política Website de Proteção de Dados Pessoais (1 Tópicos)

Seus direitos como titular de dados pessoais (1 Tópicos)

A LGPD lhe confere direitos que a XYZ zelará para que sejam observados, de acordo com os princípios gerais e regras também nela previstas.

Situação

Cockpit do DPO



Ocorrências e Incidentes		Direito do Titular		Prioridades							
Incidente	Prioridade da...	Nome	Prioridad...	Responsável	Qtd	Área	Sistemas	Partes	Atividades	Incidente	Total
Registro no reclameaqui.com - Exemplo	16,0	Jair Andando	16,0	Líder RH	18	9,6	41,9	4,6			56,2
Notificação da ANPD a pedido de Titular - Exemplo	16,0	Ana Liza	16,0	Projeto LGPD	15		0,0		49,4		49,4
Jair Andando	16,0	Juscelino Oliveira	12,0	Líder Adm & Fin	16	3,5	21,5	18,8			43,7
Ana Liza	16,0	Joaquim José da Silva	12,0	Líder NBSb	8	9,3		30,6			40,0
Lista de dados pessoais divulgadas no Pastebin - Exemplo	15,0	Ivete Eva	12,0	Líder Infraestrutura	16		39,2	0,0			39,2
Gestor perdeu o seu token em local não sabido - Exemplo	15,0	Carla Pires	12,0	Infra TI LGPD	7				28,8	9,0	37,8
Nova campanha MKT001	12,0	Usuário solicitou retirada da base RH - Exemplo	9,0	Encarregado/DPO LGPD	13			7,0	9,6	18,0	34,6
Juscelino Oliveira	12,0	Neymar Neto	9,0	Comunicação e Marketing LGPD	3					30,0	30,0
Joaquim José da Silva	12,0	Privacy by Design/Default		Equipe Cliente LGPD	4				28,8		28,8
Ivete Eva	12,0	Nova atividade	Priorida...	Líder RJN	5	3,3	19,3	1,6			24,2
Carla Pires	12,0	Nova campanha MKT001	12,0	Líder MKT	6		21,3	0,0			21,3
Usuário solicitou retirada da base RH - Exemplo	9,0	Novo sistema Sys001	9,0	TIC LGPD	1					15,0	15,0
Novo sistema Sys001	9,0	Novo sistema ERPRH	9,0	Seg Empresarial LGPD	3		4,6		9,6		14,2
Novo sistema ERPRH	9,0	Novo serviço de diretório AD em nuvem	9,0	Líder Comunicação	2	12,5					12,5
Novo serviço de diretório AD em nuvem	9,0	Novo Produto P001	9,0	Gestão de Incidentes LGPD	2				12,0		12,0
Novo Produto P001	9,0	Novo ponto de venda	9,0	Marcelo Lopes	1					9,0	9,0
Novo ponto de venda	9,0	Novo armazenamento de processos judiciais	9,0	Líder Serviços	4		8,6				8,6
Novo armazenamento de processos judiciais	9,0	Nova Filial	9,0	Diretor Serviços I	2	7,7					7,7
Nova Filial	9,0										

Assunto		3. Áreas de ...		4. Sistemas e Suportes de Dados			5. Partes Relacionadas	
Assunto	Qtd	Área	PriorArea	Sistema/Suporte	PriorSist	Nome	PriorParte	
	194	4.2 RH	9,6	Backup	10,7	Uber	2,4	
(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais	37	2.2 U2	9,3	App Facebook, Instagram, Twitter	7,9	PI Saúde	2,4	
(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais, (Art 39) Operador, (Art 5...	1	2.1 Mkt	7,0	Site GoToWebinar	6,7	Forn Telefonia2	2,4	
(Art 01 .. 06) Contexto - Tratamento de Dados Pessoais, (Art 46 .. 49) Segurança ...	1	2.3 U3	5,5	Site Broadcast	6,7	Forn ERP	2,4	
(Art 04) Segurança e Defesa	9	1.3 UCM	5,5	MS LinkedIn	6,7	Easy Taxi	2,4	
(Art 07) Base Legal, Hipóteses de Tratamento	13	3.4 S4	4,0	LAG	6,7	Booking	2,4	
(Art 08) Consentimento	21	3.2 S2	4,0	CFTV, Câmeras	6,4	Airbnb	2,4	
(Art 09, 17 .. 22) Direito do Titular	53	4.4 TI	3,7	Site Curriculuns/vagas	5,9	Ag Viagem	2,4	
(Art 10) Legítimo Interesse	6	4.3 Fin	3,5	MS Dynamics	5,9			

6. Plano de Ação			DPOs		
Atividade	Descrição	Priori...	Título	Nome	PriorParte
Orientar a área quanto ao tratamento de dados pessoais de crianças e adolescentes	Atividade-guia	16,0			
Orientar a área quanto ao tratamento de dados pessoais de crianças e adolescentes	Atividade-guia (todas as áreas que tratem dados pesso...	16,0			
Avaliar e justificar a base legal (hipótese de tratamento) dos sistemas e suportes de dados	Atividade-guia (todos os sistemas e suportes de dados ...	16,0			
Avaliar e justificar a base legal (hipótese de tratamento) dos sistema/repositório	Atividade-guia	16,0			
Avaliar e implementar cláusulas contratuais de tratamento de dados pessoais dos sistemas e repositóri...	Atividade-guia	16,0			
Avaliar com a área a real necessidade de utilizar dados pessoais sensíveis e a possibilidade de minimizar	Atividade-guia	16,0			
Avaliar com a área a real necessidade de utilizar dados pessoais sensíveis e a possibilidade de minimizar	Atividade-guia (todas as áreas que realizem o tratament...	16,0			

A listagem não possui dados.

API – Registro do Tratamento, Gestão do Consentimento, Cadastro



GABRI

Flow Rule Editor Interface:

- Risk Manager Trigger** (FlowRule's Trigger)
- Find in View** (Get View)
- Patch Item** (Patch Entity Item)

Create Node Panel:

- Regular
- Trigger
- All

- Everest**: Integrate with Módulo Everest Software via API
- No Operation, do nothing**: No Operation
- Risk Manager**: Create data inside Organization and Workflow Module
- Spiceworks**: Select the sqlite database to fetch the inventory scan and vulnerabilities
- Start**: Starts the workflow execution from this node

Execute Workflow