EQUATORIAL TRANSMISSORA 7 SPE S.A.

Companhia Aberta

CNPJ/ME nº 26.845.702/0001-60

NIRE 53.300.017.71-9 | Código CVM nº 024457

ATA DA REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO REALIZADA EM 10 DE NOVEMBRO DE 2020

1. DATA, HORA E LOCAL: Em 10 de novembro de 2020, às 14:00 horas, na sede social da Equatorial Transmissora 7 SPE S.A. ("Companhia"), na cidade de Brasília, no Distrito Federal, ST SCS-B, Quadra n° 09, Bloco A, Sala 1201, Parte 7, Centro Empresarial Parque Cidade, Asa Sul, CEP 70.308-200.

2. CONVOCAÇÃO E PRESENÇA: Convocação realizada por correio eletrônico, nos termos do artigo 25, §1º, do estatuto social da Companhia. Presentes os membros do Conselho de Administração da Companhia por videoconferência, nos termos do artigo 25 §4º do Estatuto Social, conforme indicados a seguir: Augusto Miranda da Paz Junior e Leonardo da Silva Lucas Tavares de Lima.

3. MESA: Os trabalhos foram presididos pelo Sr. Augusto Miranda da Paz Júnior e secretariados pelo Sr. Leonardo da Silva Lucas Tavares de Lima.

4. ORDEM DO DIA: Os conselheiros reuniram-se para deliberar sobre a seguinte ordem do dia: **(i)** manifestar-se sobre os resultados operacionais e financeiros da Companhia referentes ao terceiro trimestre de 2020; **(ii)** aprovação da Política de Proteção de Dados do Grupo Equatorial Energia S.A.; **(iii)** eleição de novo membro do Conselho de Administração; **(iv)** convocação da Assembleia Geral de Acionistas da Companhia; e **(v)** autorização dos diretores da Companhia para a prática de todos os atos necessários para efetivar o quanto aprovado na presente reunião.

5. DELIBERAÇÕES: Foi aberta a sessão, tendo assumido a Presidência da Mesa o Sr. Augusto Miranda da Paz Júnior, que convidou o Sr. Leonardo da Silva Lucas Tavares de Lima para secretariar os trabalhos. Após o exame e a discussão das matérias da ordem do dia, os membros do Conselho de Administração deliberaram, por unanimidade dos votos, o quanto segue:

(i) Aprovar e apresentar os resultados operacionais e financeiros da Companhia referentes ao terceiro trimestre de 2020, compreendendo o Balanço Patrimonial, a Demonstração de Resultados e as Notas Explicativas referentes ao encerramento do terceiro trimestre de 2020;

(ii) Aprovar a Política de Proteção de Dados do Grupo Equatorial Energia S.A, conforme anexo I;

(iii) Nos termos do artigo 150 da Lei de S.A. e art. 23 § 2° do Estatuto Social da Companhia, os conselheiros presentes elegem como membro do Conselho de Administração da Companhia, o Sr. **Sérvio Túlio dos Santos**, brasileiro, casado sob o regime da comunhão parcial de bens, engenheiro eletricista, portador da Cédula de Identidade RG nº 43998602012-6, expedido pelo SSP/MA, inscrito no CPF/ME sob o nº 456.942.224-15, domiciliado à Alameda A, Quadra SQS, nº. 100, Loteamento Quitandinha, Altos do Calhau, São Luís, Estado do Maranhão, CEP: 65.070-900, com mandato até a primeira assembleia geral que for realizada pela Companhia após a data desta reunião.

(iv) Aprovar a convocação dos acionistas da Companhia para se reunirem em Assembleia Geral Extraordinária para discutirem e votarem a respeito da eleição de novo membro para o Conselho de Administração da Companhia; e

(v) Autorizar os diretores da Companhia para a prática de todos os atos necessários para efetivar o quanto aprovado na presente reunião.

6. **ENCERRAMENTO**: Nada mais havendo a ser tratado, lavrou-se a presente ata, a qual, após lida e aprovada, foi assinada pelo Secretário da Mesa e pelo Presidente da Mesa, por si, na qualidade de Presidente da Mesa e Presidente do Conselho de Administração, e pelos demais membros do Conselho de Administração, nos termos do artigo 25, §5º do Estatuto Social da Companhia.

CERTIDÃO

Confere com o original, lavrado em livro próprio.
Brasília/DF, 10 de novembro de 2020.

Mesa:

Augusto Miranda da Paz Júnior
Presidente

Leonardo da Silva Lucas T. de Lima
Secretário

Esta página é parte integrante da ata da Reunião do Conselho de Administração da Equatorial Transmissora 7 SPE S.A., realizada em 10 de novembro de 2020.

EQUATORIAL TRANSMISSORA 7 SPE S.A.

Companhia Aberta

CNPJ/ME nº 26.845.702/0001-60

NIRE 53.300.017.71-9 | Código CVM nº 024457

ANEXO I À ATA DA REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO REALIZADA EM 10 DE NOVEMBRO DE 2020

POLÍTICA INTERNA DE PROTEÇÃO DE DADOS PESSOAIS DO GRUPO EQUATORIAL

EQUATORIAL ENERGIA S.A.

Companhia Aberta

CNPJ n.º 03.220.438/0001-73

NIRE 2130000938-8 | Código CVM n.º 02001-0

POLÍTICA INTERNA DE PROTEÇÃO DE DADOS PESSOAIS DO GRUPO EQUATORIAL

---

06 de novembro de 2020

SUMÁRIO

1. INTRODUÇÃO E ESCOPO

A presente Política Interna de Proteção de Dados Pessoais da Equatorial Energia S.A. ("Política" e "Equatorial", respectivamente) foi elaborada com o objetivo de estabelecer as melhores práticas e identificar e definir os princípios, conceitos e diretrizes relacionados ao Tratamento de Dados Pessoais pela Equatorial. Esta se aplica a todos os funcionários, diretores, conselheiros e parceiros da Equatorial, suas subsidiárias e afiliadas, bem como terceirizados que possuam acesso a suas informações ("Colaboradores").

Todos os Colaboradores estão sujeitos às diretrizes desta Política e quaisquer eventuais alterações. O Anexo I traz o Termo de Compromisso com a Política Interna de Proteção de Dados Pessoais" ("Termo de Compromisso"), que deverá ser assinado por todos os Colaboradores no momento em que tiverem acesso ao presente documento.

Esta Política foi elaborada em consonância com a Lei Geral de Proteção de Dados Pessoais ("LGPD") – Lei Federal nº. 13.709, de 14 de agosto de 2018 e suas alterações, e com as demais legislações correlatas que versem sobre dados de pessoais, devendo ser interpretada em consonância com os demais manuais e políticas da Equatorial . Deverá ser atualizada a cada 24 (vinte e quatro meses), ou em caso de alterações significativas do normativo legal.

A estrutura da presente Política tem base nas Definições e nos Princípios Fundamentais que regem a proteção de dados pessoais no Brasil, e se desenvolve a partir da identificação das medidas de segurança dos Dados Pessoais e dos procedimentos de *compliance* direcionados especificamente aos objetivos da Equatorial.

1.1. DEFINIÇÕES

CONCEITOS ESSENCIAIS DE PROTEÇÃO DE DADOS PESSOAIS	
"**Dados Pessoais**" são informações relacionadas à pessoa natural identificada ou identificável. São dados relativos a um indivíduo (tais como Colaboradores, fornecedores, clientes) que, isoladamente ou em conjunto com outras informações, são ou podem ser utilizados para identificá-lo, coletados e/ou tratados de forma física ou eletrônica.	"**Tratamento**" é toda operação realizada com Dados Pessoais, tais como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
"Consentimento" manifestação livre, informada, prévia e inequívoca, por escrito ou outro meio, que demostre a manifestação de vontade.	"**Controlador**" é a pessoa que, por si só, isoladamente ou em conjunto, decide o quê, o por que e como os Dados Pessoais devem ser tratados.
"**Operador**" é qualquer pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do Controlador.	"**Titular**" é a pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

"**Autoridade Nacional de Proteção de Dados**" ou "**ANPD**" é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento de leis de proteção a Dados Pessoais em todo o território nacional.

"**Dados Anonimizados**" são dados relativos a um titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. As leis de proteção a Dados Pessoais e, consequentemente, esta Política não são aplicáveis ao tratamento de Dados Anonimizados.

"**Dados de Crianças e Adolescentes**" são Dados Pessoais que se referem a Titulares que são crianças e adolescentes e, portanto, o consentimento para tratar seus Dados Pessoais deve ser dado por pelos pais ou responsáveis legais. Pertencem a uma categoria especial de Dados Pessoais e, como tais, possuem restrições acerca dos Fundamentos Legais que podem embasar o Tratamento.

"**Dados Sensíveis**" são Dados Pessoais 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, quando vinculado a uma pessoa natural. Há restrições acerca dos Fundamentos Legais que podem embasar o Tratamento de Dados Sensíveis.

"Encarregado" ou ***"Data Protection Officer (DPO)***", nomenclatura instituída pelo Regulamento Geral sobre Proteção de Dados da União Européia (GDPR) , é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os Titulares e a Autoridade Nacional de Proteção de Dados.

"**Fundamentos Legais**" são as hipóteses, bases ou fundamentos jurídicos que permitem o tratamento dos dados pessoais pela Equatorial e seus respectivos operadores.s.

"**LGPD**" é a Lei Geral de Proteção de Dados Pessoais – Lei Federal nº. 13.709, de 14 de agosto de 2018, conforme alterada.

"**Terceiros**" são quaisquer pessoas naturais ou jurídicas, de direito público ou privado, que não os identificados acima ou que estejam sob as ordens do Controlador.

Os termos no plural definidos acima incluem o singular e vice-versa, conforme a circunstância.

1.2. PRINCÍPIOS FUNDAMENTAIS

Em linha com as melhores práticas atinentes à proteção de Dados Pessoais, a presente Política considera os princípios a seguir como fundamentais, os quais deverão ser observados por todos os Colaboradores, quais sejam:

a. **Responsabilidade, Justiça e Transparência**: os Dados Pessoais devem ser tratados pela Equatorial de forma responsável, justa e transparente em relação ao Titular, garantindo o livre acesso aos Dados Pessoais pelos seus Titulares.

b. **Prevenção e Segurança**: a Equatorial deve adotar medidas técnicas e administrativas para prevenir incidentes que possam levar a acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou difusão dos Dados Pessoais.

c. **Proteção do Titular de Dados Pessoais**: a Equatorial deve respeitar os direitos do Titular de Dados Pessoais, conforme determinado pela legislação nacional aplicável. Os Dados Pessoais devem ser mantidos de forma segura durante todo o período de Tratamento, desde a coleta até a sua exclusão definitiva.

d. **Legalidade no Tratamento**: só poderá ser realizado Tratamento de Dados Pessoais pela Equatorial quando baseado em pelo menos um dos Fundamentos Legais estabelecidos no item 2.5 abaixo.

e. **Transparência na Obtenção de Dados Pessoais**: como regra geral, os Dados Pessoais devem ser coletados diretamente de seus Titulares. Quando ocorrer a coleta de forma indireta, ou seja, por meio de compartilhamento realizado por Terceiros, as regras para tanto deverão ser

observadas.

f. **Limitação de Finalidade**: os Dados Pessoais devem ser coletados para finalidades determinadas, explícitas e legítimas e serem tratados, exclusivamente, de acordo com essas finalidades.

g. **Minimização dos Dados Pessoais**: a Equatorial deve tratar apenas os Dados Pessoais necessários para suas atividades. Desta forma: (i) os Dados Pessoais tratados devem ser adequados e pertinentes às finalidades a que se destinam e de acordo com o Fundamento Legal aplicável; (ii) não deverão ser tratados mais Dados Pessoais do que os necessários para cumprimento de suas finalidades; (iii) quando possível, os Dados Pessoais deverão ser anonimizados; e (iv) Dados Pessoais excedentes e desnecessários para as atividades da Equatorial devem ser eliminados.

h. **Precisão**: os Dados Pessoais devem ser precisos e, se necessários, atualizados.

i. **Limitação de Armazenamento**: os Dados Pessoais deverão ser tratados pela Equatorial pelos prazos necessários para atendimento de suas finalidades, após decorridos os prazos em questão deverão ser eliminados.

j. **Prestação de Contas**: a Equatorial deverá ser capaz de demonstrar as medidas adotadas em cumprimento das normas de proteção a Dados Pessoais e atendimento aos direitos dos Titulares, entre elas medidas com o fim de evitar a ocorrência de danos, demonstrando os padrões de segurança e mecanismos internos de mitigação de riscos, em especial no que se refere aos Dados Sensíveis e aos Dados de Crianças e Adolescentes.

2. SEGURANÇA DOS DADOS PESSOAIS

2.1. A ESTRUTURA DE GOVERNANÇA CORPORATIVA

A estrutura de governança é composta pelas seguintes figuras:

• CEO da Equatorial: responsável por ratificar as decisões de alto risco tomadas em relação à matéria de proteção de Dados Pessoais, bem como deliberar máterias de alto risco que não sejam objeto de análise do Comitê.

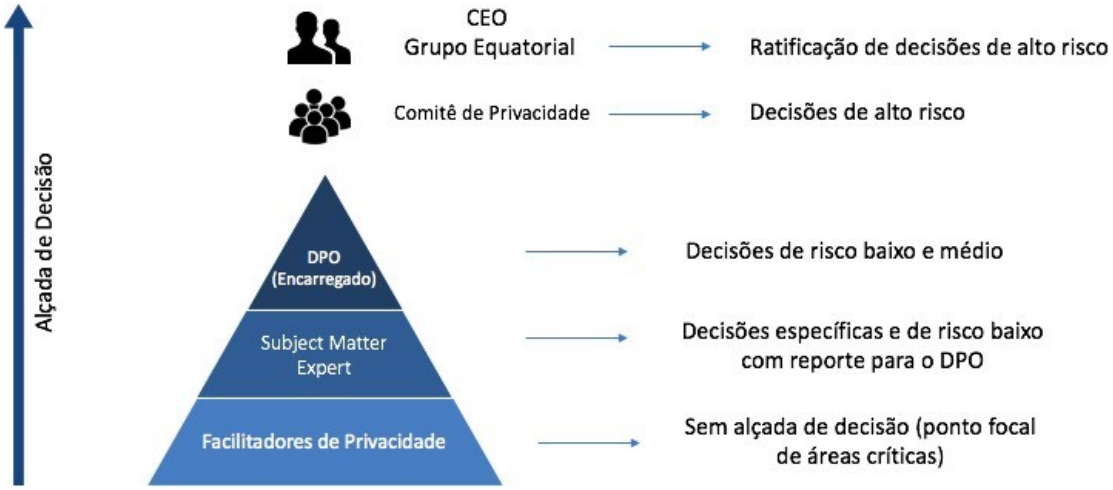
• Comitê de Privacidade: responsável pela tomada de decisões de alto risco, que depois passarão pela ratificação do CEO.

• DPO (Encarregado): responsável pela tomada de decisões de risco baixo a médio em relação à matéria de proteção de Dados Pessoais.

• *Subject Matter Experts*: atuarão junto ao DPO em assuntos de baixo risco, porém de alto grau de especificidade de uma determinada área.

• Facilitadores de Privacidade: não possuem alçada para tomar decisões, mas representam o ponto norteador para áreas críticas da Equatorial em relação aos assuntos que envolvem Dados Pessoais.

Abaixo, temos um pequeno resumo das atribuições e finalidade de c ada uma dessas figuras:



2.2. COMITÊ DE PRIVACIDADE

O Comitê de Privacidade ("Comitê") será presidido pelo Encarregado e formado por demais membros a serem indicados pelo CEO. Ele será responsável pela tomada de decisões de alto risco, que estarão sujeitas a ratificação pelo CEO. As decisões de alto risco que por quaisquer motivos não forem objeto de deliberação pelo Comitê, deverão serdeliberadas diretamente pelo CEO.

Dentre as atribuições do Comitê estão aprovar soluções, produtos e/ou práticas de negócio cujo risco seja classificado como alto para a proteção de Dados Pessoais, discutir e tomar decisões sobre novas atividades de Tratamento de Dados Pessoais, nivelar conhecimento sobre privacidade com *stakeholders* críticos e determinar, , entre outras atribuições, terá a responsabilidade de supervisionar a implementação desta Política e observância de seus termos, assim como dos demais procedimentos ligados a proteção de Dados Pessoais e assuntos correlacionados.junto às áreas da Equatorial, quanto aos Dados Pessoais tratados e acessados por cada área e acessos permitidos (Anexo V).

Caberá ao Comitê analisar os incidentes de segurança e classificá-los de acordo com o nível de gravidade (alto, médio ou baixo). Caso a Equatorial receba uma notificação de incidente de segurança, o Encarregado deverá comunicar imediatamente o CEO e convocar reunião extraordinária do Comitê a ser realizada no prazo máximo de 24 (vinte e quatro) horas, em conjunto com o responsável pelo departamento de T.I., o responsável pelo departamento afetado pelo incidente, e demais áreas e/ou Colaboradores estratégicos que estejam envolvidas no incidente ou possam auxiliar na determinação de medidas mitigadoras.

O Comitê deverá analisar a extensão e gravidade do incidente e identificar se atende os requisitos de comunicação às autoridades. A ata da reunião do Comitê que tratar de matéria relacionada a notificação de incidente deverá ser encaminhada para o CEO imediatamente após o término da reunião. Os procedimentos técnicos a serem adotados estarão previstos na Política de Segurança da Informação e na Norma de Procedimento para Gestão de Incidentes de Segurança da Informação e Dados Pessoais. Eventuais medidas estratégicas deverão ser aprovadas,aprovadas

pelo CEO, bem como quaisquer decisões que envolvam alto risco.

O Comitê reunir-se-á ordinariamente mediante convocação do Encarregado, a qual deverá ser enviada por correio eletrônico com até 5 (cinco) dias de antecedência e só poderá ser oficialmente instalada com a presença de no mínimo 3 (três) membros. Em caso de urgência, o Encarregado poderá solicitar a realização da reunião em prazo inferior.

2.3. FUNÇÕES E RESPONSABILIDADES DO ENCARREGADO (DPO)

O Encarregado, além de ser o responsável pela tomada de decisões de risco baixo a médio em relação à proteção de Dados Pessoais, é a pessoa de contato inicial na Equatorial no caso de qualquer questão, esclarecimento, dúvida ou assunto que envolva a matéria, sendo responsável por:

a. Monitorar as leis, regulamentos e quaisquer outras informações relevantes à privacidade e proteção de Dados Pessoais que possam impactar a Equatorial, garantindo que a presente Política e demais políticas e procedimentos sobre o tema estejam em conformidade com os requisitos legais.

b. Monitorar o cumprimento da presente Política e demais políticas e procedimentos sobre o tema.

c. Gerir assuntos ligados a privacidade e proteção de Dados Pessoais da Equatorial, conduzindo periodicamente seu *assessment* de maturidade, mantendo as evidências de sua execução (*accountability*) e acompanhando os planos de ação para correção de possíveis *gaps*.

d. Apoiar e fornecer informações necessárias ao Comitê, para que este possa cumprir suas funções.

e. Orientar e assessorar os Colaboradores no que diz respeito às questões de privacidade e proteção de Dados Pessoais, esclarecendo dúvidas e estabelecendo os procedimentos necessários para observância da presente Política.

f. Coordenar com todas as áreas e negócios da Equatorial os assuntos ligados à privacidade e proteção de Dados Pessoais.

g. Gerenciar pedidos de Titulares de Dados Pessoais e comunicação com estes no que se referir a assuntos de Proteção de Dados Pessoais, bem como aceitar reclamações e comunicações dos Titulares, prestar esclarecimentos e adotar as providências necessárias.

h. Receber as comunicações e coordenar as respostas a solicitações da Autoridade Nacional de Proteção de Dados envolvendo consultas e investigações de incidentes.

i. Avaliar projetos que envolvam Dados Pessoais de modo a verificar se estão em conformidade com esta Política e demais legislações e regulamentos aplicáveis.

j. Acompanhar os processos de Tratamento de Dados Pessoais de modo a verificar se estão em conformidade com esta Política e demais legislações e regulamentos aplicáveis.

k. Informar todas as áreas e negócios da Equatorial acerca de solicitações de retirada de consentimento feita por Titulares para que todo e qualquer Tratamento de Dados Pessoais feitos com base em consentimento seja cessado e os referidos Dados Pessoais eliminados.

l. Adotar e implementar diretrizes necessárias para assegurar que os Tratamento ocorram em observância aos termos da presente Política.

m. Elaborar e manter atualizado, em conjunto com o Comitê e o departamento de T.I., a Norma de Procedimento para Gestão de Incidentes de Segurança da Informação e Dados Pessoais, para minimizar danos e falhas de segurança e estabelecer ações imediatas em situações de crise.

n. Em caso de notificação de incidente de segurança, imediatamente comunicar a Diretoria da companhia e convocar reunião extraordinária do Comitê.

o. Elaboração e análise dos relatórios de impacto à proteção de dados pessoais.

2.4. FUNÇÕES E RESPONSABILIDADES DOS *SUBJECT MATTER EXPERTS* E FACILITADORES DE PRIVACIDADE

Conforme mencionado acima, a estrutura de governança corporativa em Dados Pessoais da Equatorial conta ainda com os *Subject Matter Experts* e os Facilitadores de Privacidade. Ambos exercem posições estratégicas em matéria de proteção de Dados Pessoais, conforme será visto a seguir:

(a) *Subject Matter Experts*. São representantes indicados pelo CEO da Equatorial, que reportam diretamente ao DPO, e são responsáveis por decisões específicas e de baixo risco. Entre suas responsabilidades estão: (i) aprovar soluções, produtos e/ou práticas de negócio cujo risco seja classificado como baixo para a proteção de Dados Pessoais; (ii) supervisionar, no âmbito das gerências da Equatorial, se suas práticas estão em conformidade com leis, regulamentos e quaisquer outras informações relevantes à privacidade e proteção de Dados Pessoais; (iii) monitorar, no âmbito das gerências da Equatorial, o cumprimento da presente Política e demais políticas e procedimentos sobre o tema; (iv) servir de ponto focal de assunto ligados à privacidade e proteção de Dados Pessoais dentro das unidades de negócio da Equatorial; (v) auxiliar o DPO na elaboração e análise dos relatórios de impacto à proteção de dados pessoais; e (vi) auxiliar o DPO manter as evidências de sua execução (*accountability*) e acompanhar os planos de ação para correção de possíveis *gaps*.

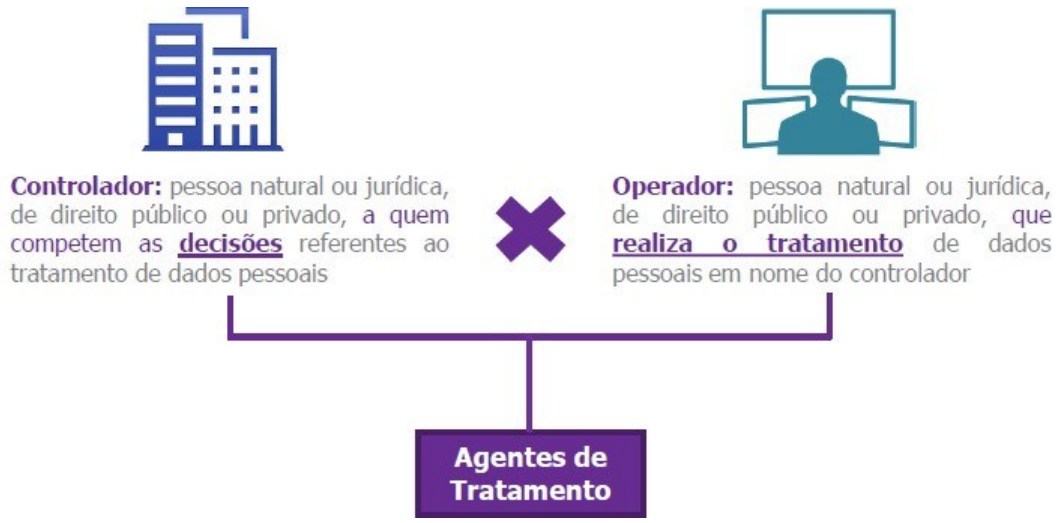
(b) Facilitadores de Privacidade. São facilitadores sem poder decisório, essenciais para a criação da cultura de privacidade, que representam o ponto norteador para áreas críticas da Equatorial em relação aos assuntos que envolvem Dados Pessoais. Entre suas responsabilidades estão: (i) facilitar de treinamento e comunicações para os Colaboradores de sua área; (ii.) levantar informações a respeito de projetos de sua área para auxiliar o DPO na elaboração e análise de relatórios de impacto à proteção de dados pessoais; e (iii.) servir de ponto focal dos Colaboradores da sua área na comunicação com o Encarregado.

2.5. RELAÇÃO COM TERCEIROS CONTROLADORES E OPERADORES

A Equatorial apenas deverá compartilhar Dados Pessoais com Terceiros (sejam Controladores ou Operadores) que adotem medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado.

Por essa razão, previamente ao compartilhamento, as atividades dos Terceiros devem estar em conformidade com a LGPD, e a Equatorial deverá tomar e documentar medidas de precaução para garantir a segurança dos Dados Pessoais compartilhados.

Assim, é muito importante saber diferenciar um Controlador de um Operador, pois as precauções que a Equatorial deverá tomar em relação ao compartilhamento com outro Controlador são diferentes das precauções necessárias na relação com um Operador, conforme será disposto a seguir.



CONTROLADOR	OPERADOR
• Determina o motivo, as finalidades e como os dados pessoais serão tratados pelo Operador.	• Apenas realizam o Tratamento dos Dados Pessoais em nome e em benefício do Controlador. Nunca em seu próprio benefício.

• Deve garantir que possui um Fundamento Legal para realizar o Tratamento – inclusive para garantir a legalidade do compartilhamento com Terceiros.	• Devem seguir as diretrizes e instruções do Controlador para realizar o Tratamento dos Dados Pessoais.
• Deve fiscalizar os Operadores e garantir que eles possuem condições de tratar, de forma segura, os Dados Pessoais recebidos.	• Poderá ser responsabilizado em caso de violação à LGPD se tiver descumprido as diretrizes e instruções do Controlador.

2.6. RELACIONAMENTO COM OPERADOR

A Equatorial deverá orientar e instruir o Operador a respeito da realização do Tratamento de Dados Pessoais em nome da Equatorial, e verificar se o Tratamento dos Dados Pessoais está de acordo com as instruções e respeitando as obrigações de confidencialidade e medidas de segurança aplicáveis.

A relação entre a Equatorial e seus Operadores deverá ser regulada por meio de contrato que contenha cláusulas específicas de proteção de Dados Pessoais, estabelecendo a posição e responsabilidades das partes na condição de Controlador e de Operador, bem como as instruções a serem seguidas pelo Operador.

Os Colaboradores da Equatorial podem utilizar algumas referências para analisar se o terceiro em questão está na condição de Operador, mas note que os conceitos não são absolutos. Devem ser interpretados em conjunto com os princípios fundamentais descritos no item 1.2, e com os direitos dos titulares.

AVALIAÇÃO DO TERCEIRO OPERADOR (opera os dados pessoais)
• Não tem tomada de decisão sobre o que é feito com os Dados Pessoais;

• Depende de uma decisão do Controlador e fica limitado ao que for determinado; • Parceiro técnico especializado para atingir os objetivoos definidos pelo Controlador.	
O que a Equatorial deve fazer?	1. Determinar a finalidade e hipótese legal para o Tratamento dos dados Pessoais. 2. Instruir e fiscalizar o Tratamento e documentar as instruções e fiscalizações. 3. Demonstrar que observou seu dever de diligencia. 4. Formalizar toda relação por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relação de Controlador/Operador.
O que o Operador deve fazer?	1. Realizar o Tratamento dos Dados Pessoais em nome da Equatorial. 2. Utilizar as melhores práticas para proteção de Dados Pessoais. 3. Cumprir todas as práticas e diretrizes estabelecidades nesta Política, na legislação aplicável, e no contrato celebrado com a Equatorial, bem como instruções específicas adicionais que o Colaborador e/ou a área entender necessárias.

2.7. RELACIONAMENTO COM OUTRO CONTROLADOR

Na relação entre dois Controladores não é necessário que a Equatorial oriente e instrua os demais Controladores, os quais serão os únicos responsáveis em caso de violações à legislação aplicável de proteção de Dados Pessoais que derem causa.

Contudo, embora não haja o dever de orientação, há o dever de diligencia e da mesma forma a relação entre a Equatorial e demais Controladores deverá ser regulada por meio de contrato que contenha cláusulas específicas de proteção de Dados Pessoais, estabelecendo as obrigações e responsabilidades das partes na condição de Controlares, bem como o Tratamento a ser realizado e demais condições.

Caso a Equatorial receba e trate Dados Pessoais coletados por Terceiros com base unicamente em consentimento, a Equatorial deve certificar-se de que o Titular concedeu novo consentimento para o compartilhamento ou que esteja dentre um dos imperativos e/ou permissivos legais para o partilhamento das referidas informações.

Os Colaboradores da Equatorial podem utilizar algumas referências para analisar se o terceiro em questão está na condição Controlador, mas note que os conceitos não são absolutos. Devem ser interpretados em conjunto com os princípios fundamentais descritos no item 1.2, e com os direitos dos titulares.

<table>
<tr><th colspan="2">AVALIAÇÃO DO TERCEIRO CONTROLADOR
(controla os dados pessoais)</th></tr>
<tr><td colspan="2">• Possui relação direta com o Titular;
• Possui responsabilidade primária de garantir conformidade com a LGPD;
• Controla a finalidade e os meios gerais do Tratamento;
• É responsável pela tomada de decisão em relação aos dados pessoas;
• Primeiro alvo das ações de fiscalização.</td></tr>
<tr><td>O que a Equatorial deve fazer?</td><td>1. Demonstrar que observou seu dever de diligencia.</td></tr>
</table>

	2. Caso esteja na posição de receber Dados Pessoais e o Tratamento for com base em consentimento, certificar-se de que o Titular concedeu consentimento para o compartilhamento (controlador/controlador). 3. Formalizar toda relação por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relação de Controlador/Controlador. 4. Verificar o cumprimento do contrato.
O que o Terceiro Controlador deve fazer?	1. Utilizar as melhores práticas para proteção de Dados Pessoais. 2. Cumprir a legislação aplicável, em matéria de proteção de Dados Pessoais e o contrato celebrado com a Equatorial.

2.8. FUNDAMENTOS LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

A Equatorial e seus Colaboradores somente poderão tratar Dados Pessoais caso exista pelo menos uma base ou fundamento jurídico para tal, nos termos desta Política e/ou da LGPD ("Fundamento Legal"). Assim, antes de realizar qualquer atividade de Tratamento, o Fundamento Legal correto precisa ser identificado e registrado. Caso seja identificado qualquer Tratamento de Dados Pessoais pela Equatorial, sem o devido Fundamento Legal, tal Tratamento deve ser interrompido e os dados eliminados.

Fundamento Legal é a justificativa, nos termos da LGPD, para realização de Tratamento de Dados Pessoais. O Tratamento pela Equatorial e seus Colaboradores de Dados Pessoais que não pertençam a categoriais especiais deve ser sempre baseado em um ou mais dos seis Fundamentos Legais abaixo:

i. Execução de contrato do qual seja parte o Titular;

ii. Cumprimento de obrigação legal ou regulatória pelo Controlador;

iii. Proteção da vida ou da incolumidade física do Titular;

iv. Exercício regular de direitos em processo judicial, administrativo ou arbitral;

v. Legítimo interesse da Equatorial ou Terceiros, exceto quando prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos Dados Pessoais; e

vi. Consentimento fornecido pelo do Titular.

Quando o Tratamento for realizado com base no consentimento do Titular, o termo de consentimento deve cumprir as seguintes exigências: ser prévio, por escrito, de forma destacada, clara e inequívoca, bem como prever a finalidade específica para o Tramento a ser realizado.

Caso ocorra mudanças da finalidade para o Tratamento de Dados Pessoais, cujo Fundamento Legal é o consentimento, o Titular deverá ser previamente informado sobre tais mudanças de finalidade e o termo de consentimento deverá ser devidamente atualizado.

O consentimento, de acordo com disposição legal, pode ser revogado pelo Titular a qualquer momento, mediante comunicação à Equatorial. Assim, toda vez que o Encarregado informar que determinado Titular revogou o consentimento para Tratamento de Dados Pessoais tratados sem nenhum outro Fundamento Legal, todos os Colaboradores deverão cessar qualquer Tratamento referente a eles e exclui-los, em conformidade com as recomedações publicadas e/ou instauradas pelo Encarregado.

2.9. DIREITOS DOS TITULARES

Os Titulares possuem diversos direitos garantidos pela legislação de proteção de dados, que devem ser respeitados pela Equatorial e todos os seus Colaboradores, dentre eles:

a. Direito de obter confirmação da existência de Tratamento;

b. Direito de acesso aos seus Dados Pessoais e a informações acerca da natureza do Tratamento;

c. Direito de pedir a correção de seus Dados Pessoais que estiverem incompletos, inexatos ou desatualizados;

d. Direito de pedir a anonimização, bloqueio ou eliminação de seus Dados Pessoais que forem desnecessários, excessivos ou tratados em desconformidade com o disposto na legislação aplicável;

e. Direito de revogar o consentimento para o Tratamento de seus Dados Pessoais e de pedir a qualquer Controlador que elimine tais dados quando eles forem tratados somente com base no consentimento revogado;

f. Direito de pedir informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

g. Direito de ser informado sobre quais entidades públicas e privadas o Controlador realizou uso compartilhado de dados.

Todos os pedidos ligados aos direitos dos Titulares deverão ser dirigidos ao Encarregado, conforme instruções que deverão constar no *site* da Equatorial (ver Anexo III). Os direitos listados acima não são absolutos e, portanto, a Equatorial pode se negar a atendê-los caso esteja sujeita a obrigações legais que podem impedi-la de pôr em prática determinadas solicitações.

A Equatorial deverá responder as solicitações dos Titulares no prazo máximo de até 15 (quinze) dias, contado da data do requerimento do Titular.

2.10. CATEGORIAS ESPECIAIS DE TRATAMENTO DE DADOS PESSOAIS

Existem duas categoriais especiais de Dados Pessoais: Dados Sensíveis e Dados de Crianças e Adolescentes. Por serem Dados Pessoais com características especiais, somente podem ser tratados com base em Fundamentos Legais específicos, conforme previsto abaixo.

1. Dados Sensíveis.

O Tratamento de Dados Sensíveis somente poderá ocorrer com o consentimento do Titular ou em atendimento a uma obrigação legal ou regulatória. Assim, toda vez que o Colaborador em questão for tratar Dados Sensíveis, deverá comunicar o Encarregado para verificar se existe alguma obrigação legal ou regulatória que obriga a Equatorial a realizar aquele Tratamento ou, caso não haja, obter o consentimento específico do Titular em questão.

2. Dados de Crianças e Adolescentes.

O Tratamento de Crianças e Adolescentes somente poderá ocorrer com o consentimento dos pais ou responsável legal. Assim, toda vez que o Colaborador em questão for tratar Dados Pessoais de Crianças e Adolescentes, deverá comunicar o Encarregado para se certificar que a empresa possui um consentimento específico assinado pelos pais ou responsáveis legais da criança ou adolescente em questão.

2.11. CONTROLE DO TRATAMENTO REALIZADO

Todo Tratamento realizado pela Equatorial com base em interesse legitimo deverá ser registrado e controlado pelo Colaborador responsável pelo Tratamento. Assim, o Colaborador que realizar o Tratamento de Dado Pessoal com base em interesse legítimo deverá preencher e entregar

ao Encarregado documento específico referente àquele Tratamento, nos termos do Anexo IV.

É recomendável, porém não obrigatório, que os Colaboradores responsáveis por Tratamentos baseados em outros Fundamentos Legais também registrem e controlem a atividade em questão.

2.12. DIVULGAÇÃO E TRANSFERÊNCIA DE DADOS PESSOAIS A TERCEIROS NÃO AUTORIZADOS

A Equatorial deve envidar seus melhores esforços para que os Dados Pessoais não serão divulgados a Terceiros não autorizados, ou seja, aqueles para os quais não há Fundamento Legal para compartilhamento. Todos os Colaboradores devem ter cautela quando questionados a divulgar Dados Pessoais para Terceiros e dirigir ao Encarregado quaisquer dúvidas a respeito.

2.13. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Toda e qualquer transferência internacional de Dados Pessoais deverá ser comunicada ao Encarregado previamente. A comunicação deverá se dar com antecedência à efetivação do Tratamento e deverão ser informados:

i. País destinatário das informações;

ii. Agente que receberá as informações;

iii. Quais Dados Pessoais serão transferidos;

iv. Identificação do Titular;

v. Fundamento Legal – ou fundamentos legais – que embasam o Tratamento; e

vi. Como os Dados Pessoais em questão foram coletados pela Equatorial.

A transferência internacional somente poderá ser realizada após a autorização do Encarregado e mediante previsão contratual específica estabelecendo as obrigações e responsabilidades das partes. A autorização também deverá determinar se a transferência poderá ser feita de forma contínua, de acordo com a necessidade exigida, ou se cada transferência referente ao escopo deverá ser submetida à nova autorização.

2.14. ELIMINAÇÃO DE DADOS PESSOAIS

O Tratamento dos Dados Pessoais pela Equatorial somente deverá ocorrer enquanto houver Fundamento Legal para tanto, sem prejuízo do direito à eliminação dos dados, seja pela revogação dos Titulares ou pelo término do prazo de tratamento. Desta forma, os gestores das áreas da Equatorial reunir-se-ão anualmente com o Encarregado para avaliação acerca dos Dados Pessoais tratados pela área e eliminação daqueles cujo Fundamento Legal tenha expirado.

3. PROCEDIMENTOS DE *COMPLIANCE*

3.1. MEDIDAS TÉCNICAS E ORGANIZACIONAIS

A Equatorial deverá envidar seus melhores esforços para implementar medidas técnicas e organizacionais necessárias à segurança adequada de Dados Pessoais de acordo com as orientações do departamento de TI, da Política de Segurança da Informação e demais políticas aplicáveis, sempre acompanhadas pelo Encarregado. Todos os Colaboradores são responsáveis por garantir que os Dados Pessoais que a Equatorial detém e é responsável, sejam mantidos de forma segura e não sejam divulgados a Terceiros, a menos que esse terceiro tenha sido especificamente autorizado pela Equatorial para receber essas informações.

Os Dados Pessoais devem ser acessíveis apenas para aqueles que precisam usá-los, e o acesso só pode ser concedido em conformidade com esta Política.

Os Dados Pessoais só podem ser excluídos ou descartados em consonância com esta Política

e demais regulamentos, diretrizes e outros documentos aplicáveis.

3.2. GESTÃO DE INCIDENTES DE SEGURANÇA

Qualquer suspeita de violação a esta Política e à legislação aplicável de proteção de Dados Pessoais deve ser imediatamente reportada ao Encarregado, conforme previsto no Anexo II. Nenhum Colaborador deverá investigar por conta própria, a não ser que seja instruído de tal forma pelo Encarregado ou pelo próprio Comitê.

Violações, incidentes e fragilidades relevantes que possam causar prejuízos financeiros ou materiais à Equatorial precisam ser reportados ao Comitê para que delibere quais ações corretivas precisam ser tomadas, permitindo uma resposta institucional em tempo hábil.

3.3. AÇÕES EM CASO DE NÃO CONFORMIDADE

Os descumprimentos a esta Política serão submetidos ao Comitê, que endereçará o referido descumprimento e suas eventuais consequências aos superiores hierárquicos do(s) Colaborador(es) responsável(is) pelo descumprimento.

A violação comprovada a esta Política poderá constituir justa causa para possível aplicação de sanção disciplinar, independente das funções exercidas, e sem prejuízo das penalidades legais cabíveis, observadas as regras constantes do estatuto social da Equatorial.

A omissão diante da violação conhecida das leis aplicáveis ou de qualquer disposição desta Política não é uma atitude correta, incidindo como descumprimento das normas e políticas internas do Grupo Equatoria.

No caso de conhecimento sobre o descumprimento a esta Política, o Colaborador deve informar tal descumprimento ao Encarregado, que tem o dever de analisar e recomendar as respectivas ações corretivas para o Comitê.

4. CONSIDERAÇÕES FINAIS

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes desta Política não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar o Encarregado e/ou Comitê.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar ao desligamento ou outras sanções, inclusive decorrentes da legislação ou regulamentação aplicável.

Esta Política será amplamente divulgada pela Equatorial para todos os Colaboradores e partes interessadas, sob a coordenação do Comitê.

4.1. CONTROLE DE REVISÕES

REV	DATA	ITEM	DESCRIÇÃO DA MODIFICAÇÃO	RESPONSÁVEL
00	06 / 11/ 2020	Todos	Emissão Inicial	José Sobral

APROVACÃO:

ELABORADOR (ES) / REVISOR (ES)

Gerência Corporativa de TI/TELECOM

Sérgio Rodrigo Pereira de Araujo

Sarah Giselle Menezes Bezerra

Gerência Corporativa de Contencioso e Compliance

Érika Wilza Erika Wilza Brito de Assis Lorenzo Alves

Brenna Caroliny de Sousa Cunha

APROVADOR (ES)

Encarregado/DPO do Grupo Equatorial

José Sobral Silva Neto

ANEXO 1

TERMO DE COMPROMISSO

Declaro que, nesta data, recebi, li e compreendi a Política Interna de Proteção de Dados Pessoais da Equatorial Energia S.A. em sua totalidade, estou ciente de seu conteúdo e da sua importância para o exercício de todas as atividades da empresa., e, livremente, comprometo-me a seguir suas disposições e zelar por seu cumprimento dentro da Companhia.

Estou consciente de que minha conduta deve se pautar sempre pelos mais altos padrões previstos na legislação aplicável à proteção de Dados Pessoais, sempre levando em consideração as melhores práticas, princípios, conceitos e diretrizes relacionados ao Tratamento de Dados Pessoais pela Equatorial.

A assinatura do presente Termo é manifestação de minha livre concordância e do meu compromisso em cumprir integralmente as regras da Política que me foi apresentada.

Este Termo de Compromisso passa a ser parte integrante do meu Contrato de Trabalho.

Data:_____/_____/_____

_____
Assinatura

Nome:

Cargo:

Matrícula:

ANEXO 2

Formulário para que o Colaborador possa notificar imediatamente após o seu conhecimento sobre incidentes, falhas ou fragilidades. Documento poderá ser disponibilizado pela Equatorial em sua *intranet* e quaisquer outras plataformas eletrônicas escolhidas pela Equatorial e, após preenchido, deverá ser direcionado ao Encarregado.

O Colaborador deverá enviar as informações por e-mail ao Encarregado e solicitar a confirmação de envio.

FORMULÁRIO DE NOTIFICAÇÃO DE INCIDENTES

Nome e Área* E-mail e tefone para Contato*	
Descrição da natureza dos dados pessoais afetados*	
Informações sobre os titulares envolvidos *	
Riscos relacionados ao incidente*	
Indicação das medidas técnicas e de segurança já utilizadas	
Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo	
Os motivos da demora, no caso de a comunicação não ter sido imediata	
Outras informações pertinentes	

* Informações obrigatórias

ANEXO III

Formulário para que o Titular possa solicitar acesso aos seus Dados Pessoais. Documento poderá ser disponibilizado pela Equatorial em seu *site* e quaisquer outras plataformas eletrônicas escolhidas pela Equatorial e, após preenchido, deverá ser direcionado ao Encarregado.

Após o preenchimento do formulário, recomendamos que o Titular seja solicitado a marcar um "X" em uma janela *pop-up* concordando com o envio das informações e, logo abaixo, a informação acerca da estimativa de tempo de resposta à solicitação.

É recomendável que o Titular também receba por e-mail a confirmação de envio.

FORMULÁRIO DE SOLICITAÇÃO DE INFORMAÇÕES PESSOAIS

Nome Completo do Solicitante*	
E-mail para Contato*	
Telefone para Contato*	
Informação Requerida*	
Outras Solicitações	

* Informações obrigatórias

Caso maiores detalhes sobre a minha solicitação sejam necessários, eu autorizo a Equatorial a entrar em contato por meio do meu e-mail e/ou telefone informados acima.

ANEXO IV

TABELA DE CONTROLE DE TRATAMENTO DE DADOS PESSOAIS (INTERESSE LEGÍTIMO)

Área	Dados Pessoais Tratados	Hipótese Legal	Coleta, Armazenamento, Acesso e Eliminação	Compartilhamento	Justificativa para o Uso do Dados Pessoais
			Como é feita a coleta: **Onde são armazenados:** **Quem tem acesso:** **Existe eliminação periódica?**	**Dados são compartilhados com agentes externos (ex.: outras empresas)?** **Existe algum contrato que regula o compartilhamento?**	

⇨ Instruções de preenchimento: essa tabela deverá ser preenchida pelo responsável da área toda vez que for realizado um Tratamento com base em interesse legítimo. O objetivo da tabela é justamente controlar esse tipo de Tratamento e, caso necessário, comprovar para a Autoridade Nacional de Proteção de Dados (ANPD) que o procedimento foi feito de forma legal e correta.

A partir do preenchimento da tabela, é essencial ficar claro quais dados foram tratados, por quem, por que, onde eles estão armazenados, quem tem acesso e, se tiver havido compartilhamento, a indicação de quem são os agentes externos. Caso seja um Tratamento recorrente, é importante também registrar na tabela.

Se o Tratamento baseado em interesse legítimo não for controlado, a Equatorial pode ser investigada, ou até mesmo responsabilizada, por violar as regras da LGPD.

ANEXO 1

MANUAL DE TRATAMENTO DE DADOS PESSOAIS

Princípios de Gestão no Tratamento de Dados Pessoais

Capacitação e Desenvolvimento: Cada área deverá empregar os melhores esforços para garantir que os Colaboradores da área tenham ciência de que os Dados Pessoais a que tiverem acesso pertencem aos próprios Titulares, sobre os cuidados necessários com os Dados Pessoais, conforme estabelecido pela legislação aplicável, e que assinem o Termo de Recebimento e Compromisso com a Política Interna de Proteção de Dados Pessoais.

Segurança da Informação: As informações geradas, armazenadas, processadas, administradas ou de qualquer forma confiadas à companhia são de propriedade dos Titulares. Assim, a companhia deve envidar esforços para proteger tais informações, valendo-se da sua estrutura de segurança da informação, e seus Colaboradores devem proteger esses ativos de informação visando a garantir sua confidencialidade, integridade e disponibilidade.

Medidas de Segurança Adotadas: Os Colaboradores devem sempre verificar e submeter ao Encarregado/DPO: (i) se a área possui adequada segurança (física e tecnológica) para proteger os Dados Pessoais; (ii) se utilizam acesso por senhas e com contas de e-mail corporativos criptografadas; e observar condutas adequadas tais como, bloquear computadores ao sair da mesa, não deixar documentos nas áreas e impressoras de uso coletivo, guardar documentos físicos em armários com chave, sempre verificar os destinatários das mensagens antes de compartilhar dados, evitar compartilhar dados por plataformas que não tenham requisitos de segurança.

Cópia e Eliminação de Dados: Identificar e submeter ao Encarregado/DPO: (i) se a área elimina dados desnecessários com alguma periodicidade; (ii) se os Colaboradores da área conseguem apagar definitivamente e extrair cópias dos dados salvos na rede da companhia. Deve-se preferencialmente identificar e registrar nos sistemas o *login* e data de cópias e eliminações.

Compartilhamento de Dados com Terceiros: Identificar e submeter ao Encarregado/DPO: (i) quais os Dados Pessoais são compartilhados

com outras empresas (dentro e fora do grupo empresarial a qual pertencem); (ii) se são compartilhados preferencialmente por meio de sistemas, com acesso por senhas e registro das informações de acesso, cópias, impressões. Deve-se evitar que o compartilhamento seja feito por e-mail.

Dados Pessoais Recebidos de Terceiros: Verificar e submeter ao Encarregado/DPO: (i) se a área recebe dados pessoais coletados por outras áreas da companhia; (ii) por outras empresas (dentro e fora do grupo empresarial a qual pertencem); e (iii) e quais as áreas e/ou empresas em questão.

Incidentes, Falhas e Fragilidades: Notificar imediatamente o Encarregado/DPO a ocorrência de qualquer incidente, falha ou fragilade que possa acarretar em risco ou dano.

Fluxo de Atendimento aos Titulares: Coordenar com o Encarregado/DPO o fluxo de atendimento aos Titulares para as solicitações que chegarem à companhia diretamente pela área.

Tratamento de Dados de Colaboradores

Garantir que a área receba apenas os dados estritamente necessários ao desenvolvimento das atividades e que sejam utilizados exclusivamente para a finalidade que foram coletados, inclusive dados de colaboradores terceirizados.

A Equatorial deverá orientar e instruir os terceiros operadores a respeito da realização do Tratamento de Dados Pessoais em nome da Equatorial, e verificar se o Tratamento dos Dados Pessoais está de acordo com as instruções e respeitando as obrigações de confidencialidade e medidas de segurança aplicáveis.

Dados Pessoais de Ex-Colaboradores: Submeter ao Encarregado/DPO e estabelecer, em conjunto com o Comitê, critérios para tempo de guarda e forma de armazenamento dos documentos de ex-colaboradores. Os critérios devem prever inclusive a verificação pela Equatorial

da guarda dos documentos em arquivos de terceiros.

Dados Pessoais de Candidatos: Submeter ao Encarregado/DPO e estabelecer, em conjunto com o Comitê, critérios para eliminação de dados desnecessários (currículos) com alguma periodicidade. Caso seja realizada verificação de antecedentes ou algum procedimento do gênero (*background check*) antes da contratação, é importante a adoção de medidas preventivas (este Tratamento deverá ser enquadrado como legítico interesse e, portanto, a área deverá preencher e entregar ao Encarregado/DPO documento de controle específico referente ao Tratamento).

Administradores: Deve-se indicar preferencialmente o endereço comercial dos administradores e evitar informar o endereço residencial, bem como qualquer Dado Pessoal que não seja estritamente necessário nos documentos públicos (atas, procurações). Da mesma forma, as cópias dos documentos devem ser compartilhados na medida em que sejam estritamente necessários.

Tratamento de Dados de Crianças e Adolescentes

Levando em consideração a natureza das atividades do grupo Equatorial, atualmente os Dados de Crianças e Adolecentes são coletados pela companhia apenas no Departamento Pessoal, exclusivamente para fins de execução dos contratos de trabalhos e cumprimento de obrigações legais relacionadas aos empregados e seus dependentes/benficiários.

É necessário obtenção de termo de consentimento por escrito de pelo menos um dos pais ou do responsável legal (deverá ser incluído no kit-contratação e colaboradores com contratos ativos também devem assinar).
Caso a coleta de Dados de Crianças e Adolescentes surgir em contexto diverso do apontado acima, a coleta somente poderá ser realizada após a autorização do Encarregado/DPO.

Tratamento de Dados Sensíveis

Os dados sensíveis, de acordo com a LGPD, são dados que podem sujeitar o Titular a algum tipo de discriminação. São eles dados 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.

Deve-se verificar se existe obrigação legal ou regulatória para realizar determinado tratamento de Dados Sensíveis, e caso não haja, obter o consentimento específico do Titular em questão para a finalidade que foram coletados.

Ainda, em relação às informações de saúde, devem ser observadas com maior critério condutas adequadas, tais como bloqueio de computadores ao sair da mesa, utilizar impressoras privadas ou com acesso por senha, guardar documentos físicos, atestados e prontuários médicos em armários com chave, sempre verificar os destinatários das mensagens antes de compartilhar os dados, evitar compartilhar dados e informações por plataformas que não tenham requisitos de segurança.

No que diz respeito aos dados biométricos, a relação entre a Equatorial e seus Operadores (inclusive licença de software) deverá ser regulada por meio de contrato que contenha cláusulas específicas de proteção de Dados Pessoais, estabelecendo a posição e responsabilidades das partes.

Tratamento de Dados de Consumidores

Deve-se observar que muito embora a aplicação de legislação específica (LGPD), a relação é regulada pela Lei nº 8.078/1990, o Código de Defesa do Consumidor, que dipõe sobre o direito à efetiva prevenção e reparação de danos ao consumidor.

Contudo, diversas questões relacionadas à privacidade e proteção de dados de consumidores não se enquadram no Código de Defesa do Consumidor, como a transparência sobre as modalidades de coleta, a finalidade e utilização de Dados Pessoais e nesse contexto, ressalta-se a importância do consentimento e da prestação de contas a partir de padrões e práticas que garantam efetivamente o cumprimento dos direitos dos Titulares pela Equatorial.

No Tratamento de Dados Pessoais dos seus Consumidores a Equatorial, em conjunto com o Comitê, deverá cumprir suas responsabilidades como Operador, e estabelecer critérios claros e objetivos para o compartilhamento com terceiros, em especial com os sistemas de proteção ao crédito e com o poder público.

Tratamento de Dados Relacionados a Contratos em Geral

Caso exista algum compartilhamento externo de informações pela área, verificar se os contratos celebrados com esses terceiros contêm cláusulas de proteção de dados.

Compartilhamento de Dados Pessoais com o Poder Público

Tendo em vista que o poder público está sujeito às normas da LGPD, e considerando os princípios da transparência e da prestação de contas, para que seja possível a Equatorial posteriormente demonstrar o atendimento aos direitos dos Titulares, o compartilhamento de Dados Pessoais pela Equatorial com pessoas jurídicas de direito público deverá observar os seguintes critérios:

(i) Comunicação imediata ao Encarregado/DPO na ocorrência de qualquer solicitação; e

(ii) As solicitações deverão ser formais, por escrito, indicando a finalidade para qual se destinam os Dados Pessoais, conforme disposto no artigo 23, I da LGPD.

Diretrizes Básicas para as Áreas Realizarem o Tratamento de Dados Pessoais

Tendo em vista os Fundamentos Legais utilizados pelas áreas para realizar o Tratamento de Dados Pessoais em suas atividades cotidianas, listamos abaixo as diretrizes básicas que os Colaboradores de cada área deverão seguir para que o Tratamento seja realizado conforme as disposições da LGPD:

1. EQUATORIAL, DISTRIBUIDORAS, 55 SOLUÇÕES, INTESA E SPES 1 A 8

Área	Abrangência	Fundamentos Legais e Providências Necessárias	Pontos de Atenção para Cada Área
RH	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obtenção do termo de consentimento: Certificar que a área está obtendo os consentimentos necessários..	1) Área afirma que não realiza *background check* antes da contratação: caso algum procedimento do gênero seja feito, é importante a adoção de medidas preventivas. 2) Contratos: toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. A área deverá instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.

		3) Cumprimento de obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal.	3) Dados de crianças e adolescentes: obtenção de termo de consentimento (deverá ser incluído no kit-contratação e colaboradores com contratos ativos também devem assinar). 4) Inclusão de cláusulas contratuais nos contratos de trabalho que protejam as Empresas de quaisquer denúncias de violação à LGPD. 5) Dados Sensíveis: verificar se existe obrigação legal ou regulatória para realizar determinado tratamento de dados sensíveis e, caso não haja, obter o consentimento específico. Sempre que possível, anonimizar esse tipo de informação. 6) Inexistência de uma regra de eliminação de dados desnecessários. 7) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 8) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. 9) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 10) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais.
	55 Soluções	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que	1) Área afirma que não realiza *background check* antes da contratação: caso algum procedimento do gênero seja feito, é importante a adoção de medidas preventivas para evitar riscos.

		o mesmo possui cláusulas de proteção de dados pessoais. 2) Obtenção do termo de consentimento: Certificar que a área está obtendo os consentimentos necessários. 3) Cumprimento de obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal.	2) Contratos: toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. A área deverá instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 3) Dados de crianças e adolescentes: obtenção de termo de consentimento (deverá ser incluído no kit-contratação e colaboradores com contratos ativos também devem assinar). No caso do menor aprendiz, o responsável legal também deve assinar um termo de consentimento especifico. 4) Dados de colaboradores: inclusão de cláusulas contratuais nos contratos de trabalho que protejam as Empresas de quaisquer denúncias de violação à LGPD. 5) Dados sensíveis: a área afirma que não realiza tratamento de dados sensíveis. Caso algum tratamento seja feito, é importante verificar se existe obrigação legal ou regulatória para realizar determinado tratamento e, caso não haja, obter o consentimento específico. Sempre que possível, anonimizar esse tipo de informação. 6) Inexistência de uma regra de eliminação de dados desnecessários. 7) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 8) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. 9) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos

			os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 10) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais.
Jurídico	Geral – Contratos	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal. 3) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo.	1) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento. 2) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 3) Inexistência de uma regra de eliminação de dados desnecessários. 4) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 5) Contratos: toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. Cada área deverá instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 6) Em caso de compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade.

	Geral – Tributário	1) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal. 2) Exercício regular de direitos em processo judicial, administrativo ou arbitral: Identificar qual o processo judicial, administrativo ou arbitral e avaliar se a informação de fato é necessária.	1) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade. 2) Dados pessoais armazenados em planilhas: armazenamento considerado inseguro, pois pode ter suas informações vazadas facilmente. 3) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando não for possível compartilhar as informações por sistemas, compartilhar arquivos de Word e Excel criptografados com senha e incluir avisos de privacidade. Evitar utilizar mídias portáteis como CD ou *pen drive* e quando estritamente necessário ao cumprimento de determinações específicas, criptografar com senha e incluir aviso de privacidade. 4) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 5) Inexistência de uma regra de eliminação de dados desnecessários. 6) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 7) Contratos: toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.

	Equatorial Maranhão	1) Exercício regular de direitos em processo judicial, administrativo ou arbitral: Identificar qual o processo judicial, administrativo ou arbitral e avaliar se a informação de fato é necessária. 2) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo.	1) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade. 2) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento. 3) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 4) Inexistência de uma regra de eliminação de dados desnecessários. 5) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 6) Contratos: toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 7) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade.
	Equatorial Piauí	1) Exercício regular de direitos em processo judicial, administrativo ou arbitral: Identificar qual o processo	1) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade.

		judicial, administrativo ou arbitral e avaliar se a informação de fato é necessária. 2) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo.	2) Contrato com a SERASA S.A.: análise da regularidade do compartilhamento, adotar medidas preventivas e sempre manter o controle do tratamento. Incluir cláusulas de proteção de dados pessoais. 3) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 4) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento. 5) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade emquestão. 6) Inexistência de uma regra de eliminação de dados desnecessários. 7) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 8) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade.
	Equatorial Pará	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que	1) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento.

		o mesmo possui cláusulas de proteção de dados pessoais. 2) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal. 3) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo. 4) Exercício regular de direitos em processo judicial, administrativo ou arbitral: Identificar qual o processo judicial, administrativo ou arbitral e avaliar se a informação de fato é necessária.	2) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 3) Inexistência de uma regra de eliminação de dados desnecessários. 4) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 5) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade. 6) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 7) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade.
	Equatorial Alagoas	1) Exercício regular de direitos em processo judicial, administrativo ou arbitral: Identificar qual o processo judicial, administrativo ou arbitral e avaliar se a informação de fato é necessária.	1) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade.

		2) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo.	2) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento. 3) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade emquestão. 4) Inexistência de uma regra de eliminação de dados desnecessários. 5) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 6) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 7) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade.
Regulatório	Geral	1) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal.	1) Tratamento baseado em obrigação legal: é importante verificar se os compartilhamentos estão de fato baseados nesta hipótese legal, especialmente as solicitações feitas por meio de ofícios. 2) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade.

			3) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 4) Inexistência de uma regra de eliminação de dados desnecessários. 5) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários.
Financeiro	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo.	1) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade. 2) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento. 3) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 4) Inexistência de uma regra de eliminação de dados desnecessários. 5) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 6) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.

			7) Avaliar necessidade de obter consentimento para compartilhamento dos dados com instituição financeira. 8) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade. 9) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha e utilizar avisos de privacidade.
Rel. com o Cliente	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais.	1) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam devem estar envolvidos diretamente na atividade em questão. 2) Inexistência de uma regra de eliminação de dados desnecessários. 3) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 4) Instruir os funcionários da área para que tenham entendimento sobre os cuidados necessários com os dados pessoais e verifiquem medidas técnicas e requisitos de segurança aplicáveis. 5) Incluir os consentimentos necessários e verificar medidas técnicas e requisitos de segurança aplicáveis a cada canal de atendimento (revisar os formulários e documentos semelhantes já utilizados pela companhia).

			6) Observar os roteiros de atendimento aplicáveis a cada canal de atendimento. 7) Quando o atendimento for por Whatsapp: (i) garantir que os titulares recebam um "opt-in" para autorizar a Equatorial tratar os seus dados pessoais para as finalidades pretendidas e que o atendimento siga o roteiro adequado; e (ii) garantir que o dispositivo que irá receber os dados pessoais dispõe das configurações mínimas de segurança exigidas pela Equatorial. 8) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.
Gestão e Controle Operacional	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal.	1) Informações obtidas da base de dados de terceiros (SPC, SERASA, Boa Vista, etc.): verificar como se deu esse recebimento (existe contrato?) e analisar possibilidade de excluir tais informações. 2) Auditoria: verificar se existe contrato com empresas de auditoria. 3) Verificar se existe algum instrumento regulando compartilhamento para a 55 Soluções. 4) Toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. 5) Prestações de serviços que envolvem tratamento de dados pessoais de funcionários de terceiros que prestam serviços nas dependências da Equatorial, devem conter previsões contratuais nesse sentido e o tratamento deverá passar por

			análise para adoção processos adequados de tratamento, caso aplicável. 6) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 7) Inexistência de uma regra de eliminação de dados desnecessários. 8) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 9) Instruir os funcionários da área para que tenham entendimento sobre os cuidados necessários com os dados pessoais e verifiquem medidas técnicas e requisitos de segurança aplicáveis. 10) Verificar necessidade de incluir os consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área (revisar os formulários e documentos semelhantes já utilizados pela companhia). 11) Verificar se os dispositivos que eventualmente irão receber dados pessoais (smartphones) dispõe das configurações mínimas de segurança exigidas pela Equatorial. 12) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.
Desenv. de Fornecedores	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que	1) Confirmar se a área realmente não trata dados sensíveis e dados de crianças e adolescentes.

		o mesmo possui cláusulas de proteção de dados pessoais. 2) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal.	2) Área não informou sobre a realização de *background check* antes da contratação: caso algum procedimento do gênero seja feito, é importante a adoção de medidas preventivas para evitar riscos. 3) Dados pessoais armazenados em planilhas: armazenamento considerado inseguro, pois pode ter suas informações vazadas facilmente. Sempre que possível, coletar ou compartilhar dados pessoais por meio de sistemas ou portais institucionais. Evitar uso de e-mails e Whatsapp. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha. 4) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. 5) Dados de colaboradores terceirizados: inclusão de cláusulas contratuais nos contratos de trabalho que protejam as Empresas de quaisquer denúncias de violação à LGPD. 6) Prestações de serviços que envolvem tratamento de dados pessoais de funcionários de terceiros que prestam serviços nas dependências da Equatorial, devem conter previsões contratuais nesse sentido e o tratamento deverá passar por análise para adoção processos adequados de tratamento, caso aplicável. 7) Inexistência de uma regra de eliminação de dados desnecessários. 8) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 9) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos

			os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 10) Toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. 11) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.
Marketing	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obtenção do termo de consentimento: Certificar que a área está obtendo os consentimentos necessários.	1) Confirmar se a área realmente controla as autorizações para o tratamento de dados de crianças e adolescentes. 2) Programa "Energia em Dia". Sugestões: Aditar contrato com a empresa GMZ para incluir cláusulas de proteção de dados e medidas de segurança adequadas. Instruir e avaliar o prestador, verificar o cumprimento do contrato. Incluir "opt-in" no hotsite. Todos os serviços disponíveis aos usuários devem apresentar um opt-in para o usuário marcar ao acessar autorizando o tratamento de seus dados pessoais para as finalidades pretendidas, bem como informando, que a plataforma é administrada por terceiros. Também reavaliar necessidade de permitir acesso ao sistema. 3) Dados pessoais armazenados em planilhas: armazenamento considerado inseguro, pois pode ter suas informações vazadas facilmente. 4) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Sempre que possível, coletar ou compartilhar dados pessoais por meio de sistemas ou portais institucionais. Evitar uso de e-mails, Whatsapp e permissão de acesso aos sistemas da Equaotiral por terceiros

			(situação verificada com a GMZ). Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha, incluir avisos d privacidade. 5) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 6) Inexistência de uma regra de eliminação de dados desnecessários. 7) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 8) Verificar necessidade de incluir os consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área (revisar os formulários e documentos semelhantes já utilizados pela companhia). 9) Verificar se os dispositivos que eventualmente irão receber dados pessoais (smartphones) dispõe das configurações mínimas de segurança exigidas pela Equatorial. 10) Toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. 11) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas.

Segurança	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal. 3) Legítimo interesse: Preencher a tabela de controle para o interesse legítimo.	1) Confirmar se a área realmente não compartilha informações com terceiros externos, em especial órgãos públicos e observar as hipóteses legais. 2) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais, devidamente formalizadas. Verificar medidas técnicas e requisitos de segurança aplicáveis e incluir avisos de privacidade. 3) Confirmar existência de prestadores de serviços externos, como fonoaudiólogos, engenheiros, ou outras consultorias na área de segurando do trabalho. Esses contratos devem conter cláusulas de proteção de dados pessoais. 4) Toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. 5) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 6) Dados pessoais armazenados em planilhas: armazenamento considerado inseguro, pois pode ter suas informações vazadas facilmente. 7) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e requisitos de segurança aplicáveis. Sempre que possível, coletar ou compartilhar dados pessoais por meio de sistemas ou portais institucionais. Evitar uso de e-mails e Whatsapp. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha.

			8) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 9) Inexistência de uma regra de eliminação de dados desnecessários. 10) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 11) Dados pessoais sensíveis (em especial, informações de saúde): verificar dados coletados e obrigações legais aplicáveis; verificar necessidade de incluir consentimentos dos colaboradores; verificar medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área; revisar os formulários e documentos semelhantes já utilizados pela área; adequar sistemas e arquivos físicos em armários com chave e acesso restrito.
TI	Geral	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obrigação legal: Identificar qual lei/regulamento satisfaz a obrigação legal. 3) Legítimo interesse: Preencher a tabela de controle para o interesse	1) Garantir que os funcionários da área tenham entendimento sobre os cuidados necessários com os dados pessoais e medidas de segurança aplicáveis. 2) Documentar o fornecimento de equipamentos da empresa e verificar as configurações mínimas exigidas, em especial nos dispositivos móveis (smartphones). 3) Dados pessoais armazenados em planilhas: armazenamento considerado inseguro, pois pode ter suas informações vazadas facilmente. Realizar análise técnica acerca da possibilidade de adoção de outra forma de armazenamento. 4) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail e verificar medidas técnicas e

		legítimo.	requisitos de segurança aplicáveis. Sempre que possível, coletar ou compartilhar dados pessoais por meio de sistemas ou portais institucionais. Evitar uso de e-mails e Whatsapp. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha, incluir avisos de privacidade. Realizar análise técnica para verificar formas segura de compartilhamento. 5) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. Análise técnica acerca da limitação de acesso e manutenção do registro das atividades dos usuários, especialmente no caso de terceiros externos (incluindo cópias e eliminações). 6) Inexistência de uma regra de eliminação de dados desnecessários. Análise técnica acerca da possibilidade de adoção de uma regra para eliminação automática. 7) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 8) Verificar necessidade de incluir os consentimentos e medidas técnicas e requisitos de segurança aplicáveis, tanto aos procedimentos da área como da companhia de modo geral. Avaliar sistemas e canais de atendimentos. Revisar os formulários e documentos semelhantes já utilizados pela área. 9) Toda relação com terceiros deve ser formalizada por meio de contrato, com cláusulas padrão de proteção de dados pessoais – relações de controlador/operador ou de 2 controladores. 10) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em

			relação às cláusulas de proteção de dados e medidas de segurança adequadas. Atenção especial aos terceiros envolvidos na manutenção de sistemas críticos da companhia e infraestrutura de TI. 11) Compartilhar internamente apenas os dados necessários para a área que irá recebe-los executar suas atividades. 12) Tratamento baseado no interesse legítimo: verificar se não existe nenhuma outra base legal e, caso não haja, sempre manter o controle do tratamento. 13) Elaborar e manter atualizadas políticas e diretrizes de segurança da informação a serem observadas pela companhia e seus Colaboradores, de forma a preservar adequadamente os ativos de informação e os dados pessoais. Definir critérios para realização de *back-ups* e plano com ações imediatas e contingenciamento de danos em caso de falhas e incidentes, de segurança, em conjunto com o Encarregado/DPO. 14) Definir processos adequados e regras em relação aos acessos em conjunto com as áreas de negócios. Avaliar os sistemas a serem controlados e buscar soluções técnicas e ferramentas adequadas. 15) Utilizar *data room* que atenda os critérios de segurança, técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração. 16) No caso de haver transferências internacionais de dados, verificar as medidas adequadas (servidores). 17) Compartilhamento de dados pessoais com órgãos do poder público ou reguladores, devem ocorrer apenas para cumprimento de obrigações legais e as medidas de segurança aplicáveis.

			18) Verificar constantemente a segurança, o sigilo e a privacidade dos dados, observando condutas adequadas. 19) Prestações de serviços que envolvem tratamento de dados pessoais de funcionários de terceiros que prestam serviços nas dependências da Equatorial, devem conter previsões contratuais nesse sentido e o tratamento deverá passar por análise para adoção processos adequados de tratamento. 20) Comunicar imediatamente o Encarregado/DPO em casos de incidentes de segurança, falhas, ou fragilidades.

2. EQTPREV

Área	**Abrangência**	**Fundamentos Legais e Providências Necessárias**	**Pontos de Atenção para Cada Área**
Área Administrativa	EQTPREV	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obtenção do termo de consentimento: Certificar que a área está obtendo os consentimentos necessários.	1) Dados de crianças e adolescentes: obtenção de termo de consentimento (deverá ser incluído no kit na hora do preenchimento do cadastro). 2) Dados Sensíveis: verificar se existe obrigação legal ou regulatória para realizar determinado tratamento de dados sensíveis e, caso não haja, obter o consentimento específico. Sempre que possível, anonimizar esse tipo de informação. 3) Inclusão de cláusulas contratuais nos contratos em que os colaboradores e demais participantes aderem ao plano de previdência privada.

			4) Dados pessoais armazenados na rede sem restrição de acesso: armazenamento considerado inseguro, pois pode ter suas informações vazadas facilmente. 5) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha. 6) Aditar contratos com terceiros em que há o compartilhamento de dados pessoais (ex. ADITUS): inclusão de cláusulas contratuais que protejam as Empresas de quaisquer denúncias de violação à LGPD. Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 7) Inexistência de uma regra de eliminação de dados desnecessários. 8) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 9) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 10) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 11) Verificar necessidade de incluir consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área. Avaliar sistemas e revisar os

			formulários e documentos semelhantes já utilizados pela área. Adequar sistemas e arquivos físicos em armários com chave e acesso restrito.
Área de Benefício	EQTPREV	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obtenção do termo de consentimento: Certificar que a área está obtendo os consentimentos necessários.	1) Dados de crianças e adolescentes: obtenção de termo de consentimento (deverá ser incluído no kit na hora do preenchimento do cadastro). 2) Inclusão de cláusulas contratuais nos contratos em que os colaboradores e demais participantes aderem ao plano de previdência privada. 3) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha. 4) Aditar contratos com terceiros em que há o compartilhamento de dados pessoais: inclusão de cláusulas contratuais que protejam as Empresas de quaisquer denúncias de violação à LGPD. Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 5) Inexistência de uma regra de eliminação de dados desnecessários. 6) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 7) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão.

			8) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 9) Verificar necessidade de incluir consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área. Avaliar sistemas e revisar os formulários e documentos semelhantes já utilizados pela área. Adequar sistemas e arquivos físicos em armários com chave e acesso restrito.
Área de Contabilidade	EQTPREV	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais.	1) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha. 2) Aditar contratos com terceiros em que há o compartilhamento de dados pessoais: inclusão de cláusulas contratuais que protejam as Empresas de quaisquer denúncias de violação à LGPD. Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 3) Inexistência de uma regra de eliminação de dados desnecessários. 4) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 5) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão.

			6) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 7) Verificar necessidade de incluir consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área. Avaliar sistemas e revisar os formulários e documentos semelhantes já utilizados pela área. Adequar sistemas e arquivos físicos em armários com chave e acesso restrito.
Área de Controle de Riscos	EQTPREV	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais.	1) Compartilhamento de dados pessoais com terceiros: evitar que seja feito por e-mail. Quando for necessário compartilhar arquivos de Word e Excel, criptografar com senha. 2) Aditar contratos com terceiros em que há o compartilhamento de dados pessoais: inclusão de cláusulas contratuais que protejam as Empresas de quaisquer denúncias de violação à LGPD. Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 3) Inexistência de uma regra de eliminação de dados desnecessários. 4) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 5) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão.

			6) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 7) Verificar necessidade de incluir consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área. Avaliar sistemas e revisar os formulários e documentos semelhantes já utilizados pela área. Adequar sistemas e arquivos físicos em armários com chave e acesso restrito. 8) Dados de crianças e adolescentes: verificar necessidade de obtenção de termo de consentimento específico.
Tecnologia da Informação – T.I.	EQTPREV	1) Execução de contrato: Certificar que a relação está formalizada por um contrato e que o mesmo possui cláusulas de proteção de dados pessoais. 2) Obtenção do termo de consentimento: Certificar que a área está obtendo os consentimentos necessários.	1) Aditar contratos com terceiros em que há o compartilhamento de dados pessoais: inclusão de cláusulas contratuais que protejam as Empresas de quaisquer denúncias de violação à LGPD (ex. contrato com o fornecedor do programa Intech). 2) Instruir e avaliar terceiros envolvidos no tratamento de dados pessoais, e manutenção de sistemas críticos. Verificar o cumprimento dos contratos em relação às cláusulas de proteção de dados e medidas de segurança adequadas. 3) Instruir os funcionários da área para que tenham entendimento sobre os cuidados necessários com os dados pessoais e verifiquem medidas técnicas e requisitos de segurança aplicáveis. 4) Inexistência de uma regra de eliminação de dados desnecessários. 5) Avaliar a necessidade de manter determinadas informações sensíveis no “Módulo de Seguridade”, e eliminar dados desnecessários.

			6) Acesso do sistema somente por profissionais que possuem a necessidade de acessar determinados dados pessoais: todos os profissionais que acessam os dados devem estar envolvidos diretamente na atividade em questão. 7) Checar de forma contínua se a área não recebe mais informações e/ou documentos que contém dados pessoais desnecessários. 8) Verificar necessidade de incluir consentimentos e medidas técnicas e requisitos de segurança aplicáveis aos procedimentos da área. Avaliar sistemas e revisar os formulários e documentos semelhantes já utilizados pela área. Adequar sistemas e arquivos físicos em armários com chave e acesso restrito. 9) Dados de crianças e adolescentes e dados sensíveis: verificar critérios de acesso. 10) Documentar o fornecimento de equipamentos da empresa e verificar as configurações mínimas exigidas, em especial nos dispositivos móveis (smartphones). 11) Observar os processos adequados de acordo com políticas institucionais e quando necessário, definir regras em relação aos acessos em conjunto com as áreas de negócios. Avaliar os sistemas a serem controlados e buscar soluções técnicas e ferramentas adequadas.

Augusto Miranda da Paz Júnior
Presidente

Leonardo da Silva Lucas T. de Lima
Secretário