CBL
COMPANHIA BRASILEIRA DE LÍTIO

FICHA TÉCNICA

DIRETOR SUPERINTENDENTE

VINÍCIUS ALVARENGA

DIRETOR INDUSTRIAL

ANTÔNIO CARLOS SANTANA

DIRETOR DE MINERAÇÃO

GLEN CLEUBER LOPES MARQUES

ELABORAÇÃO E REVISÃO

IGOR ALLAN DE MORAIS NASCIMENTO –
COORDENADOR DE TI

COMPANHIA BRASILEIRA DE LÍTIO
PLANTA QUÍMICA
BR. 116 KM 3,5 ZONA RURAL - CEP 39.995-000
DIVISA ALEGRE/MG
MINERAÇÃO
BR. 367 KM 276 ZONA RURAL – CEP 39.600-000
ARAÇUAÍ/MG
ESCRITÓRIO CENTRAL
Rua Trípoli, 92, salas 131 a 134,
13° andar | Vila Leopoldina CEP 05.303-020 | São Paulo – SP

Sumário

MENSAGEM

O Manual de Proteção de Dados para adequação à LGPD - contém orientações e boas práticas de governança de dados, onde surge nesse contexto, elaborado pela CBL – Companhia Brasileira de Lítio, por meio de seu Grupo de Trabalho de LGPD composto pela Alta Direção e Gerência, Coordenador de TI, SGI e em parceria com o escritório de Advocacia Salvoni e Miranda Advogados Associados, responsáveis em conjunto pelo desenvolvimento do seu conteúdo.

"É fundamental que as empresas se estruturem para a escolha das tecnologias e processos mais adequados, conforme seus respectivos modelos de negócio, para que atendam às normas e garantam que as informações sejam tratadas com sigilo e transparência, preservando as marcas, respeitando as pessoas e a privacidade do público consumidor."
Citação: (Nelcina Tropardi, Presidente da ABA e Vice Presidente de Sustentabilidade e Assuntos Corporativos da HEINEKEN)

Por meio deste manual, a CBL viabilizou uma entrega concreta no tocante ao tratamento de dados, com o objetivo de difundir e esclarecer as regras da LGPD, especialmente no que tange a relação direta com os todos os envolvidos na organização.

TRATAMENTO DE DADOS

A LGPD é destinada a todas as operações de tratamento de dados "**pessoais**" abrangendo todo o território brasileiro.

De forma prática e didática, serão encontrados neste Manual de Proteção de Dados adequação à **LGPD** - orientações e boas práticas de governança de dados - os termos e conceitos relevantes para o entendimento da lei, as bases previstas pelas novas diretrizes para o tratamento de dados e os passos a serem observados durante o processo de adequação das organizações.

Ciente da importância da relação ética e responsável com o consumidor, a CBL assume o compromisso pelas melhores práticas para assegurar integridade dos dados tratados. A criação deste documento, assim como o nascimento da LGPD, representa conquista coletiva para os integrantes do time CBL.

TERMOS E CONCEITO

Titular: É a pessoa física ou jurídica a quem um dado pessoal se refere.

Dado pessoal: é qualquer informação relacionada a uma pessoa física identificada ou identificável, RG, CPF, endereço, data de nascimento são alguns exemplos de dados pessoais, mas informações como hábitos de consumo e outras informações semelhantes, quando relacionadas a uma pessoa física identificada ou identificável, são considerados "dados pessoais". Da mesma forma, informações sobre navegação na internet, como endereço IP e cookies, entre outras, são em geral consideradas como dados pessoais sempre que for possível identificar a pessoa relacionada a essas informações.

Dado pessoal sensível: É o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. A lei traz exigências adicionais e impõe algumas restrições para o tratamento de dados sensíveis.

Dado anonimizado e pessoa identificável: dado anonimizado é o oposto de dado pessoal, ou seja, é o dado que não pode ser associado a um indivíduo. É importante notar que ainda que um dado não esteja direta e explicitamente associado a uma pessoa identificada, ele pode ser considerado um dado pessoal (e não anônimo) sempre que for possível associá-lo a um indivíduo utilizando os meios técnicos disponíveis na ocasião.

Atribuições: Qualquer setor que faça um levantamento estatístico que não precise declarar quem.

DPO: Encarregado de Dados

MEIOS TECNICOS RAZOÁVEIS E DISPONÍVEIS:

A LGPD não estabelece de maneira especifica quais padrões, meios técnicos ou processos devem ser aplicados para que os dados sejam considerados suficientemente anonimizados
A interpretação sobre o que deve ser considerado “meio técnico razoável” em cada cenário será feita pela Autoridade Nacional de Proteção de Dados e a **LGPD** indica apenas que a autoridade deve considerar fatores objetivos, tais como custo e tempo necessários, considerando as tecnologias disponíveis e utilização exclusiva de meios próprios.

TRATAMENTO DE DADOS

É toda operação realizada com dados pessoais – da coleta ao descarte, incluindo o mero armazenamento. A **LGPD** menciona expressamente diversos outros exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Atribuições: Departamento de Pessoal, Financeiro, Fiscal, Expedição, SESMT, Medicina, Almoxarifado, Produção, SGI e Laboratório.

PRINCIPIOS GERAIS E MELHORES PRÁTICAS

A LGPD estabelece alguns princípios que se aplicam a todas as atividades de tratamento de dados.
São valores gerais que orientam a compreensão, interpretação e aplicação das regras estabelecidas pela LGPD e que devem sempre ser considerados quando uma atividade envolver tratamento de dados pessoais.
Entre os princípios mais relevantes estão os seguintes:

a) Princípios da Finalidade, Adequação, Necessidade

De acordo com esses princípios, dados pessoais só devem ser coletados e tratados para os propósitos específicos e legítimos que tenham sido informados ao titular de dados e sejam compatíveis com o contexto do tratamento. O tratamento deve ser limitado ao mínimo necessário para aquelas finalidades que foram informadas aos titulares.

Isso significa que antes de coletar, armazenar ou de qualquer maneira utilizar dados pessoais, é importante verificar:

- Se o titular daqueles dados foi informado de maneira clara e específica sobre como os dados serão tratados e para quais finalidades – o porquê do tratamento;

- Se o tratamento é adequado ao contexto em que os dados foram coletados, ou seja, às expectativas que o titular de dados tinha ao fornecer os seus dados ou torná-los disponíveis; e

- Se é realmente necessário tratar aqueles dados para atingir aquela finalidade.

b) Princípios da Transparência, Livre acesso

É importante garantir que os titulares de dados pessoais tenham acesso a informações claras e facilmente acessíveis sobre como seus dados são tratados, por quem e para quais finalidades.

Isso pode ser feito de diversas maneiras, conforme a natureza do tratamento. Uma recomendação é sempre utilizar linguagem clara, objetiva, sucinta e específica nas políticas de privacidade ou em outros materiais semelhantes, e facilitar o acesso a esses materiais para os titulares de dados.

Além disso, é também necessário oferecer um canal de comunicação acessível para que os titulares de dados possam esclarecer suas dúvidas e solicitar informações.

c) Princípios da Segurança e Prevenção

Ao tratar dados pessoais, é importante implementar medidas técnicas e administrativas capazes de proteger esses dados de acessos não autorizados, perda, destruição, alteração, ou divulgação indevida, bem como prevenir quaisquer incidentes que possam causar danos aos titulares de dados. Isso pode incluir, por exemplo, controles de acessos, técnicas de criptografia, revisão de arquitetura de sistemas, separação de bancos de dados, entre outros.

Atualmente são utilizados sistemas de auditoria “DLP – Software para analise, auditoria e controle de acesso a dados”, identificando o usuário no ato da solicitação da informação, se fez somente uma consulta, exclusão ou transmissão.

Conforme nosso **Manual de Segurança da Informação** são aplicadas também restrições de acesso somente ao setor que destina uma informação.

d) Princípio da Não discriminação

O tratamento de dados pessoais não deve ser realizado para fins discriminatórios, ilícitos ou abusivos.

e) Principio da finalidade

Todo dado tratado deve ter uma finalidade e é vedado a coleta de dados de forma demasiada sem que haja fundamento para a coleta.

MELHORES PRÁTICAS

Clareza e objetividade são essenciais

Procure sempre oferecer informações de forma simples e direta, evitando ambiguidades e termos muito técnicos em seus documentos e políticas.

Flexibilidade

Sempre que possível, dê liberdade para o usuário concordar ou não com o fornecimento de seus dados pessoais e gerenciar suas escolhas de privacidade, preferencialmente por meio de painéis de controle (dashboards) ou ferramentas similares. Não deixe as checkboxes pré-marcadas. Não colete dados excessivos ou desnecessários.

Seja disponível

Crie um canal de atendimento e de comunicação para que os usuários entrem em contato de maneira fácil e simplificada para tirar dúvidas sobre o tratamento de dados pessoais. Este canal está disponível no site através do endereço LGPD | CBL (cblitio.com.br) e com os DPO´s das unidades.

Impactos nas rotinas operacionais

Os direitos e as obrigações estabelecidos pela **LGPD** requerem a revisão, e adequação de diversas rotinas operacionais das empresas. Por exemplo, a **LGPD** estabelece que os titulares de dados possam solicitar o acesso aos dados pessoais mantidos pelas empresas, bem como a revisão dos seus respectivos perfis pessoais ou de consumo que tenham sido formados com base em tratamento automatizado de dados (p.ex. por meio de códigos). Será também necessário estabelecer rotinas para a exclusão de dados mediante revogação do consentimento do titular ou

de dados que não servem mais à finalidade para a qual foram originalmente coletados “exceção de período mínimo estabelecido por lei”.

Consentimento

Todo tratamento deverá ter o consentimento e descrever como e aonde serão utilizadas.

.

Em casos de alteração do tratamento dos dados deve ser requerido ao titular um novo aceite “consentimento”, desde que os dados sejam utilizados para um fim específico de acordo com o novo requisito.

Imagens em circuito de TV não é necessária uma autorização, porém se utilizado o mesmo deve estar identificado para que a pessoa tenha conhecimento que o ambiente é monitorado

Imagens, para que seja feita a autorização do uso de imagens, esta deve estar previamente informada no **FO-TI-DA-008** Termo de consentimento para Tratamento de dados pessoais. O operador de dados deve ter uma lista de controle para informar as áreas quem autoriza / não autoriza o uso de imagens.

Tratamento sem o consentimento do Titular

A **LGPD** algumas hipóteses em que é possível tratar dados pessoais sem obter o consentimento do titular. No caso específico da CBL são:

- **Cumprimento de obrigação legal ou regulatória**: se uma lei ou uma regulamentação setorial exige determinada atividade de tratamento de dados, não é preciso solicitar a autorização do titular de dados. É o caso, por exemplo, de registros de acesso a aplicações online para cumprir com as obrigações de retenção previstas no Marco Civil da Internet, legislação que exige que os últimos seis meses de atividade do usuário sejam registrados pelas empresas que oferecem funcionalidades online.

- Para atender aos **interesses legítimos** da empresa responsável pelo tratamento ou aos interesses legítimos de terceiros, desde que o tratamento de dados não ofereça um risco importante aos direitos e liberdades fundamentais dos titulares de dados.

Dados de crianças e de adolescentes

O tratamento de dados pessoais de crianças (menores de 12 anos) só pode ser realizado com o consentimento específico e destacado de um dos pais ou do responsável legal.

O tratamento destes dados deve obedecer ao critério que enquanto tiver um propósito como por ex.: Se a empresa concede auxílio creche ou salário família, não será permitido ter estes dados guardados se não tiver finalidade ou uso. No caso de desligamento de um empregado, se o dado do dependente não tiver finalidade legal, deve ser eliminado do sistema ficando somente as informações necessárias.

Contratos entre Fornecedores e Clientes

No caso de contratos entre clientes e fornecedores, havendo a necessidade de informação de dados pessoais dos representantes, fica a CBL responsável por este tratamento, garantindo assim a integridade, segurança e confidencialidade dos representantes. O tratamento e guarda não excederá o prazo do contrato acrescido de 03 (três) anos. Será inserida cláusulas padrões firmando a manutenção da LGPD conforme anexo

LGPD na prática

Cada unidade possui sua equipe onde eles serão os responsáveis pela manutenção, segurança e tratamento dos dados

Equipe	DA	AR	SP
Controlador de Dados	Igor Allan de Morais Nascimento		
Enc. de Dados	José Nailza Ribeiro Pereira	Jader Valverde Júnior	Simone Cardoso
Operadores	Colaboradores que trabalham na recepção de dados “Dep. de pessoal”, “Financeiro”, “Fiscal, Medicina, SESMT e Administrativo”		

Guarda de dados

RH: Sistemas e planilhas;
Financeiro/Fiscal: Sistema e planilhas;
SESMT/ Medicina do Trabalho: Sistema e Planilhas
Produção: Sistema e Planilhas
SGI: Planilhas
Administrativo: Sistema e Planilhas
Todos os sistemas e planilhas, são arquivados em servidor de posse da CBL e mantidos em nuvem as copias de segurança. Exceção aos dados do cadastramento de funcionários que é mantido em servidor CLOUD.

Fica o controlador com acesso geral às estruturas criadas em modo somente leitura.
Não é permitido o acesso ao conteúdo das informações, somente à parte de registro de segurança e auditoria.

Mapa de dados

Dados Pessoais		Depto Pessoal	Medicina	SESMT Seg Trabalho	Demais setores
	Nome completo	x	x	x	x
	Data de Nascimento	x	x	x	
	Número da carteira de identidade (RG)	x	X	x	
	Número do Cadastro de Pessoas Físicas (CPF)	x	x	x	
	Número da Carteira Nacional de Habilitação (CNH) *	x		x	
	Fotografia 3x4	x		x	
	Estado civil	x	x	x	
	Dependentes	x			
	Nível de instrução ou escolaridade	x	x	x	
	Endereço completo	x	x	x	x
	Telefone, WhatsApp e endereços de e-mail – informação opcional	x	x	x	x
	Dados bancarios (Banco, agência e número de conta bancária)	x			
Tempo de guarda		30 anos	30 anos	20 anos	05 anos

*A guarda de dados não relacionadas na tabela acima como fichas de registro de acesso a visitantes dentre outros documentos, estão descritos no **IT-SGI-DA-002** – ANEXO I TABELA DE TEMPORALIDADE.

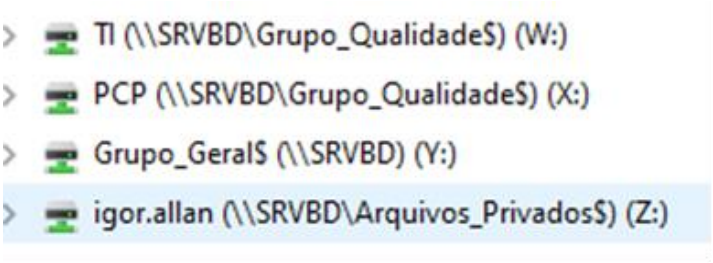
Dados pessoais:
Nome, CPF, RG, carteira de habilitação, passaporte, número de telefone, endereço, e-mail, IP, data de nascimento

Dados sensíveis:
Convicção religiosa, condição de saúde, origem racial ou étnica, vida e orientação sexual, filiação a sindicato ou à organização política, crenças de ordem religiosa ou filosófica e aspectos biométricos ou genéticos.

Exclusão
Os dados serão excluídos dos sistemas quando findar o período de guarda legal ou definição interna da empresa e deverá ser documentada a eliminação dos dados.

Compartilhamento
Identifica-se como compartilhamento de informações o uso de dados pessoais em diferentes setores para o cumprimento do trabalho e apresentado o mapa acima no termo de consentimento.
Apenas o dado pertinente para o andamento do trabalho deve ser compartilhado.

Controle de Acesso
Os dados em mídia digital são alocados por nível de acesso onde somente as pessoas autorizadas para cada setor tem acesso para tratamento dos dados
No caso de compartilhamento com outros setores, são enviados arquivos eletrônicos ou ambos os setores possuem unidade compartilhada entre eles.



Um usuário ou grupo de trabalho tem a unidade privada ou compartilhada Z: a unidade de Grupo Público é uma unidade de compartilhamento entre todos os usuários e não deve ser utilizada para guarda de documentos com informações ou dados pessoais e sim para compartilhamento de arquivos.
São aplicadas as regras de controle de acesso garantindo que somente o setor interessado, possa fazer consultas e/ou alterações nos documentos.

Segurança

USB, Antivírus, Backup monitorados, informados e descritos no Manual de Segurança da Informação.

Vazamento de Dados

Caso ocorra algum tipo de vazamento, deverá imediatamente o **Encarregado de Dados** comunicar a **ANPD** (Autoridade Nacional de Proteção de Dados) e internamente identificar o provável local/setor onde ocorreu o vazamento junto com o Controlador. Utilizar os sistemas de auditoria para verificar os últimos acessos. Identificando origem, notificar o setor e caso identificado o colaborador que fez a divulgação dos dados, este poderá ser demitido por justa causa. No caso de algum colaborador tentar forjar um vazamento e identificado esta finalidade, ele poderá também ser demitido por justa causa.
Em qualquer situação de apuração, a **ANPD** deverá ser notificada.

Governança e boas práticas

Para com os titulares sempre existirá um canal de comunicação livre onde eles possam fazer suas solicitações a respeito do tratamento de seus dados. Para tanto existe em nosso site um canal de acesso a LGPD onde os termos, manual e procedimentos posam em ser acessados e um canal direto através de um formulário eletrônico https://www.cblitio.com.br/cópia-contato-1.
A Companhia Brasileira de Lítio mantém internamente os dados sob sigilo, onde somente os autorizados de cada setor podem fazer uso destas informações. Regras de acesso aos dados e políticas de acesso são constantemente revisadas para garantir tanto a segurança quanto o acesso a quem deve tratar estes dados.
Foram implantados sistemas de segurança “ESET ENDOPINT ANTIVÍRUS, SAFETICA DLP – PROTEÇÃO CONTRA VAZAMENTO DE DADOS e AUDITOR DE CONTEÚDO WEB” de auditoria em tempo real, onde os dados são categorizados em seu conteúdo e os gestores e encarregado de dados, podem avaliar se os operadores estão fazendo uso correto das informações cedidas.
Foi eleito um **comitê de proteção de dados**, composto pelos DPO´s das unidades.

O DLP tem como objetivo monitorar as ações gerais de como os dados são transitados na empresa. Caso ocorra algum vazamento, mesmo que interno entre setores, a ferramenta emitirá os alertas tanto ao setor de TI para averiguação como aos gestores e encarregado de dados ou ao comitê.

Estas ações são descritas no relatório de impacto a proteção de dados, onde a planilha mestre de risco mostra o impacto ao titular em caso de vazamento.

Como medida preventiva caso algum dado saia através da rede lógica o gestor do setor, TI e Encarregado de dados é comunicado no ato e caso a categorização seja um dado sensível e o destino não esteja na lista de compartilhamentos de dados mostrada no fluxo de dados o bloqueio do operador é realizado no ato para averiguação.

Nenhuma entidade que não esteja devidamente levantada poderá receber dados sem um termo de confidencialidade e proteção previamente ajustados.

Mensalmente relatórios são emitidos para mostrar a eficácia das plataformas de segurança internas.

No caso de um vazamento assim que identificado, o primeiro passo é comunicar o encarregado de dados, Agencia Nacional de Proteção e o titular dos dados. Em seguida serão analisados os logs´s dos sistemas DLP, Auditor interno Windows e externo “controle de acessos” a fim de verificar a origem e o último usuário que fez uso dos dados pessoais vazados. Com este levantamento a informação será categorizada conforme o relatório de impacto tendo os graus baixo impacto, médio impacto e alto impacto.

Independente do grau de risco a tratativa interna sempre será a mesma “comunicar as partes envolvidas, rastrear a informação nos sistemas de proteção, bloquear o operador – “até finalizar o processo”, aplicar as medidas protetivas, verificar impacto e prestar esclarecimentos e/ou comunicados aos órgãos pertinentes.

Internamente a empresa possui dispositivos de recuperação de dados, Backup para restaurar alguma informação “descrito no Manual de Segurança da Informação” e equipamentos reserva para impedir a interrupção das operações de tratamento de dados “nobreaks, servidor”. O acesso ao CPD é controlado e o uso de unidades removíveis é bloqueada como política de segurança.

Caso seja identificado o vazamento, deve-se verificar com a ANPD as penas cabíveis, seja multa, medida disciplinar ou qualquer outro tipo.

Caso o vazamento não tenha ligação com a empresa, os envolvidos serão notificados sendo informados que não houve vazamento, devendo ser de outra origem.

Em caso de identificação de falhas dos sistemas, os operadores devem comunicar ao encarregado de dados e o mesmo em conjunto com o comitê e setor de TI, averiguar as falhas e solicitar a correção seja dos aplicativos ou de ordem interna nas políticas de acesso.

É de fundamental importância o bom envolvimento dos agentes de dados, seja encarregado, operador ou controlador. Receber as solicitações diversas dos titulares “correção, exclusão ou qualquer outra” deve ser encaminhado ao setor onde o operador e o encarregado darão um prazo para resposta a solicitação e este não sendo superior a 48 horas em dias úteis.

Da coleta, respeitar o consentimento explícito do titular e nunca utilizar para uso além do que está discriminado no consentimento.

Em caso de menores de 12(doze) anos, é necessário um termo constante no termo geral de uso e consentimento de dados, onde apenas o responsável legal, poderá fornecer as informações do menor.

No uso destas informações no setor de medicina, onde é permitido o atendimento aos dependentes, é de livre acesso a estes dados por parte do titular/responsável legal, mediante solicitação formal. O tratamento a respeito da segurança é o mesmo dado internamente.
Fica o setor como apoio as demais áreas quando da realização de relatórios que possam conter dados pessoais ou relatórios de agregação de informações. A avaliação é em caráter geral e não da elaboração de documentos.

Política de Proteção de Dados e Privacidade

O Programa de Proteção de Dados e Privacidade da CBL reflete sua cultura de integridade, associada a importância atribuída ao cumprimento da legislação aplicáveis às atividades desenvolvidas.

A CBL tem como um de seus valores a manutenção do sigilo e proteção dos dados que são no exercício de suas atividades. As informações tratadas internamente são de cunho profissional e legal e jamais haverá solicitações em excesso. Para isso, serão verificados padrões éticos e morais, bem como as orientações emanadas pela Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”).

O ponto principal desta Política é que a CBL tem como uma de suas principais preocupações o armazenamento e destinação responsável dos dados a ela confiados e a manutenção de uma relação transparente com os titulares dos dados. Dito isso, as unidades envidam seus melhores esforços para estar em conformidade com a **LGPD** e normas de Compliance. Portanto, o tratamento irresponsável de dados pessoais e de terceiros é condenado pela CBL e pelas regulamentações aplicáveis, nacional (“Lei Geral de Proteção de Dados Pessoais, sendo vedado a todos os envolvidos conduzir tais práticas, devendo coibir este tipo de atitude e alertar a área de Compliance caso testemunhem ou tenham legítima desconfiança em relação a irregularidades.

Nosso objetivo é que você, colaborador, saiba como seus dados pessoais são tratados. Priorizamos a transparência nesse sentido e, por isso, caso algo não tenha ficado claro nesta Política, não hesite em tirar suas dúvidas com a área de Compliance ou com o Encarregado de Dados de sua unidade.

Da Coleta

Feita de forma clara e com autorização expressa do titular através de termos, cláusulas contratuais ou eletrônica “para nosso website”.

A base de Dados formada por meio da coleta de Dados é de propriedade e responsabilidade da CBL, sendo que seu uso, acesso e compartilhamento, quando necessários, são feitos dentro dos limites e dos propósitos dos negócios descritos nesta Política.

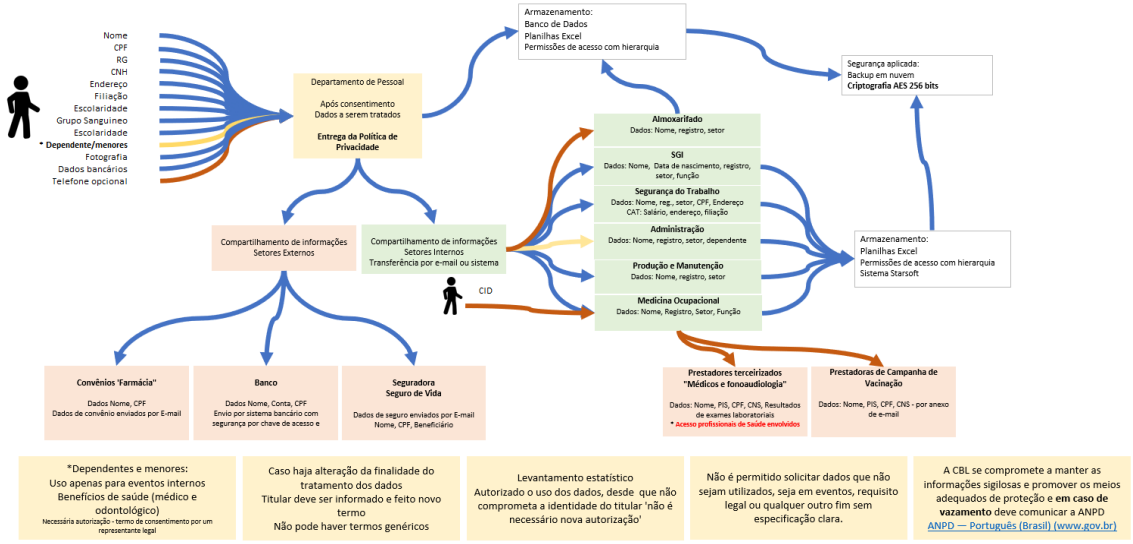
Caso empresas terceirizadas realizem o Tratamento em nome da CBL de quaisquer Dados Pessoais que coletamos, elas devem, obrigatoriamente, respeitar as condições estipuladas e as normas de segurança da informação e sigilo de seus respectivos contratos.

Caso necessite de informações adicionais a respeito do tratamento, uso, descarte, anonimização, exclusão, deve ser encaminhada uma solicitação ao Encarregado de Dados ou DPO.

	DA	**AR**	**SP**
DPO	Nailza Ribeiro Pereira	Jader Valverde Júnior	Simone Cardoso
e-mail	nailza.ribeiro@cblitio.com.br	jader.valverde@cblitio.com.br	simone.cardoso@cblitio.com.br

Fluxo de dados

Na imagem, o fluxo como os dados são trabalhados na CBL e por quais setores passam, bem como, o tipo de segurança aplicada.



Principais Alterações

QUADRO DE CONTROLE DE REVISÕES			
Data	**Revisão**	**Descrição**	**Motivo**
20/10/2020	00	Emissão inicial.	-
09/06/2022	01	Revisão geral - Alteração DPO e Guarda de dados com prestador contábil, inclusão FO-TI-DA-012;	4
29/06/2023	02	Revisão geral	4
24/11/2023	03	Revisão geral	4
29/12/2023	04	Revisão geral	4
09/10/2024	05	Revisão geral	4
Motivo: 1- Atendimento a NC / 2- Incorporação de nova atividade / 3- Alteração de metodologia / 4- Melhoria no processo			

Registros

FO-TI-DA-008 Termo de consentimento para Tratamento de dados pessoais
FO-TI-DA-012 Termo de consentimento para tratamento de dados pessoais (menores 12 anos)

Anexos

Anexo I - Cláusula Padrão para firmar Contratos entre Fornecedores e Clientes;