

GOVERNANÇA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

ÍNDICE

1.	FINALIDADE.....	3
2.	ABRANGÊNCIA.....	3
3.	REFERÊNCIAS.....	3
4.	CONCEITOS.....	4
4.1	ANONIMIZAÇÃO.....	4
4.2	AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD).....	4
4.3	COLABORADOR.....	4
4.4	COLETA MÍNIMA.....	4
4.5	CONSENTIMENTO.....	4
4.6	CONTROLADOR.....	4
4.7	DADO ANONIMIZADO.....	4
4.8	DADO PESSOAL.....	4
4.9	DADO PESSOAL SENSÍVEL.....	4
4.10	DPO (DATA PROTECTION OFFICER) – ENCARGADO PELO TRATAMENTO DOS DADOS PESSOAIS	5
4.11	ELIMINAÇÃO.....	5
4.12	LGPD (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS).....	5
4.13	OPERADOR.....	5
4.14	PRIVACIDADE DESDE A CONCEPÇÃO (<i>PRIVACY BY DESIGN</i>).....	5
4.15	PSEUDONIMIZAÇÃO.....	5
4.16	RIPD (RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS).....	5
4.17	RTD (REGISTRO DE TRATAMENTO DE DADOS).....	5
4.18	SISTEMA DE DEMANDA DE TITULAR DE DADOS (DATA SUBJECT REQUEST – DSR).....	6
4.19	TITULAR.....	6
4.20	TRANSFERÊNCIA INTERNACIONAL DE DADOS.....	6
4.21	TRATAMENTO.....	6
5.	DIRETRIZES.....	6
5.1	ADEQUAÇÃO DE PROCESSOS DE NEGÓCIOS À LGPD.....	6
5.2	ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO.....	6

5.3	BASE LEGAL DE TRATAMENTO DE DADOS.....	7
5.4	COLETA MÍNIMA DE DADOS E CONSENTIMENTO.....	7
5.5	CONSENTIMENTO.....	7
5.6	DIREITOS DOS TITULARES DE DADOS.....	7
5.7	GESTÃO DE INSTRUMENTOS CONTRATUAIS.....	7
5.8	GESTÃO DE INCIDENTES.....	8
5.9	GOVERNANÇA DOS RISCOS.....	8
5.10	SEGURANÇA DA INFORMAÇÃO.....	8
5.11	INVENTÁRIO DE DADOS.....	9
5.12	GOVERNANÇA DE PRIVACIDADE E DADOS PESSOAIS.....	9
5.13	CAPACITAÇÃO E CONSCIENTIZAÇÃO.....	9
5.14	NAVEGAÇÃO NA WEB E COOKIES.....	9
5.15	SISTEMAS DE TECNOLOGIA DE INFORMAÇÃO.....	10
5.16	METODOLOGIA DE PROJETOS.....	10
5.17	ATENDIMENTO A REQUERIMENTOS DO TITULAR DE DADOS PESSOAIS.....	10
5.18	TRATAMENTO DE DADOS PESSOAIS.....	10
6.	COMPETÊNCIAS.....	11
6.1	DIRETORIA EXECUTIVA DA ELETROBRAS ELETRONUCLEAR.....	11
6.2	UNIDADE ORGANIZACIONAL RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO CORPORATIVA	11
6.3	DEPARTAMENTOS DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (ST.A)	12
6.4	UNIDADES ORGANIZACIONAIS DE CONTRATAÇÃO DE BENS E SERVIÇOS.....	12
6.5	UNIDADES ORGANIZACIONAIS RESPONSÁVEIS POR PROCESSOS QUE LEVAM AO TRATAMENTO DOS DADOS PESSOAIS.....	12
6.6	DPO (DATA PROTECTION OFFICER) – ENCARREGADO PELO TRATAMENTO DOS DADOS PESSOAIS	12
6.7	GESTORES DAS UNIDADES ORGANIZACIONAIS.....	13
6.8	COLABORADORES.....	13
6.9	UNIDADES ORGANIZACIONAIS DE GESTÃO DE PESSOAS.....	13
7.	PROCEDIMENTOS.....	14
7.1	TRATAMENTO DE DADOS PESSOAIS.....	14
7.2	DIREITOS/DEMANDAS DOS TITULARES DE DADOS PESSOAIS.....	14
7.3	CONFORMIDADE DE CONTRATOS.....	15
7.4	CONFORMIDADE DE SOFTWARES E SERVIÇOS DE TECNOLOGIA.....	15
8.	DISPOSIÇÕES GERAIS.....	15
	ANEXO 1: FORMULÁRIO RTD.....	17
	ANEXO 2: FORMULÁRIO RIPD.....	26

1. FINALIDADE

Estabelecer diretrizes para a governança de privacidade e de proteção dos dados pessoais, visando à gestão do tratamento de dados pessoais e a sua segurança, no ambiente convencional ou de tecnologia da Eletrobras Eletronuclear, com o propósito de proteger a privacidade de clientes, colaboradores, parceiros e fornecedores.

2. ABRANGÊNCIA

Esta Instrução Normativa se aplica a todas as Unidades Organizacionais da Eletrobras Eletronuclear, em especial, a todos os colaboradores da Eletrobras Eletronuclear que realizem atividades que envolvam, de forma direta ou indireta, o tratamento de dados pessoais.

3. REFERÊNCIAS

A presente Instrução Normativa está fundamentada em:

- Lei nº 12.527/2011, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI) – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;
- Lei nº 12.813/2013 – Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego (Lei de Conflitos de Interesses);
- Lei nº. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) – Dispõe sobre a proteção de dados pessoais e altera a Lei nº. 12.965/2014. Também conhecida como Marco Civil da Internet;
- Lei nº. 13.853/2019 - Altera a Lei nº 13.709/2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados (ANPD);
- Lei nº. 12.965/2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet);
- Decreto nº. 8.771/2016 - Indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações;
- Decreto nº. 9.637/2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
- Política de Gestão de Documentos e Informações Corporativas das Empresas Eletrobras – 2ª Edição – 2017;
- Política de Segurança da Informação das Empresas Eletrobras;
- Plano de Classificação de Documentos das Empresas Eletrobras, aprovado pela Resolução de Diretoria Executiva 497/2019;
- Regulamento de Governança de Privacidade e Proteção de Dados das Empresas Eletrobras;
- Instrução Normativa 14.12 – Tratamento de Incidentes de Segurança da Informação;
- Procedimento Corporativo PC-AG-IN-015 – Tratamento de Incidentes de Segurança da Informação;

4. CONCEITOS

4.1 Anonimização

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

4.2 Autoridade Nacional de Proteção de Dados (ANPD)

Órgão da administração pública federal, responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional.

4.3 Colaborador

Diretores, conselheiros, empregados, contratados, prestadores de serviço, estagiários e jovens aprendizes que atuem na Eletrobras Eletronuclear.

4.4 Coleta mínima

Conceito derivado do princípio da finalidade, que define que a coleta de dados só pode ser realizada com finalidade específica e que esta deve ser informada aos titulares previamente. Desse princípio resulta o da minimização da coleta. Ou seja, a coleta se restringe aos dados necessários para atingir ao fim específico.

4.5 Consentimento

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

4.6 Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

4.7 Dado Anonimizado

Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

4.8 Dado Pessoal

Informação relacionada a pessoa natural identificada ou identificável.

4.9 Dado Pessoal Sensível

Dado sobre origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso, filosófico ou político; referente à saúde ou à vida sexual; e genético ou biométrico, quando vinculado a uma pessoa natural.

4.10 DPO (Data Protection Officer) – Encarregado pelo Tratamento dos Dados Pessoais

Profissional indicado, em cada empresa, para tratar os incidentes relacionados a violação de privacidade ou que gerem danos aos titulares de dados pessoais e para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

O DPO deve ter as qualificações necessárias para exercer a função.

4.11 Eliminação

Exclusão de dado ou de conjunto de dados, armazenados em banco de dados, ou destruição de documentos em suporte físico, independentemente do procedimento empregado.

4.12 LGPD (Lei Geral de Proteção de Dados Pessoais)

Lei nº 13.709/2018, de 14 de agosto de 2018. Disciplina sobre o tratamento de dados pessoais no Brasil.

4.13 Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

4.14 Privacidade Desde a Concepção (*Privacy by Design*)

Metodologia na qual a proteção de dados pessoais é pensada desde a concepção de sistemas, processos, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o tratamento de dados pessoais.

4.15 Pseudonimização

Utilização de meios técnicos por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida, separadamente, pelo controlador, em ambiente controlado e seguro.

4.16 RIPD (Relatório de Impacto à Proteção de Dados Pessoais)

Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas, as salvaguardas e os mecanismos de mitigação de risco.

Em algumas organizações e na literatura especializada, o termo "RIPD" também costuma ser referenciado em sua forma na língua inglesa: "DPIA", que é a sigla para *Data Protection Impact Assessment*.

4.17 RTD (Registro de Tratamento de Dados)

Formulário que o controlador e o operador devem manter com o registro dos processos de tratamento de dados pessoais que realizarem, especialmente no caso de tratamento baseado no legítimo interesse.

4.18 Sistema de Demanda de Titular de Dados (Data Subject Request – DSR)

Sistema pelo qual uma solicitação formal é feita por um titular de dados à empresa, para executar uma ação em seus dados pessoais.

4.19 Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

4.20 Transferência Internacional de Dados

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual a Eletrobras Eletronuclear seja membro.

4.21 Tratamento

Toda operação realizada com dados pessoais, como as que se referem 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.

5. DIRETRIZES

5.1 Adequação de Processos de Negócios à LGPD

As adequações dos processos, inclusive em seus sistemas, formulários e procedimentos, são de responsabilidade das respectivas áreas de negócio e devem contar com apoio técnico do Encarregado pelo Tratamento de Dados Pessoais (DPO).

As adequações dos processos devem ter uma abordagem sistemática que se apoie em padrões e adote condutas de privacidade, de forma proativa e consistente, na aplicação em tecnologias da informação, práticas organizacionais, *design* de produtos ou redes de informação.

5.2 Anonimização e Pseudonimização

Sempre que possível e oportuno, a Eletrobras Eletronuclear pode fazer uso de técnicas de anonimização de dados pessoais, a fim de impossibilitar a associação entre o dado e seu titular, fazendo com que os dados deixem de ser considerados pessoais. A anonimização não pode ser passível de reversão.

A anonimização dos dados pessoais pode ser utilizada para permitir a manutenção dos dados do titular, mesmo após o término da finalidade do tratamento.

Sempre que possível e oportuno, a Eletrobras Eletronuclear pode fazer uso de técnicas de pseudonimização, com o objetivo de minimizar os riscos e danos ao titular, em caso de algum incidente de violação de dados pessoais.

As áreas da Eletrobras Eletronuclear dedicadas ao tratamento de denúncias podem utilizar técnicas de pseudonimização, buscando reforçar as medidas de proteção dos dados de denunciantes, em alinhamento com o disposto no artigo 6º, §4º, do Decreto nº 10.153/2019.

A ouvidoria da Eletrobras Eletronuclear pode usar técnicas de pseudonimização para proteger a identidade de autor de manifestação, conforme previsão do art. 24 do Decreto nº 9.492/2018.

5.3 Base Legal de Tratamento de Dados

O tratamento de dados pessoais, ou seja, a realização de coleta, acesso, exclusão, edição, ou qualquer outra operação, somente deve ser realizada dentro de uma das bases legais dispostas na LGPD.

Quando o tratamento de dados pessoais tiver como base o legítimo interesse do controlador/operador, este deverá ser acompanhado de um RIPD.

5.4 Coleta Mínima de Dados e Consentimento

Os processos que envolvam coleta de dados pessoais deverão ser ajustados pelas unidades responsáveis da Eletrobras Eletronuclear com base no conceito de coleta mínima, com finalidades específicas e obtenção do respectivo consentimento, quando couber.

5.5 Consentimento

No momento da coleta, o titular do dado pessoal deve consentir e ser informado de forma clara e explícita sobre a finalidade, a natureza obrigatória ou facultativa do fornecimento, e sobre as consequências da negativa em fornecê-los. O consentimento poderá ainda ser renovado periodicamente e pode ser revogado a qualquer momento, a pedido do titular. O consentimento só deve ser usado pela Eletrobras Eletronuclear se não houver outra base legal possível para a atividade.

5.6 Direitos dos Titulares de Dados

A Eletrobras Eletronuclear deve dispor, em seu *site*, de página dedicada ao relacionamento com os titulares de dados, contendo, no mínimo:

- a) *link* para a Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras;
- b) identidade e informações de contato do DPO indicado pela empresa;
- c) Sistema de Demandas do Titular de Dados (*Data Subject Request* – DSR);
- d) Sistema de Gerenciamento de *Cookies* do *site*.

Os sistemas dedicados a demandas do titular de dados – DSR, citados, devem estar preparados para que os titulares de dados possam exercer seus direitos previstos nos artigos 18 e 19 da LGPD.

5.7 Gestão de Instrumentos Contratuais

Os contratos, convênios e demais instrumentos contratuais relacionados a atividades que envolvam tratamento de dados pessoais, devem prever de forma explícita em suas cláusulas a responsabilidade do

correto tratamento de dados por parte de terceiros, bem como garantir a realização de diligências, com previsão de “direito de regresso” da Eletrobras Eletronuclear em caso de descumprimento da outra parte.

Os contratos voltados para contratação de mão de obra e/ou para o tratamento de dados pessoais, devem passar pelo Encarregado de Dados Pessoais – DPO, para que esse verifique a necessidade de cláusulas adicionais às cláusulas padrão da Eletrobras Eletronuclear.

5.8 Gestão de Incidentes

A Instrução Normativa 14.12 e o Procedimento Corporativo PC-AG-IN-015 orientam o processo de tratamento e resposta a incidentes de segurança da informação e devem abranger ocorrências que envolvam violação dos direitos dos titulares de dados, a partir de critérios de controle e registro de vazamentos, bem como comunicação aos envolvidos e à ANPD.

Os incidentes relacionados a violação de privacidade, ou que gerem danos aos titulares de dados pessoais, devem ser encaminhados para o DPO, que deve realizar o tratamento de acordo com o Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras, com a Instrução Normativa 14.12 e o Procedimento Corporativo PC-AG-IN-015.

5.9 Governança dos Riscos

Os riscos gerados para a Eletrobras Eletronuclear, em razão da vigência LGPD, devem ser gerenciados e priorizados por meio de eventos e fatores de riscos na Matriz de Riscos da Eletrobras Eletronuclear.

A gestão de riscos para os titulares de dados, gerada a partir dos tratamentos de dados identificados na Eletrobras Eletronuclear, deve utilizar o RTD, que contém identificação, análise e avaliação dos riscos, e o RIPD, que contém as medidas de respostas aos riscos.

Os RTDs e os RIPDs devem ser revisados anualmente, ou sempre que houver qualquer mudança no tratamento do dado pessoal.

Caso os tratamentos sejam baseados no legítimo interesse do controlador/operador, envolvam dados pessoais sensíveis ou ainda gerem riscos às liberdades civis e aos direitos fundamentais do titular, deve ser elaborado o RIPD, com o objetivo de identificar medidas, salvaguardas e mecanismos de mitigação de risco.

Todo RIPD deve ter como anexo o RTD correspondente.

5.10 Segurança da Informação

As medidas contra vazamento de dados, bem como investimentos em ferramentas e processos de segurança, devem priorizar a proteção de dados pessoais sensíveis, bem como daqueles dados cujo tratamento utiliza como base legal, o legítimo interesse do controlador. Cada Unidade Organizacional é responsável por solicitar apoio da área de segurança da informação e do DPO para proteger seus processos envolvendo tratamento de dados pessoais.

5.11 Inventário de Dados

O inventário de dados pessoais da Eletrobras Eletronuclear é realizado por cada Unidade Organizacional que manuseia dados pessoais e deverá ser mantido permanentemente atualizado, identificando os tipos documentais e as informações que esses contêm, visando seu tratamento (incluindo eventual obtenção de consentimento do titular) em acordo com a respectiva base legal, com adoção do conceito de coleta mínima.

Devem constar informações sobre a finalidade, base legal utilizada, compartilhamento de dados, término da finalidade, prazo de manutenção da informação, local de arquivamento, tipos de dados e sistemas utilizados para cada processo de negócio.

O inventário deve ser realizado considerando o contexto de produção ou acúmulo dos documentos e informações, estruturado a partir do Plano de Classificação de Documentos das empresas Eletrobras.

5.12 Governança de Privacidade e Dados Pessoais

O Programa de Governança em Privacidade da Eletrobras Eletronuclear deve ter por objetivo o estabelecimento de relação de confiança com os titulares de dados pessoais, por meio de atuação transparente, com monitoramento contínuo e avaliações periódicas integradas a sua estrutura geral de governança. Deve ser composto por processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

5.13 Capacitação e Conscientização

Devem ser promovidas, de forma continuada, ações educacionais, de capacitação, sensibilização e conscientização sobre as melhores práticas acerca do tratamento de dados pessoais na Eletrobras Eletronuclear bem como a ampla divulgação dos riscos e ameaças da não observância dessas práticas.

Deve ser dada especial atenção ao treinamento de colaboradores que atuam diretamente com o tratamento de dados pessoais, sendo de responsabilidade de cada Unidade Organizacional o direcionamento de seus colaboradores à realização dos treinamentos oferecidos pela Eletrobras Eletronuclear, tanto aqueles disponibilizados na seção especializada da LGPD na Nucweb, como em campanhas de educação e conscientização em proteção de dados pessoais.

As ações de conscientização serão promovidas pela Coordenação de Comunicação Institucional (CI.P), em parceria com o DPO.

5.14 Navegação na Web e Cookies

A Eletrobras Eletronuclear poderá, mediante mecanismos de obtenção e revogação de consentimento dos usuários, utilizar-se de *cookies* e tecnologias semelhantes, visando compreender melhor o comportamento dos usuários, informando quais páginas e conteúdo dos sites foram visitados, contribuindo para a eficácia na distribuição de conteúdo.

5.15 Sistemas de Tecnologia de Informação

Os sistemas de Tecnologia da Informação de suporte a processos e atividades que envolvam tratamento de dados pessoais que forem desenvolvidos ou adquiridos pela Eletrobras Eletronuclear deverão seguir o conceito de *Privacy by Design*.

O DPO deve ser consultado sempre que um novo sistema for implantado na empresa, de maneira a garantir que o sistema atenda aos requisitos legais de privacidade e proteção de dados pessoais.

5.16 Metodologia de Projetos

A metodologia de gestão de projetos da Eletrobras Eletronuclear deverá considerar o conceito de *Privacy by Design*, visando evitar o surgimento de novos processos, atividades, sistemas, práticas, projetos, produtos ou qualquer outra solução que não esteja aderente à LGPD.

Os sistemas de Tecnologia da Informação de suporte a processos e atividades que envolvam tratamento de dados pessoais que forem desenvolvidos ou adquiridos pela Eletrobras Eletronuclear devem seguir o conceito de *Privacy by Design*. Portanto, sua aderência à LGPD e aos instrumentos normativos da empresa deve ser observada desde sua concepção/aquisição.

5.17 Atendimento a Requerimentos do Titular de Dados Pessoais

A Eletrobras Eletronuclear deve desenvolver mecanismos para atendimento aos direitos dos titulares de dados previstos na LGPD, com destaque para confirmação e acesso a dados, retificação, restrição de tratamento, revogação de consentimento e exclusão de dados, sempre observando os impactos e os direitos do controlador.

A Eletrobras Eletronuclear disponibilizará, preferencialmente em seu site na internet, os canais oficiais de recebimento dos requerimentos dos titulares de dados pessoais, apoiando o DPO.

5.18 Tratamento de Dados Pessoais

A identificação dos tratamentos de dados pessoais na Eletrobras Eletronuclear deve ser orientada por processos, tendo como base a Arquitetura de Processos das Empresas Eletrobras, descrita no Caderno Executivo Arquitetura de Processos das Empresas Eletrobras.

As unidades organizacionais devem manter registro das operações de tratamento de dados pessoais que realizam, especialmente no caso de tratamento baseado no legítimo interesse ou quando envolver dados pessoais sensíveis. Tal registro deve se dar por meio do RTD, que deve ser preenchido pelas áreas responsáveis pelas atividades que envolvam tratamento de dados e arquivados pelo DPO da empresa.

Os tratamentos dos dados pessoais devem observar os seguintes princípios: finalidade, adequação, necessidade, qualidade dos dados, transparência, segurança, prevenção, livre acesso, não discriminação, responsabilização e prestação de contas.

Os tratamentos dos dados pessoais podem ser realizados somente mediante enquadramento em uma das bases legais previstas no artigo 7º da LGPD. No caso de dados pessoais sensíveis, deve considerar o rol mais restrito de bases legais, previstas no artigo 11 da LGPD.



Em caso de realização de tratamento baseado no fornecimento de consentimento pelo titular, devem ser observadas as condições para obtenção, previstas no artigo 8º da LGPD: deve ser expresso, claro e destacado de outras cláusulas envolvidas na atividade/serviço, livre de vícios e possuir finalidades determinadas.

O término do tratamento de dados pessoais ocorrerá sempre que a finalidade de tratamento for alcançada, por determinação da ANPD, ou mediante solicitação do titular de dados.

Os dados pessoais devem ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades. Sua manutenção está autorizada para cumprimento de obrigação legal e regulatória, ou mediante anonimização destes, descaracterizando-os enquanto dados pessoais.

Consideram-se para fins de obrigação legal e regulatória os instrumentos de gestão e preservação documental, como os planos de classificação e as tabelas de temporalidade utilizadas pela Eletrobras Eletronuclear.

Quando o tratamento de dados pessoais envolver a obrigação legal de sua difusão em transparência ativa, esses devem ser publicados em formato interoperável e estruturado para o uso compartilhado, em cumprimento ao disposto no artigo 25 da LGPD e previsto no artigo 8º, §3, da Lei nº 12.527/2011, a Lei de Acesso à Informação.

6. COMPETÊNCIAS

6.1 Diretoria Executiva da Eletrobras Eletronuclear

Aprovar esta Instrução Normativa, permitindo a implantação dos requisitos da Política de Proteção de Dados e Privacidade das Empresas Eletrobras.

Indicar e revisar a indicação do DPO da Eletrobras Eletronuclear.

6.2 Unidade Organizacional responsável pela Segurança da Informação Corporativa

São responsabilidades da Unidade Organizacional responsável pelos processos de Segurança da Informação Corporativa:

- a) Apoiar o DPO em suas atribuições;
- b) Coordenar e apoiar metodologicamente a realização do inventário de dados pessoais, a partir de informações fornecidas pelas Unidades Organizacionais da empresa;
- c) Colaborar com a elaboração dos procedimentos para tratamento e resposta a incidentes relativos à privacidade de titulares de dados, de acordo com o Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras.

6.3 Departamentos da Superintendência de Tecnologia da Informação e Comunicação (ST.A)

Garantir a aplicação do princípio *Privacy by Design* nos seus processos de desenvolvimento e especificações técnicas de sistemas, bem como garantir a aplicação das melhores práticas e recursos para segurança dos dados pessoais conforme a seguir:

- a) Assegurar que os sistemas sejam projetados, desde a sua concepção, para que a coleta e o tratamento de dados pessoais estejam limitados ao propósito identificado e declarado;
- b) Garantir o descarte de dados pessoais temporários e dos dados pessoais que estiverem em formato digital, após o término do tratamento;
- c) Garantir a anonimização dos dados pessoais quando necessária sua manutenção para além da finalidade original;
- d) Garantir o controle de acesso aos dados pessoais, bem como primar por sistemas que possam realizar auditoria de *log* e rastreabilidade do fluxo dos dados;
- e) Assegurar a exigência do cumprimento do princípio *Privacy by Design* junto a fornecedores de soluções de Tecnologia da Informação de Comunicação (TIC), prevendo essas condições em Termos de Referências (TR) e editais de licitação.

6.4 Unidades Organizacionais de Contratação de Bens e Serviços

Consultar o DPO sempre que a contratação envolver tratamento de dados pessoais pela Eletrobras Eletronuclear (em nome da contratada), ou pela contratada (em nome da Eletrobras Eletronuclear), de forma a garantir a conformidade por meio de cláusulas contratuais adequadas ao tipo de contrato.

6.5 Unidades Organizacionais Responsáveis por Processos que Levam ao Tratamento dos Dados Pessoais

Todas as Unidades Organizacionais da Eletrobras Eletronuclear que conduzem processos dos quais decorrem a necessidade de tratamento de dados pessoais devem:

- a) Viabilizar ao titular de dados, com apoio dos departamentos da ST.A — quando aplicável — e orientação do DPO, mecanismos que permitam a revogação do consentimento a qualquer momento, mediante manifestação expressa;
- b) Elaborar RTD e RIPD, de acordo com o descrito nesta Instrução Normativa;
- c) Atender às demandas do DPO e da Unidade Organizacional responsável pelos processos de Segurança da Informação Corporativa, acerca dos dados sob sua responsabilidade.

6.6 DPO (Data Protection Officer) – Encarregado pelo Tratamento dos Dados Pessoais

São responsabilidades do DPO:

- a) A interlocução junto aos titulares de dados e junto à ANPD, incluindo reporte de incidentes, orientando colaboradores e terceiros a respeito das práticas relativas à proteção de dados pessoais e privacidade;
- b) Zelar pela conformidade da empresa através da orientação dos gestores quanto à adequação de seus processos de negócios e através da realização de auditorias;
- c) Apoiar e revisar a elaboração dos RTDs e RPDs feitos pelas Unidades Organizacionais da empresa;
- d) Receber e tratar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências;
- e) Receber comunicações da ANPD e adotar providências;
- f) Orientar os colaboradores da empresa a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- g) Orientar as Unidades Organizacionais responsáveis pelo processo/atividade que leva ao tratamento dos dados na elaboração do RTD e do RPD;
- h) Executar as demais atribuições determinadas pela Eletrobras Eletronuclear ou estabelecidas em normativos complementares.

6.7 Gestores das Unidades Organizacionais

Devem zelar pelas informações produzidas e recebidas por sua equipe em razão das atividades da área, realizando e monitorando o inventário de dados sob sua responsabilidade, sua adequada classificação e autorização de acesso, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir os instrumentos normativos da Eletrobras Eletronuclear.

Os gestores também devem manter os RTDs e RPDs atualizados.

6.8 Colaboradores

Cumprir o definido nos instrumentos normativos e procedimentos que regulamentam a proteção de dados e privacidade na empresa, utilizando de forma responsável, profissional, ética e legal as informações corporativas que contenham dados pessoais, respeitando os direitos e a privacidade dos titulares dos dados.

Realizar as ações de treinamentos e desenvolvimento disponibilizadas pela área de gestão de pessoas, referentes à proteção de dados pessoais e privacidade.

6.9 Unidades Organizacionais de Gestão de Pessoas

Promover ações de treinamento e desenvolvimento referentes à proteção de dados pessoais e privacidade, incluindo aspectos técnicos, normativos e comportamentais.

7. PROCEDIMENTOS

7.1 Tratamento de Dados Pessoais

7.1.1 Identificação da necessidade de tratamento de dados pessoais e elaboração do RTD

1. O gestor da Unidade Organizacional, ao identificar a necessidade de tratamento de dados pessoais, deve elaborar o respectivo RTD, conforme orientações do formulário "REGISTRO DE TRATAMENTO DE DADOS PESSOAIS", cujo modelo para preenchimento está disponível na NucWeb, pelo menu "**Institucional**", submenu "**Documentação Administrativa**" e submenu "**Formulários Padronizados**";
2. Após o preenchimento, o gestor encaminha o RTD ao DPO por meio do *e-mail* **dpo@eletronuclear.gov.br**;
3. O DPO analisa o RTD, propõe ajustes, se necessário, e o reencaminha ao gestor da Unidade Organizacional. O gestor, então, realiza os eventuais ajustes necessários, assina e devolve o RTD ao DPO;
4. Caso ajustes não sejam necessários, o DPO recebe, assina e arquiva o RTD.

7.1.2 Necessidade de preparação de RIPD

1. Caso haja necessidade de preenchimento de RIPD, o DPO encaminha o formulário ao gestor da Unidade Organizacional;
2. O gestor da Unidade Organizacional preenche o RIPD e o encaminha ao DPO;
3. O DPO analisa o RIPD, propõe medidas adicionais, se necessário, e o reencaminha ao gestor;
4. O gestor, então, realiza os ajustes necessários, assina e devolve o RIPD ao DPO;
5. Caso novas medidas não sejam necessárias, o DPO recebe, assina e arquiva o RIPD;
6. O DPO encaminha o RIPD à ANPD, quando solicitado.

7.2 Direitos/Demandas dos Titulares de Dados Pessoais

O titular registra sua solicitação por meio da abertura de demanda nos canais disponíveis no *site* da Eletrobras Eletronuclear.

O DPO recebe a demanda e realiza sua verificação, conforme segue:

Se houver sistema específico disponível, pelo qual o titular possa, de maneira autenticada, exercer seus direitos, encaminha *link* e encerra a demanda.

Se não houver sistema disponível para acesso direto do titular, identifica a área responsável pelo tratamento dos dados, solicita ao gestor o envio das informações necessárias, disponibiliza-as ao titular e encerra a demanda.



7.3 Conformidade de Contratos

Quando as unidades organizacionais de contratação de bens e serviços, observarem que o objeto em contratação inclui o tratamento de dados pessoais, devem encaminhar ao DPO, pelo e-mail **dpo@eletronuclear.gov.br**, as seguintes informações para análise pelo DPO:

- Objeto da contratação;
- Duração da contratação;
- Informações sobre tratamento de dados pessoais possíveis no contrato;
- Se ocorre transferência internacional de dados;
- Armazenamento de dados por terceiros;
- Acesso de terceiros à dados pessoais;
- Compartilhamento de dados com terceiros ou com órgãos de controle.

O DPO recebe a demanda, analisa as informações, e responde a área demandante, informando as cláusulas necessárias para adequação do contrato.

7.4 Conformidade de Softwares e Serviços de Tecnologia

As Unidades Organizacionais que pretendem contratar ou desenvolver um software ou serviço de tecnologia que incluam o tratamento de dados pessoais devem se comunicar com o DPO pelo e-mail **dpo@eletronuclear.gov.br** e informar:

- a) Finalidade do software ou do serviço;
- b) Tipos de dados pessoais tratados;
- c) Tempo de retenção dos dados;
- d) Quem terá acesso;
- e) Compartilhamento externo;
- f) Se segue o princípio de *Privacy by Design*;
- g) Desenho do fluxo de dados no sistema.

O DPO analisará os dados, fará as sugestões de adequação, se couber, e responderá ao solicitante.

O DPO poderá solicitar apoio aos departamentos da ST.A, caso seja necessário.

8. DISPOSIÇÕES GERAIS

Quando necessário, a presente Instrução Normativa será atualizada para adequação às novas regulamentações da Legislação em vigor.

O presente documento deve ser lido e considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes adotados pela Eletrobras Eletronuclear.

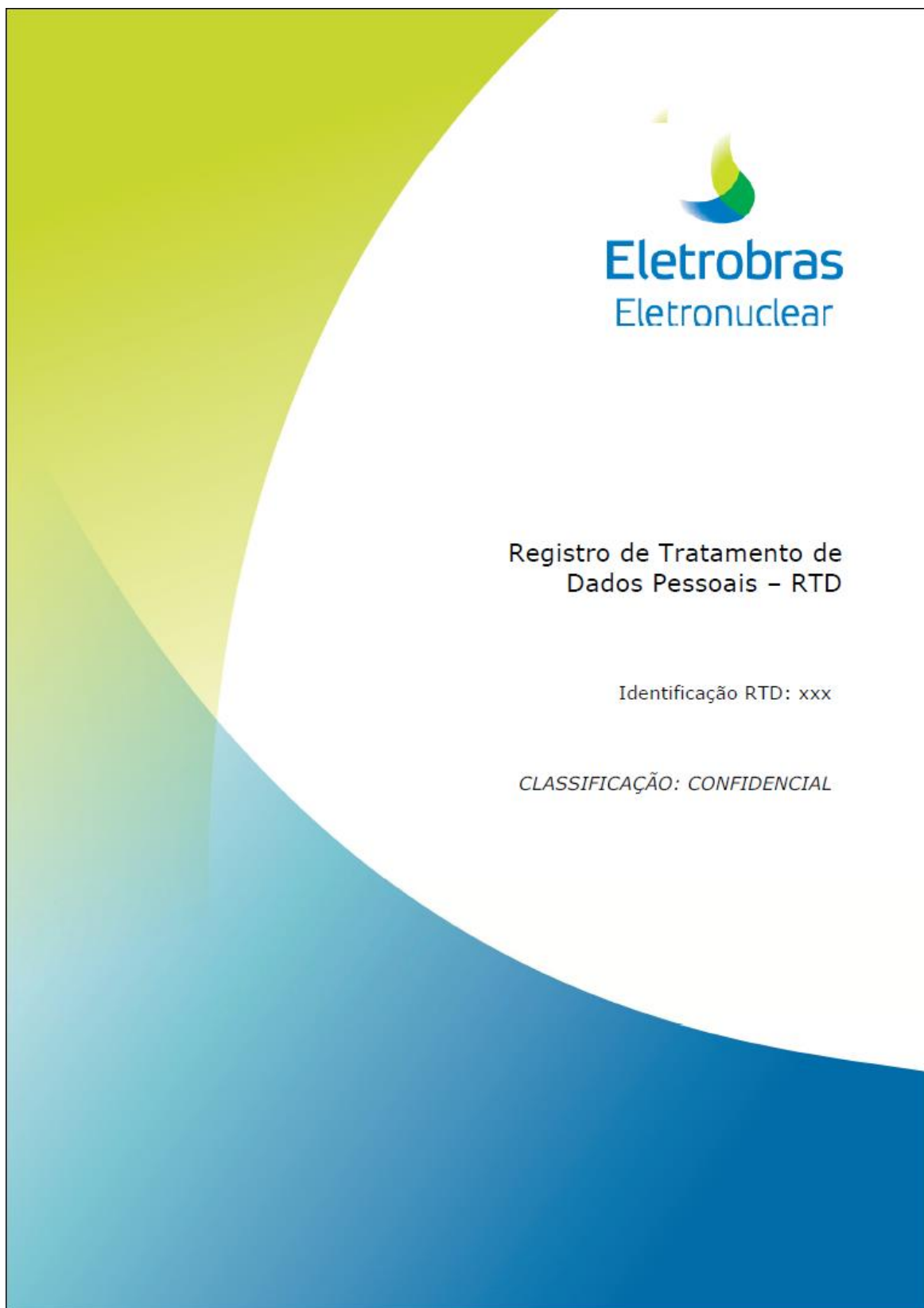
As diretrizes aqui estabelecidas devem nortear a atuação, destacadamente, das Unidades Organizacionais responsáveis por processos de TIC, gestão de pessoas, suprimentos, gestão documental e segurança da informação da Eletrobras Eletronuclear, contribuindo para uma visão única e integrada.

A Eletrobras Eletronuclear deve manter um programa de atualização, no máximo, a cada cinco anos, dos instrumentos normativos voltados aos processos de privacidade e proteção de dados pessoais, visando garantir que todos os requisitos de segurança técnicos e legais implantados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente e alinhados com a sua política de negócios.

Leonam dos Santos Guimarães

Diretor-Presidente

ANEXO 1: FORMULÁRIO RTD



Registro de Tratamento de
Dados Pessoais – RTD

Identificação RTD: xxx

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

Histórico de Revisões

Data	Versão	Descrição	Autor
	1.0	Conclusão da primeira versão do relatório	
	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	

Cód. O&M 269_RTD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

OBJETIVO

O Registro de Tratamento de Dados Pessoais tem por objetivo descrever as operações de tratamento de dados pessoais realizados pelas empresas Eletrobras.

Referência: Art. 37º da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador - Responsável pelas decisões a respeito do tratamento de dados

Operador – Realiza o tratamento em nome do controlador

Encarregado pelo Tratamento de Dados Pessoais – DPO

E-mail Encarregado

Telefone Encarregado

2 – PROCESSO/ATIVIDADE QUE GERA TRATAMENTO

Referência da Arquitetura de Processos

Atividade

Responsáveis pela Atividade

Nome:
Unidade:
E-mail:

Nome:
Unidade:
E-mail:

Cód. OSM 269_RTD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

3 – DESCRIÇÃO DO TRATAMENTO

Dados pessoais tratados

Dados pessoais sensíveis*

Sistema de Informação utilizado

Narrativa do Tratamento**

Compartilhamento de dados***

Término da finalidade****

Período e motivo da manutenção dos dados após término da finalidade.

- * Dados sobre saúde, vida sexual, genético, biométrico, etnia, religião, etc.
** Descrever as rotinas de coleta, uso e armazenamento dos dados pessoais.
*** Informar agentes de tratamento com quem os dados são compartilhados.
**** Informar prazo ou evento que representem término de finalidade.

4 – IMPACTOS DO TRATAMENTO PARA O TITULAR

Volume de Dados envolvidos no Tratamento*

Cód. OSM 269_RTD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

Número de Titulares Afetados (estimativa)
Relacionamento do Titular com Controlador**
Envolve titulares crianças e/ou adolescentes?
Formas do titular exercer seus direitos (Art. 18 LGPD)****

* Estimar número de documentos, registros ou quantidade em bytes.

** Empregado, fornecedor, visitante, estagiário, terceirizado, etc.

*** Onde são armazenados os dados e como podem ser disponibilizados ao titular.

5 – REQUISITOS PARA O TRATAMENTO DOS DADOS PESSOAIS

Finalidade do Tratamento*

Base legal para o tratamento (Art. 7º ou 11 da LGPD)

Se for baseado em consentimento, descrever processo de obtenção

Se baseado no Legítimo Interesse, descrevê-lo baseado no Art. 10 da LGPD

Controle da Conformidade do Operador**

Base legal para a Transferência Internacional de Dados (Art. 33 da LGPD)

* Informar a razão ou motivo pelo qual se deseja tratar os dados pessoais.

** Descrever medidas de controle sobre o operador, para que realize o tratamento de dados pessoais em conformidade com a LGPD e com o estabelecido pelo controlador.

Cód. OSM 269_RTD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

6 - IDENTIFICAÇÃO DE RISCOS

Riscos para o titular dos dados tratados	Assinale (X)
Acesso não autorizado aos Dados Pessoais	☐
Modificação não autorizada dos Dados Pessoais	☐
Perda, Roubo ou Remoção não autorizada dos Dados Pessoais	☐
Roubo de identidade ou fraude	☐
Coleta excessiva de Dados Pessoais	☐
Vinculação não autorizada ou Inadequada de Dados Pessoais	☐
Retenção prolongada de dados pessoais sem necessidade	☐
Danos à reputação do titular	☐
Perda Financeira para o titular	☐
Limitação do exercício de direitos fundamentais ou liberdades civis	☐
Outro Risco:	☐
Outro Risco:	☐

7 - ANÁLISE QUALITATIVA DE RISCOS

Riscos Identificados no Item 6	P	I
Risco A		
Risco B		
Risco C		
Régua de Probabilidades		
Crítica	Alta	Média
Baixa	Mínima	
Régua de Impactos		
Crítica	Alta	Média
Baixa	Mínima	

Legenda:

Probabilidade (P): chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente.

CLASSIFICAÇÃO: CONFIDENCIAL



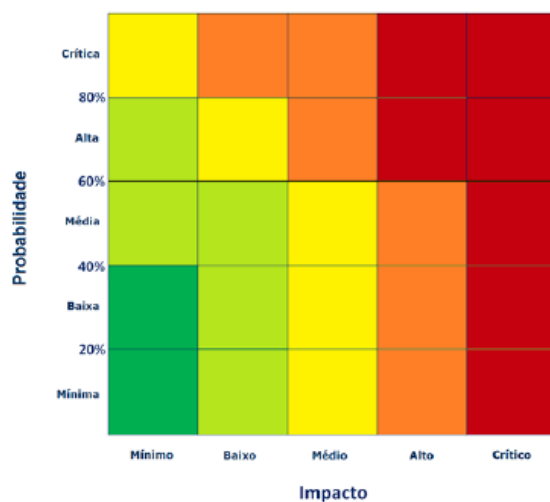
Registro de Tratamento de Dados - RTD

Impacto (I): Avaliação qualitativa e/ou quantitativa da consequência da materialização do risco para o Titular de Dados.

8 – AVALIAÇÃO DOS RISCOS

Risco referente ao tratamento de dados pessoais	Nível de Risco* (P x I)	Responsável
Risco A		
Risco B		
Risco C		

* Nível de Risco: é o produto da probabilidade pelo impacto de cada risco que deve se enquadrar em uma região do mapa de calor apresentado abaixo:



RISCO ENQUADRADO NA REGIÃO



Cód. OSM 269_RTD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

9 - VALIDAÇÃO

Responsável pela elaboração do RTD

<Nome do responsável>
<Local> , <dia> de <mês> de <ano>

10 - CIÊNCIA E ARQUIVAMENTO

Comentários do DPO

Encarregado pelo Tratamento de Dados Pessoais - DPO

<Nome do responsável>
<Local> , <dia> de <mês> de <ano>

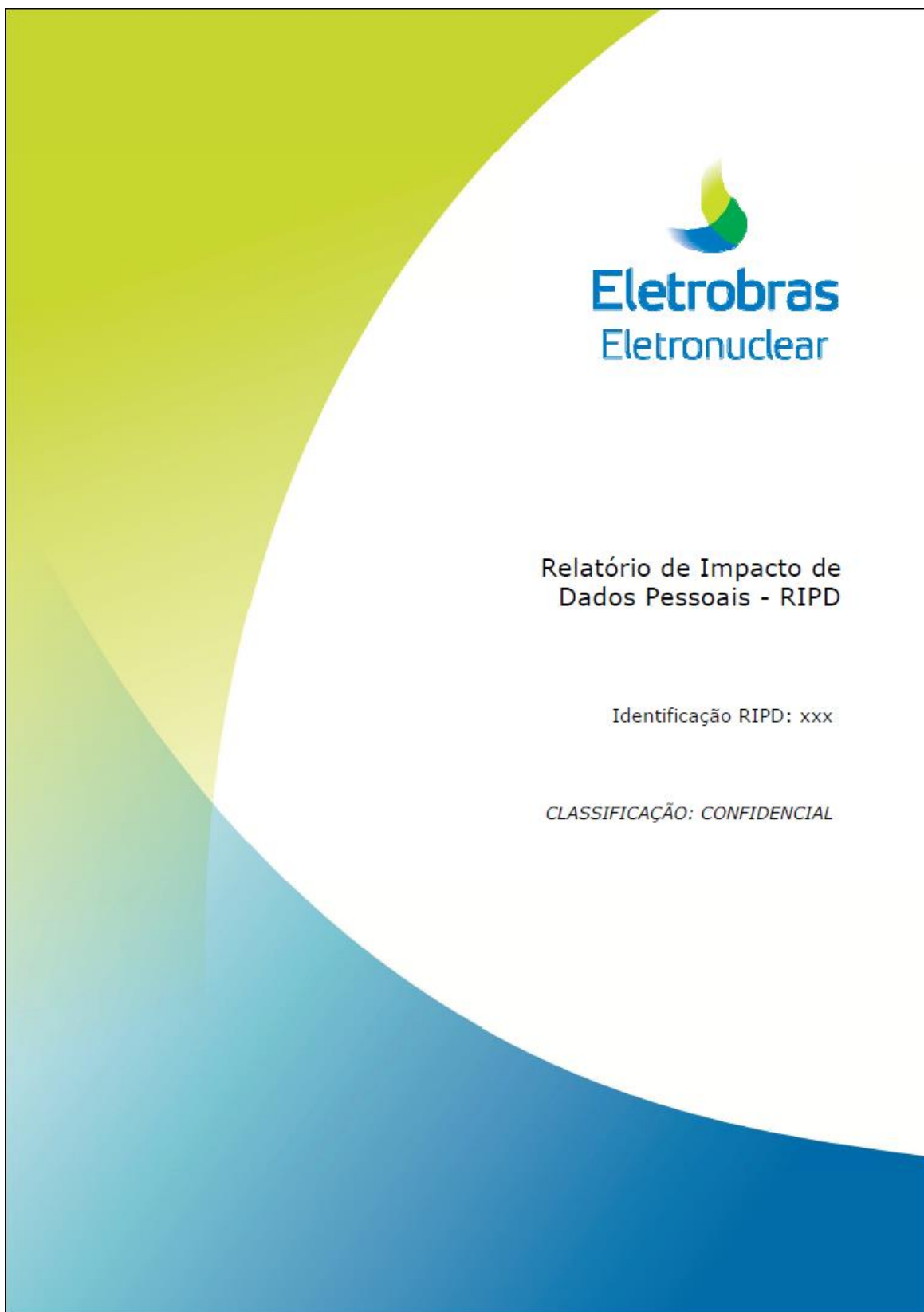
Cód. OSM 269_RTD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Registro de Tratamento de Dados - RTD

ANEXO 2: FORMULÁRIO RIPD




Eletrobras
Eletronuclear

Relatório de Impacto de
Dados Pessoais - RIPD

Identificação RIPD: xxx

CLASSIFICAÇÃO: CONFIDENCIAL



Relatório de Impacto de Dados Pessoais - RIDP

Histórico de Revisões

Data	Versão	Descrição	Autor
	1.0	Conclusão da primeira versão do relatório	
	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	

Cód. O&M 268_RIPD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Relatório de Impacto de Dados Pessoais - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais tem por objetivo avaliar a exposição ao risco do titular de dados gerada pelo tratamento de dados pessoais, bem como identificar medidas, salvaguardas e mecanismos de mitigação de risco. Recomendado especialmente para os tratamentos embasados no legítimo interesse, tratamento de dados pessoais sensíveis além daqueles com potencial de gerar riscos às liberdades civis e aos direitos fundamentais.

Referência: Art. 38º da Lei 13.709/2018 (LGPD).

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador - Responsável pelas decisões a respeito do tratamento de dados

Operador - Realiza o tratamento em nome do controlador

Encarregado pelo Tratamento de Dados Pessoais - DPO

E-mail Encarregado

Telefone Encarregado

2 - PROCESSO/ATIVIDADE QUE GERA TRATAMENTO

Número de Referência do RTD

3 - NECESSIDADE DE ELABORAÇÃO DO RIPD

Motivos	Assinale (X)
Tratamento de dados sensíveis	☐
Tratamento baseado no legítimo interesse	☐
Exposição ao risco alto ou crítico	☐
Risco às liberdades civis e aos direitos fundamentais	☐
Outro:	☐

Cód. O&M 268_RIPD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Relatório de Impacto de Dados Pessoais - RIDP

4 - AVALIAÇÃO DOS RISCOS DEFINIDOS NO RTD

Risco referente ao tratamento de dados pessoais	Nível de Risco (P x I)	Responsável
Risco A	<i>Crítico</i>	
Risco B	<i>Alto</i>	
Risco C	<i>Médio</i>	

5 - MEDIDAS DE TRATAMENTO DOS RISCOS

Risco A		
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
Risco B		
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
Risco C		
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐
<descrição da medida>		

Cód. O&M 268_RIPD_2020

CLASSIFICAÇÃO: CONFIDENCIAL



Relatório de Impacto de Dados Pessoais - RIPD

Não iniciada ☐	Em andamento ☐	Concluída ☐
<descrição da medida>		
Não iniciada ☐	Em andamento ☐	Concluída ☐

6 - RECOMENDAÇÕES ADICIONAIS DO DPO

Adequações no tratamento de dados

1 -

2 -

3 -

7 - VALIDAÇÃO

Responsável pela elaboração do RIPD

<Nome do responsável>
<Local> , <dia> de <mês> de <ano>

8 - CIÊNCIA E ARQUIVAMENTO

Comentários do DPO

Encarregado pelo Tratamento de Dados Pessoais - DPO

<Nome do DPO>
<Local> , <dia> de <mês> de <ano>

Cód. O&M 268_RIPD_2020

CLASSIFICAÇÃO: CONFIDENCIAL