POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ELETRONUCLEAR

Versão 4.0

Eletronuclear
Energia Limpa

Política de Segurança da Informação da Eletronuclear

Área responsável pela emissão

Superintendência de Processos, Riscos e Conformidade / Departamento de Gestão de Processos.

Público-alvo

Empregados, dirigentes, conselheiros e prestadores de serviço da Eletronuclear.

Aprovação

Resolução de Diretoria Executiva RDE 1722.003/23 da Eletronuclear.
Deliberação do Conselho de Administração DCA 521.011/23 da Eletronuclear

Repositório

As Políticas da Eletronuclear podem ser encontradas na rede da intranet da Empresa.

Direitos de autor e confidencialidade

Prazo máximo de revisão: 1 ano.

Histórico de versões:

Versão	Aprovação	Principais alterações
1.0	RES-833/2017, de 26/12/2017.	Não se aplica.
1.0	DEL-008/2018, de 29/01/2018.	Não se aplica.
2.0	RES-677/2018, de 25/09/2018.	Comportar as diretrizes da Política de Controle de Acesso ao SAP das empresas Eletrobras, por solicitação do Comitê de Auditoria e Riscos Estatutário – CAE.
2.0	DEL-200/2018, de 28/09/2018.	Idem acima.
3.0	RES-251/2021, de 19/04/2021 e DEL-079/2021, de 29/04/2021.	Ampliação das referências, conceitos e princípios presentes na LGPD e no Decreto sobre a Estratégia Nacional de Segurança Cibernética. Retirada do Apêndice para transformação em regulamento.
4.0	RDE-1722/2023, de 08/08/2023. DCA-521.011/23 De 26/09/2023	Alinhamento da política à nova estrutura organizacional da Eletronuclear. Inclusão de novos conceitos.

Sumário

1. Objetivo

Orientar estrategicamente as questões relacionadas à segurança da informação, definindo diretrizes para proteção, preservação e descarte de informação no ambiente convencional ou de tecnologia da Eletronuclear.

2. Referências

2.1. Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD).

2.2. Decreto nº 10.222, de 5 de fevereiro de 2020 – Aprova a Estratégia Nacional deSegurança Cibernética.

2.3. Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.

2.4. Decreto nº 3.505/2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

2.5. Portaria nº 93, de 26 de setembro de 2019, Glossário de Segurança da Informação.

2.6. Portaria nº 09 GSI, de 9 de março de 2018, NC 14 IN01, Computação em Nuvem.

2.7. Instrução Normativa GSI Nº 3, de 6 de março de 2013 – Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

2.8. Instrução Normativa IN 01/2008 GSI – Disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

2.9. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009 – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

2.10. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

2.11. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

2.12. ABNT ISO GUIA 73:2009 – Gestão de riscos.

2.13. Código de Conduta Ética e Integridade da Eletronuclear.

2.14. Política de Proteção a Dados Pessoais e Privacidade da Eletronuclear.

2.15. Política de Gestão de Riscos da Eletronuclear.

3. Princípios

3.1. Garantia de disponibilidade, para que a informação esteja acessível e utilizável sob demanda a toda empresa.

3.2. Garantia de integridade da informação, para que não seja modificada ou destruída de maneira não autorizada ou acidental.

3.3. Garantia de confidencialidade da informação, para que não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

3.4. Garantia de autenticidade de autoria e origem da informação, para que sejam sempre identificáveis.

4. Diretrizes

4.1. Gestão do ativo "informação"

4.1.1. Toda informação utilizada pela Eletronuclear é um ativo que possui valor e deve ser gerenciada adequadamente ao longo de todo seu ciclo de vida, para que esteja disponível para acesso pelo público adequado, protegida contra manipulação indevida, com tratamento adequado ao seu grau de sigilo ou restrição de acesso e passível de rastreamento.

4.2. Proprietário da informação

4.2.1. A Eletronuclear é a proprietária e a detentora do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia.

4.3. Classificação da informação

4.3.1. As informações utilizadas na Eletronuclear devem ser classificadas a partir de metodologias e critérios definidos em documentos normativos internos específicos, quanto ao seu grau de sigilo ou nível de restrição de acesso, considerando os processos e atividades nas quais estão inseridas, a fim de assegurar que essas informações recebam um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a Eletronuclear.

4.4. Utilização da informação e dos recursos corporativos

4.4.1. O gestor de cada informação deve determinar a autorização de acesso, incluindo os relacionados ao sistema de gestão empresarial, levando em consideração o sigilo adequado e a necessidade de acesso para cada tipo de público, no cumprimento dos objetivos estratégicos da Eletronuclear.

4.4.2. O acesso à informação deve ser autorizado apenas para os colaboradores que dela necessitem

para o desempenho de suas atividades profissionais.

4.4.3. Cada colaborador deve acessar apenas as informações ou os sistemas previamente autorizados. Qualquer tentativa não autorizada de acesso à informação ou sistema deve ser considerada uma falta disciplinar.

4.4.4. A credencial (*login* e senha) concedida a um colaborador é de uso individual, intransferível e de conhecimento exclusivo.

4.4.4.1. Nos ativos que não possuam recursos de individualização de acesso, a gestão das credenciais é de responsabilidade do gestor da informação de sua respectiva área, que deve determinar a autorização e a forma de acesso.

4.4.5. Os recursos de tecnologia corporativos e operativos fornecidos pela Eletronuclear, inclusive o correio eletrônico, devem ser utilizados prioritariamente para fins profissionais. Dessa forma, todo e qualquer uso não deve violar leis e normativos competentes, bem como o Código de Conduta Ética e Integridade da Eletronuclear.

4.4.6. Para garantir o cumprimento desta política, a utilização dos recursos de tecnologia corporativos e operativos deve ser registrada e monitorada pela Eletronuclear, não devendo o colaborador ter expectativa de sigilo em sua utilização.

4.4.7. Toda informação de tecnologia corporativa e operativa ou dado pessoal sob responsabilidade da Eletronuclear, deve ser mantida e tramitada utilizando apenas os recursos homologados pela Eletronuclear. É vedado o uso de correio eletrônico, repositório em nuvem ou outro recurso qualquer que não seja homologado pela empresa.

4.5. Proteção da informação

4.5.1. A segurança da informação deve ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e recursos de tecnologia.

4.5.2. A Eletronuclear orienta, por meio de seu Código de Conduta Ética e Integridade, que os colaboradores devem "preservar a integridade de documentos, registros, cadastros e sistemas de informação da Eletronuclear, em todos os meios utilizados pela empresa, tanto físico quanto eletrônico".

4.5.3. O gestor de informação de sua respectiva área deve providenciar proteção e controle de acesso físico e lógico aos seus recursos de informação, compatível com o seu nível de criticidade e/ou classificação.

4.5.4. Todo incidente de segurança da informação deve ser reportado por qualquer colaborador que o identifique, segundo os procedimentos e normativos vigentes na Eletronuclear

4.5.5. Os riscos de segurança da informação devem ser identificados, quantificados e priorizados para que se adotem medidas de proteção adequada.

4.5.6. As áreas de segurança cibernética devem manter registros atualizados dos indicadores de segurança da cibernética que mantiverem, bem como a adequada manutenção do ambiente de tecnologia, dos ativos tecnológicos, das configurações e das soluções de segurança em uso na empresa.

4.5.7. As áreas de segurança cibernética devem informar às áreas de segurança da informação quaisquer dados que se façam necessários para compor relatórios à administração da Eletronuclear.

4.6. Confidencialidade da informação

4.6.1. Os colaboradores da Eletronuclear não devem divulgar ou fazer uso de informações corporativas da empresa em benefício próprio ou de terceiros, não importando o tipo de mídia ou suporte utilizado. O descumprimento desse item deve ser investigado e poderá ser considerado uma falta disciplinar, penalizado de acordo com as normas da empresa.

4.7. Continuidade do uso da informação

4.7.1. Os recursos de tecnologia corporativos e operativos utilizados nas atividades de gestão, de suporte e operacionais da Eletronuclear, devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade definidos.

4.7.2. A Eletronuclear deve garantir que os ativos de informação do ambiente convencional, como arquivos físicos, micrográficos, filmográficos, iconográficos, cartográficos e sonoros recebam tratamento e proteção adequados para sua segurança e preservação.

4.7.3. A Eletronuclear deve definir e implementar medidas de prevenção e recuperação para situações de desastre e contingência, que devem contemplar os colaboradores e os recursos de tecnologia e de infraestrutura necessários.

4.8. Relacionamentos formais com terceiros

4.8.1. Todos os relacionamentos formais com terceiros (contratos, convênios, acordos de acionistas, acordos de gestão, formação de consórcios, dentre outros) em que haja o compartilhamento de informações da Eletronuclear e/ou a concessão de qualquer tipo de acesso aos recursos de tecnologia corporativos e operativos devem ser precedidos por termos de confidencialidade e conter cláusulas que tratem especificamente de confidencialidade, privacidade e segurança da informação.

4.8.2. Todos os prestadores de serviço e empregados cedidos de outras empresas, que prestem serviço na Eletronuclear, devem assinar o "Termo de Confidencialidade", anexo 1 desta Política.

4.9. Temporalidade da informação

4.9.1. A Eletronuclear deve garantir que qualquer informação com valor comprobatório para fins de auditorias, de conformidade e judiciais seja preservada na forma e nos prazos demandados pela legislação vigente, ou em acordo com normativo específico.

4.10. Capacitação

4.10.1. A Eletronuclear deve incluir a segurança da informação em seus programas de capacitação.

4.11. Tratamento de dados pessoais

4.11.1. A Eletronuclear deve assegurar o adequado tratamento de dados pessoais, em estrita observância aos termos da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados

(LGPD), nomeando e garantindo o exercício pleno de um encarregado de tratamento de dados pessoais, estabelecendo um canal de atendimento à sociedade civil e de interação com a Autoridade Nacional de Proteção de Dados (ANPD) e processos formais de tratamento de incidentes com privacidade dos dados pessoais.

4.12. Violações e penalidades

4.12.1. A Eletronuclear orienta aos colaboradores, por meio de seu Código de Conduta Ética e Integridade da Eletronuclear, que "o descumprimento de algum dos princípios éticos ou compromissos de conduta", bem como a mera tentativa de burlar as diretrizes desta política ou os controles estabelecidos pela empresa, quando constatada, deve ser tratado como uma violação e pode "resultar na adoção de medidas disciplinares, de caráter educativo, sem prejuízo da adoção de medidas administrativas e/ou judiciais, quando se tratar, ademais de infrações contratuais e/ou legais".

5. Responsabilidades

5.1. Conselho de Administração da Eletronuclear - Aprovar esta política e deliberar sobre as diretrizes estratégicas de segurança da informação para nortear o processo de implementação na Eletronuclear.

5.2. Diretoria Executiva da Eletronuclear - Aprovar esta política e os documentos normativos derivados que permitam sua implementação.

5.3. Comitê de Segurança da Informação da Eletronuclear – Manter e propor políticas, diretrizes, prioridades e implementações pertinentes à Segurança da Informação Corporativa. Promover o esclarecimento e a transparência dos conceitos de Segurança da Informação Corporativa pela ampla divulgação interna destes. Promover e assegurar a conformidade com organismos reguladores, normas, metodologias e legislação, no que for pertinente a Segurança da Informação Corporativa.

5.4. Área responsável pela segurança da informação na Eletronuclear – Gerir os processos e planejamento de ações de desdobramento desta política, promover treinamentos e campanhas de conscientização em SI, coordenar o tratamento de incidentes de SI, apoiar a gestão dos riscos de SI definindo controles adequados em conjunto com as áreas proprietárias de risco, gerir a matriz de classificação da informação, coordenar a implementação e manutenção do Plano de Continuidade de Negócio em relação à disponibilidade de informações, prestar suporte a 1ª linha de defesa, atuar como encarregado pelo tratamento de dados pessoais; e, apoiar e participar da execução das ações estabelecidas pelo Comitê de Segurança da Informação.

5.5. Gestores das áreas – Zelar pelas informações produzidas por sua equipe, realizando sua adequada classificação e autorização de acesso e contingência, bem como o mapeamento, implantação e operacionalização de seus controles, fazendo cumprir as diretrizes desta política.

5.6. Áreas responsáveis pela segurança cibernética – Atender as demandas da área responsável pela segurança da informação, gerir os indicadores cibernéticos, comunicar os incidentes, alinhar o planejamento de projetos e iniciativas cibernéticas com área responsável pela segurança da informação e atender às solicitações do coordenador do GRISI – Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação, planejar a segurança cibernética do ambiente em que atuam,

definindo as configurações tecnológicas necessárias para o alcance da segurança da informação.

5.7. Responsável pela segurança física – Prevenir e proteger instalações e ativos de informação contra acessos não autorizados, danos ou comprometimento de informações. Compete ainda avaliar regularmente o ambiente e encaminhar relatório das vulnerabilidades encontradas nas medidas de segurança física ao responsável pela segurança da informação.

5.8. Colaboradores – Cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, por meio do uso de forma responsável, profissional, ética e legal das informações corporativas, respeitando os direitos e as permissões de uso concedidas pela Eletronuclear.

5.9. Área de educação corporativa – Promover ações de treinamento e desenvolvimento referentes à segurança da informação, incluindo aspectos técnicos, normativos e comportamentais.

5.10. Áreas responsáveis pela gestão de documentos – Garantir o cumprimento dos princípios dessa política para os ativos de informação sob sua responsabilidade. Garantir a preservação dos ativos de informação pelos prazos legais, bem como a eliminação de documentos em acordo com o definido em lei. Manter registros dos acervos documentais da Eletronuclear e controlar seu acesso, observando sua classificação e autorização para tal.

6. Conceitos

6.1. Ambiente convencional

Composto por ativos de informação (fotos, microfilmes, documentos impressos, projetos físicos, registros não digitais em geral, etc.) que não façam parte do ambiente de tecnologia.

6.2. Ambiente de tecnologia

Composto por meios de armazenamento, transmissão e processamento de informações, assim como os equipamentos e sistemas utilizados para tal, que empreguem tecnologias eletrônicas ou digitais.

6.3. Autenticidade

Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

6.4. Tecnologia Operacional (TO)

Entende-se como Tecnologia Operacional (TO) o conjunto de sistemas de automação e de redes de comunicação operacionais necessários à gestão dos ativos, monitoração, e controle de operações industriais, aplicados nos centros de operação, subestações e usinas, e seus processos e dispositivos. Estão incluídos neste rol os equipamentos "Stand-Alone" de monitoração e controle.

6.5. Área

Unidade organizacional formal que possui determinadas atribuições e responsabilidades (exemplos: diretoria, assessoria, superintendência, departamento, divisão).

6.6. Artefato malicioso

Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou redes de computadores.

6.7. Ataque

Tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível.

6.8. Ativo

Qualquer recurso que tenha valor para a Eletronuclear.

6.9. Ativo de informação

Dados, informações e seus meios de armazenamento, transmissão e processamento, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

6.10. Colaborador

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

6.11. Ciclo de vida da informação

Compreende a utilização da informação, desde o momento em que ela é gerada, rotulada, manipulada, armazenada, classificada, transmitida, até a sua destruição.

6.12. Classificação da informação

É o processo de identificar e definir níveis e critérios adequados de proteção das informações, com objetivo de garantir a sua confidencialidade, integridade e disponibilidade

6.13. Espaço cibernético em TIC

Espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente.

6.14. Gestor de informação

Gestor da área formalmente responsável pelo ativo de informação: da produção, do tratamento e da classificação da informação em seus processos de negócio.

6.15. Confidencialidade

Propriedade que garante que a informação seja acessada somente por ativos de informação autorizados pelo gestor de informação.

6.16. Criticidade

Categorização do ativo quanto ao nível de impacto dos riscos associados ao negócio.

6.17. Disponibilidade

Propriedade que garante o acesso às informações, aos recursos associados, e aos ativos de informação autorizados, sempre que solicitado.

6.18. Incerteza

Estado, mesmo que parcial, da deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade. A incerteza pode se transformar em ameaça ou em oportunidade para a empresa.

6.19. Incidente de segurança da informação

Qualquer evento adverso, confirmado ou sob suspeita, que afete a proteção dos sistemas de informação e que comprometa ou tenha potencial para comprometer a segurança da informação.

6.20. Informação

Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

6.21. Privacidade

Propriedade da informação privada que só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata.

6.22. Proprietário da informação

Gestor de unidade organizacional responsável pela produção ou tratamento das informações em seus processos de negócio.

6.23. Proprietário do risco (ou *risk owner*)

Colaborador que possui autoridade e responsabilidade pelo gerenciamento de um ou mais Riscos de Segurança da Informação.

6.24. Risco de segurança da informação

Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças.

6.25. Segurança cibernética

Ações sobre pessoas, tecnologias e processos, com objetivo de viabilizar que os ativos de informação dos ambientes de tecnologia sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

6.26. Segurança da informação

Ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e a autenticidade da informação, dos ambientes convencionais e da tecnologia.

6.27. Segurança física

Medidas físicas destinadas a impedir, detectar e responder o acesso não autorizado a pessoas,bens, valores, equipamento, instalações relacionadas aos ativos de informação.

6.28. Recurso de tecnologia corporativo

Qualquer ativo de informação, exceto recursos humanos, no ambiente convencional ou de tecnologia da Eletronuclear, pertencente à Tecnologia da Informação, Automação e Telecomunicação (TIC).

6.29. Recurso de tecnologia operativo

Qualquer ativo de informação, exceto recursos humanos, no ambiente convencional ou de tecnologia da Eletronuclear, pertencente à Tecnologia Operacional (TO).

6.30. Titular

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

6.31. Linha de defesa

Conceito que auxilia na estruturação e definição clara dos papéis e responsabilidades, de forma que a atuação passe a ser integrada. Dividido em três linhas de defesa:

- 1ª linha: responsável por implementar e operacionalizar os controles para mitigar os riscos de

segurança da informação (área responsável pela segurança cibernética);

- 2ª linha: responsável por definir as diretrizes e monitorar o cumprimento pela primeira linha (área responsável pela segurança da informação);
- 3ª linha: realiza avaliações independentes que permeiam o ciclo completo de gestão de riscos (auditoria interna).

6.32. Unidade organizacional

As unidades organizacionais descrevem as várias unidades na empresa que são normalmente estruturadas de acordo com tarefas e funções.

6.33. Usuário

Pessoa física, ou responsável por conta de serviço, habilitada para acessar os ativos de informação da Eletronuclear.

6.34. Violação

Qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer dos demais instrumentos regulamentares que a complementem.

6.35. Violação de dados pessoais

Um incidente de Segurança da Informação em que ocorre vazamento, perda ou destruição de dados pessoais.

7. Disposições Gerais

7.1. O presente documento deve ser lido, considerado e aplicado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes adotados pela Eletronuclear, incluindo seus anexos. Além disso, esta política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

7.2. As diretrizes aqui estabelecidas devem nortear a atuação, destacadamente, das áreas responsáveis pela tecnologia da informação, tecnologia operacional e segurança da informação da Eletronuclear, contribuindo para uma visão única e integrada.

7.3. A Eletronuclear deve adequar seus documentos normativos e os controles que se fizerem necessários em consonância com o estabelecido nesta política no prazo máximo de 180 dias a partir da aprovação pelo Conselho de Administração da Eletronuclear.

7.4. Deve ser assegurado pela Eletronuclear que esta política e seus documentos normativos complementares sejam amplamente divulgados aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente, são impactados.

7.5. Esta política pode ser desdobrada em regulamentos unificados e válidos para a Eletronuclear, e ainda, em documentos normativos internos específicos da Eletronuclear, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

7.6. Esta política e demais instrumentos regulamentares subordinados a ela devem ser atualizados dentro do prazo máximo de 1 ano ou sempre que houver necessidade, visando garantir que os requisitos técnicos e legais de segurança implementados estejam sendo cumpridos, atualizados em conformidade com a legislação vigente e alinhados às diretrizes que conduzem o desenvolvimento dos nossos negócios, presentes no nosso planejamento estratégico.

ANEXO 1: TERMO DE CONFIDENCIALIDADE

O Presente Termo de Confidencialidade (doravante simplesmente, "TERMO") é celebrado entre:

A ELETRONUCLEAR S.A, pessoa jurídica de direito privado, com sede no endereço Rua da candelária n: 65 Centro- RJ, CEP 20091- 906, inscrita no CNPJ/MF sob o nº 42540211000167, neste ato representada na forma de seu Contrato Social por seus representantes legais, doravante denominada simplesmente "**ELETRONUCLEAR**"; e (NOME DO PRESTADOR DE SERVIÇO OU CEDIDO), (QUALIFICAÇÃO), (CARGO), doravante denominado simplesmente "**PRESTADOR DE SERVIÇO OU CEDIDO**".

A **ELETRONUCLEAR** e o **PRESTADOR DE SERVIÇO OU CEDIDO** serão doravante designadas individualmente como "PARTE", ou em conjunto como "PARTES", consoante as seguintes cláusulas e condições:

Resolvem as PARTES celebrar o presente TERMO, conforme abaixo:

1. DO OBJETO

O objeto do presente Termo é a proteção das Informações Confidenciais disponibilizadas pela ELETRONUCLEAR ao PRESTADOR DE SERVIÇO OU CEDIDO, em decorrência das atividades e funções inerentes à relação de trabalho ou à prestação de serviços existente entre as partes, de modo a resguardar e evitar a divulgação e utilização não autorizada de dados e informações sob a responsabilidade da ELETRONUCLEAR.

2. DAS DEFINIÇÕES

2.1. Serão consideradas Informações Confidenciais, sigilosas e de propriedade exclusiva da ELETRONUCLEAR todas e quaisquer informações reveladas, transmitidas e/ou divulgadas pela ELETRONUCLEAR ao PRESTADOR DE SERVIÇO OU CEDIDO, por quaisquer meios (oral, escrito,

eletrônico ou magnético), podendo incluir, mas não se limitando àquelas:

i. de natureza técnica, operacional, comercial, jurídica, financeira;
ii. oriundas de documentos, relatórios técnicos, contratos, pareceres, pesquisas, projetos;
iii. relacionadas a processos, metodologias e métodos operacionais e estratégicos desenvolvidos e/ou utilizados pela ELETRONUCLEAR; ou
iv. outras de qualquer natureza relacionadas às atividades desenvolvidas pela ELETRONUCLEAR.

2.2. Serão considerados Dados Pessoais todas as informações relacionadas à pessoa natural, identificada ou identificável, contidas nos bancos de dados da ELETRONUCLEAR.

2.2.2. Todos os Dados Pessoais serão considerados Informações Confidenciais para fins deste Termo.

3. DAS LIMITAÇÕES

3.1 Para fins deste Termo, Informações Confidenciais não incluem informações que:

i. Sejam de domínio público;
ii. Sejam de conhecimento do Prestador de serviço ou Cedido antes da disponibilização pela ELETRONUCLEAR;
iii. Tenham sido legitimamente recebidas de terceiros;
iv. Sejam requisitadas por determinação judicial ou de autoridade competente, desde que notifique previamente a ELETRONUCLEAR, para a adoção de medidas de proteção que julgar cabíveis;
v. Deixem de ser consideradas como Informações Confidenciais pela ELETRONUCLEAR.

4. DO USO E DAS RESPONSABILIDADES

4.1 O PRESTADOR DE SERVIÇO OU CEDIDO concorda em usar as Informações Confidenciais recebidas da ELETRONUCLEAR com o propósito único e exclusivo de desempenhar suas atividades laborais, utilizando-se apenas os dados que sejam estritamente necessários para o exercício de suas funções.

4.2. O PRESTADOR DE SERVIÇO OU CEDIDO concorda em não compartilhar quaisquer Informações Confidenciais da ELETRONUCLEAR às quais tiver acesso em decorrência da relação de emprego ou para execução de contrato de prestação de serviços, salvo em situações em que haja previsão legal ou contratual, ou mesmo nas políticas internas que dispõem acerca de informações e dados pessoais.

4.3. O PRESTADOR DE SERVIÇO OU CEDIDO se compromete a não efetuar nenhuma gravação, cópia, distribuição, reprodução, adaptação, fornecimento ou comercialização de quaisquer dados ou informações da base de dados da ELETRONUCLEAR.

4.4. O PRESTADOR DE SERVIÇO OU CEDIDO compreende seu dever de informar à ELETRONUCLEAR acerca de qualquer violação das regras de sigilo que tenha ocorrido ou que venha a ocorrer em decorrência de sua ação ou omissão, independentemente da existência de dolo, para que sejam tomadas as devidas providências.

4.5. O PRESTADOR DE SERVIÇO OU CEDIDO está ciente de que quaisquer dúvidas com relação ao sigilo e confidencialidade de dados pessoais devem ser sanadas com o encarregado de dados da ELETRONUCLEAR.

4.5. O PRESTADOR DE SERVIÇO OU CEDIDO declara estar ciente de que o uso dos dados pessoais aos quais tiver acesso deverá se dar em estrito cumprimento aos princípios e às demais disposições previstas na Lei Geral de Proteção de Dados - Lei nº 13.709/2018 (LGPD), bem como nas políticas internas da ELETRONUCLEAR.

7. DAS PENALIDADES

7.1. O PRESTADOR DE SERVIÇO OU CEDIDO declara estar ciente de que a inobservância de quaisquer das disposições estabelecidas neste Termo, devidamente comprovada, ensejará na sua responsabilização administrativa, civil e/ou penal decorrente de qualquer dano e/ou prejuízo oriundo de eventual quebra de sigilo ou confidencialidade.

7.2. O PRESTADOR DE SERVIÇO OU CEDIDO declara estar ciente de que a inobservância do sigilo e confidencialidade no que se refere a Informações Corporativas e a Dados Pessoais possui penalidades específicas, previstas na Lei de Acesso à Informação – 12.527/21011 (LAI) e na Lei Geral de Proteção de Dados - Lei nº 13.709/2018 (LGPD).

8. DA VIGÊNCIA

8.1 As obrigações de sigilo e confidencialidade decorrentes do presente Termo terão vigência enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa; enquanto não houver a autorização expressa da ELETRONUCLEAR; ou, no caso de dados pessoais, enquanto não houver manifestação livre, informada e inequívoca do titular do dado.

11. DO FORO

11.1 As PARTES elegem o foro da cidade Rio de Janeiro para dirimir quaisquer controvérsias ou dúvidas oriundas do presente TERMO, com renúncia a qualquer outro, por mais privilegiado que seja ou venha a ser.

As PARTES assinam este ACORDO em 2 (duas) vias de igual teor e forma, e para um só efeito, na presença das testemunhas abaixo.

Cidade, XX de XXXXXX de 20XX.

_____

ELETRONUCLEAR-RJ

_____

XXX

Testemunhas:

1. _____
   Nome:
   CPF:

2. _____
   Nome:
   CPF: