Universidade Federal do Rio Grande do Norte

PLANO DE AÇÃO

2021
2023

IMPLEMENTAÇÃO DA
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

LGPD NA UFRN
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

UFRN.BR

UNIVERSIDADE FEDERAL DO
RIO GRANDE DO NORTE

REITOR
José Daniel Diniz Melo

VICE-REITOR
Hênio Ferreira de Miranda

ORGANIZAÇÃO
Comissão LGPD

ELABORAÇÃO E DIAGRAMAÇÃO
Luan David Pereira do Nascimento

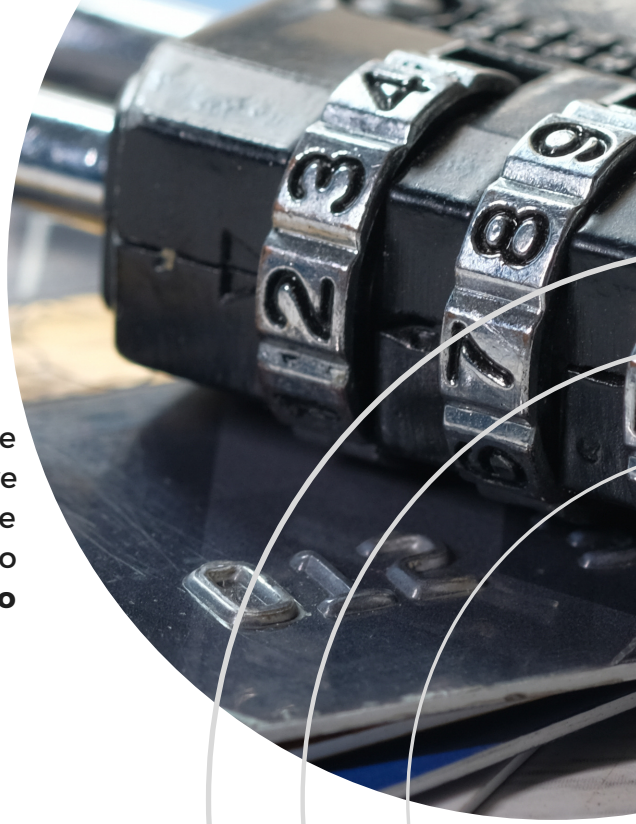
APOIO
Thiago de Oliveira

COMISSÃO LGPD

Portaria Nº 973 / 2020 - R, de 18 de agosto de 2020
publicada no Boletim de Serviço UFRN nº 161 de 19/08/2020

LUAN DAVID PEREIRA DO NASCIMENTO, Administrador, matrícula nº 2249013 (presidente).
ADRIANNE PAULA VIEIRA DE ANDRADE, Professora Adjunta, matrícula nº 1100806.
ANDRÉ MEDEIROS DANTAS, Analista de Tecnologia da Informação, matrícula nº 3083586.
BRUNNO SANTIAGO E SILVA, Analista de Tecnologia da Informação, matrícula nº 3159204.
CLARISSA LORENA ALVES COELHO LINS, Analista de Tecnologia da Informação, matrícula nº 2134722.
ELIAS JACOB DE MENEZES NETO, Professor Adjunto, matrícula nº 2353000.
JOSE ALFREDO FERREIRA COSTA, Professor Titular, matrícula nº 1142787.
MANOEL BEZERRA DA COSTA NETO, Analista de Redes e Comunicação de Dados da FUNPEC, matrícula nº 4480.
MARCOS CESAR MADRUGA ALVES PINHEIRO, Professor Associado, matrícula nº 1525670.

V. 1.1 - 10/03/2021
Consulte sempre a última versão atualizada no sítio institucional da UFRN.
Menu "Institucional", seção "Proteção de Dados".



LGPD

A Lei Geral de Proteção de Dados (LGPD) - oficialmente Lei nº 13.709 de 14 de agosto de 2018 - é a lei que promove a proteção dos dados pessoais de pessoas naturais que estão sob posse de pessoas físicas e jurídicas. Como instituição pública, **a UFRN deve realizar a proteção desse tipo de dados, conforme Art. 1º da LGPD**.

BASES DO PROJETO

Como estratégia de implantação das diretrizes da LGPD na instituição, identificar as necessidades e executar as ações, optou-se pela adoção de técnicas de gestão de projetos, de maneira a manter a regularidade no diagnóstico situacional, na intervenção e na conclusão de entregas planejadas.

Dessa forma, a primeira providência é a definição de uma equipe de projeto, oficializada em comissão, de maneira a executar os trabalhos. Como tática de operacionalização das ações da equipe, optou-se pelo estudo do arcabouço teórico-legal sobre o tema, documentação relacionada na página 4, além da execução de quatro estratégias, descritas a seguir.

CICLO DE EXECUÇÃO

01 Conhecer a LGPD. Capacitar a equipe em LGPD. Entender as implicações da LGPD na UFRN.

02 Mapear frameworks de segurança da informação. Estruturar as ações da LGPD em áreas de abordagem.

03 Planejar projeto. Estruturar ações em entregas. Executar ações. Articular entregas com setores da instituição.

04 Monitorar entregas. Refinar e corrigir ações. Avaliar o impacto, se necessário.

MÉTODO

- Avaliação de problemas;
- Reuniões semanais de report;
- Articulação com unidades responsáveis;
- Report ao Comitê de Governança;
- Distribuição de tarefas semanais;
- Comunicação aos stakeholders;
- Método Life Cycle Canvas;
- Orientação pela legislação;
- Todos são responsáveis por todas as entregas;
- Responsáveis por entrega são responsáveis pela coordenação de execução da entrega;
- Acompanhamento SCRUM.

DOCUMENTAÇÃO E LEGISLAÇÃO DE BASE

Lei n° 13.709/2018, Lei Geral de Proteção dos Dados – LGPD.

Lei n° 13.853/2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

Portaria nº 1, de 8 de março de 2021. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD.

Lei n° 12.527/2011 (Lei de Acesso à Informação), que 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; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Instrução Normativa Nº 01 GSI/PR/2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

ISO/IEC 29151:2017 - Information technology — Security techniques — Code of practice for personally identifiable information protection.

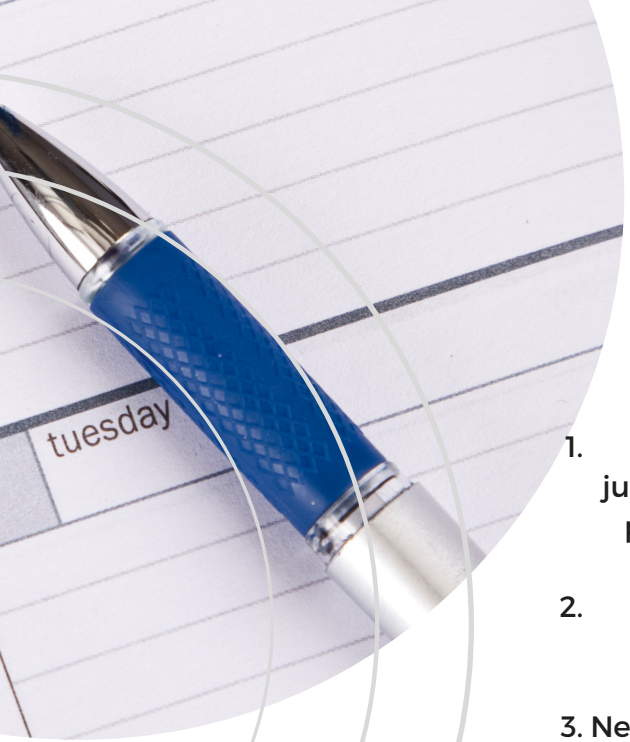
Lei n° 13.460/2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

Lei n° 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Decreto n° 7.724/2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

Decreto n° 9.492/2018, que regulamenta a Lei nº 13.460, de 26 de junho de 2017 , que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo federal, e altera o Decreto nº 8.910, de 22 de novembro de 2016, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Transparência, Fiscalização e Controladoria-Geral da União. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9492.htm

Decreto n° 8.771/2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.



JUSTIFICATIVAS

O QUE OCORRE HOJE OU OCORREU NO PASSADO?

1. Lei nº 13.709, de 14 de agosto de 2018: a LGPD é a principal justificativa para realização do projeto, já que vincula toda as pessoas jurídicas de direito privado e público a seguirem as suas orientações.
2. Necessidade da melhoria da segurança da informação: a UFRN deve aprimorar os seus mecanismos técnicos e de gestão de proteção da informação.
3. Necessidade de melhoria na governança dos dados: ter maior controle sobre a coleta, uso, compartilhamento e descarte adequado dos dados pessoais utilizados pela instituição.

OBJETIVOS

O QUE QUEREMOS?

1. Implantar as diretrizes estratégicas e operacionais da LGPD nos processos da instituição: promover o compartilhamento; promover as mudanças técnicas, infralegais, administrativas e de gestão para atender aos requisitos da LGPD e legislação associada.
2. Atender os direitos dos titulares de dados: promover, divulgar e atender os direitos dos titulares de dados pessoais, focando no atendimento em tempo razoável, automatizado (quando for possível) e com disponibilidade das informações solicitadas..
3. Operar mecanismos de governança para monitoramento do tratamento de dados pessoais: após a estruturação das ações de implementação, implantar mecanismos de controle, como o Comitê de Proteção de Dados, além de monitoramento das estatísticas dos principais processos que operam no tratamento de dados, subsidiando a tomada de decisão.

BENEFÍCIOS

O QUE ESPERAMOS?

1. Maior segurança da informação: adoção da cultura de proteção de dados pessoais na concepção de sistemas, nos sistemas já existentes, nos processos, em comportamento e atitudes e na gestão.
2. Atendimento a Lei 13709, de 14 de agosto de 2018: cumprimento dos requisitos e respeito aos direitos dos titulares de dados pessoais.
3. Criação da cultura de utilização do dado de forma mais estratégica

PRODUTOS FINAIS A SEREM ENTREGUES

1. Diretrizes da LGPD implantadas nos processos críticos da UFRN (técnicas, infra-legais e de gestão)
2. Mudança e criação das normas que suportem a LGPD na universidade
3. Governança mínima estruturada e implementada

REQUISITOS BÁSICOS COMUM AS ENTREGAS

1. Atendimento aos requisitos da Lei 13.709;
2. Alinhamento a Política de Gestão de Riscos da universidade;
3. Definição das figuras de tratamento da informação;
4. Criação de modelos-padrão de RIPD;
5. Tratamento de processos congêneres em lote.

RESTRIÇÕES DO PROJETO

1. Recursos orçamentários (mudança em ativos);
2. Restrição de pessoal (mudança de ativos; falta de dedicação exclusiva da equipe);
3. Restrição devido a questões burocráticas.

PARTES INTERESSADAS (STAKEHOLDERS)

1. Comunidade acadêmica;
2. Controlador (Alta Gestão);
3. Ouvidoria;
4. Superintendência de Informática;
5. Secretaria de Gestão de Projetos;
6. Secretaria de Governança Institucional;
7. Coordenadoria de Gestão da Informação;
8. Superintendência de Comunicação;
9. Comitê de Governança, Riscos e Controles;
10. Comitê de Segurança da Informação.

EQUIPE

Comissão informada na página 02 deste documento.

PREMISSAS BÁSICAS

1. As diretrizes da LGPD serão implantadas em lotes; (processos)
2. As demandas de alteração da LGPD terão prioridades; a frente de outras demandas.

AQUISIÇÕES

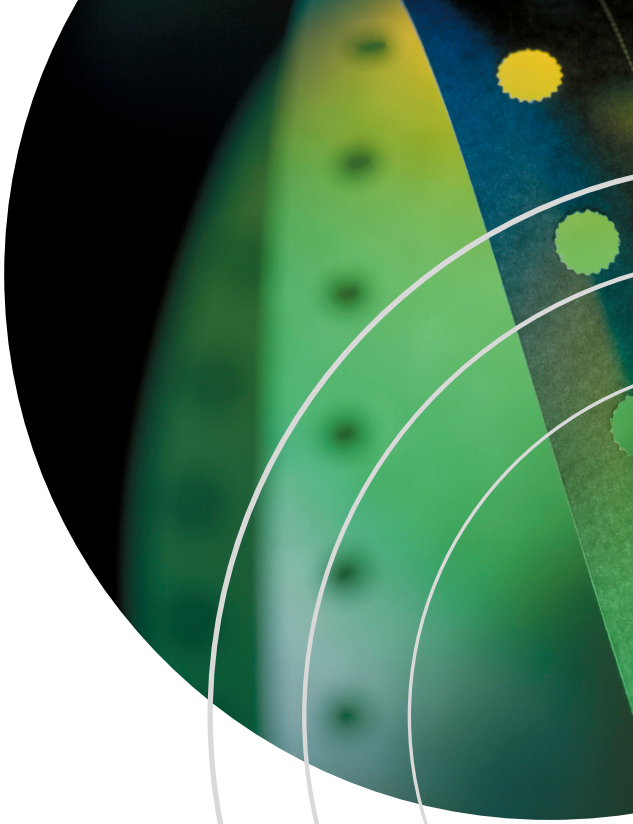
1. Projeto de Gestão de Riscos (SGP);
2. Diretoria de Compras (aquisição ou atualização de ativos);
3. Pareceres de utilização da informação pelas partes interessadas (RIPD).

RISCOS DO PROJETO

1. Mapeamento demorado, processo um a um;
2. Possibilidade da não adesão das partes interessadas ao projeto;
3. Impactos de mudança nos sistemas da universidade;
4. Termo de consentimento para responsáveis relacionados a tratamento de dados para crianças e adolescentes;
5. Normas e políticas que precisem de modificações e aprovação em conselhos;

ENTREGAS

01 - Mapeamento e identificação de unidades que realizam tratamento de dados pessoais;
02 - Mudanças nos sistemas organizacionais;
03 - Capacitação de servidores;
04 - Campanha de comunicação e conscientização;
05 - Criação e revisão de normativos;
06 - Melhorias de governança na área de tecnologia da informação;
07 - Análise de processos, riscos e relatório de impacto;
08 - Mecanismos de governança.



ENTREGA 01

Diagnóstico de unidades internas que realizam tratamento de dados.

Objetivo: Mapear, identificar e conhecer melhor a realidade das unidades que realizam tratamento de dados para definir estratégias de recomendação de adequação a LGPD para essas unidades. Pretende-se executar:

- Lançamento de questionário inicial que busque identificar as unidades organizacionais internas que realizam tratamento de dados pessoais;
- Análise e tabulação dos dados obtidos;
- Manter contato aproximado com unidades que realizam um grande volume de tratamento de dados pessoais;
- Estabelecer diretrizes e recomendações de adequação para essas unidades.

Responsáveis: Elias Jacob de Menezes Neto / Luan David Pereira do Nascimento
Unidades vinculadas: Ouvidoria / SGP

Previsão de entrega: 08/2021

ENTREGA 02

Mudanças nos sistemas organizacionais.

Objetivo: Realizar mudanças nos sistemas integrados que envolvam os direitos dos títulares elencados especialmente no art. 18 da LGPD. Entre essas ações, estão:

- Proteção/exposição de dados pessoais nas áreas públicas dos sistemas integrados;
- Mecanismo de extração de dados pessoais de titular específico (para que o titular possa solicitar cópia dos dados);
- Mecanismos de consentimento;
- Melhorias de segurança para proteger os dados pessoais armazenados;
- Publicação em página própria, de todas as operações de tratamento realizadas pela instituição;
- Rastreamento de projetos de pesquisa que envolvam o tratamento de dados pessoais, especialmente aqueles que envolvam estudos em saúde pública.

Responsáveis: André Dantas Medeiros / Clarissa Lorena Alves Coelho Lins
Unidades vinculadas: SINFO

Previsão de entrega: 12/2021

ENTREGA 03

Capacitação da comunidade de servidores.

Objetivo: Capacitar os servidores responsáveis pelo tratamento de dados, bem como a comunidade de servidores em geral sobre princípios, deveres e direitos dos usuários. Esta ação envolve o desenvolvimento de atividades relacionadas a:

- Formatação e elaboração de material didático de capacitação generalista para a comunidade de servidores;
- Submissão de proposta de capacitação nas instâncias competentes de gestão de pessoas da universidade;
- Realização de capacitação:
  - Específica, para as unidades e servidores (operadores) que realizem um maior volume de tratamento de dados, focando em aspectos técnicos e jurídicos da LGPD;
  - Generalista, para os demais servidores, focando em dicas práticas, principais deveres do servidores e direitos do usuário (titular).

Responsáveis: Adrianne Paula Vieira Andrade / Luan David Pereira do Nascimento
Unidades vinculadas: CGI-PROAD / SGP

Previsão de entrega: 12/2021

ENTREGA 04

Campanha de comunicação e conscientização.

Objetivo: Divulgar as ações de implementação da LGPD, com foco nas principais diretrizes, deveres e direito dos usuários para a comunidade acadêmica (servidores e alunos). Isso envolve:

- Criação de logo e identidade visual de campanha;
- Formatação e divulgação de banner's, folder's, guias, vídeos nos sistemas integrados, via e-mail e redes sociais;
- Formatação de conteúdo exclusivo para operadores de processos com grande tratamento de dados (coordenadores de projeto de pesquisa e extensão);
- Realização de entrevistas (internet);
- Realização de debates virtuais com especialistas.

Responsáveis: Adrianne Paula Vieira de Andrade / Luan David Pereira do Nascimento
Unidades vinculadas: CGI-PROAD / SGP

Previsão de entrega: 12/2021

ENTREGA 05

Melhorias de governança na área de tecnologia da informação.

Objetivo: Realizar mudanças em procedimentos, práticas e processos da área de tecnologia da informação. Entre essas medidas, estão:

- Estudo de frameworks de segurança da informação (ABNT/ISO 27002:2013 e ISO/IEC 29151:2016(E)), especialmente aqueles relacionados a desenvolvimento de sistemas e incidentes de segurança da informação;
- Formalização dos processos de gestão da mudança nos sistemas integrados;
- Criação de política de backup;
- Construção de política de continuidade de serviços de TI;
- Aperfeiçoamento da política de controle de acesso;
- Aperfeiçoamento do processo de desenvolvimento de software.

Responsáveis: André Dantas Medeiros / Clarissa Lorena Alves Coelho Lins
Unidades vinculadas: SINFO

Previsão de entrega: 12/2021

ENTREGA 06

Criação e revisão de normativos.

Objetivo: Adequar os normativos existentes da instituição à LGPD, além de construir diplomas infralegais com diretrizes de atuação, implementação e execução na universidade. Relaciona-se com:

- Leitura, revisão e atualização da Política de Segurança da Informação;
- Criação da Política de Proteção de Dados Pessoais;
- Construção da Política de Classificação de Informações;
- Concepção da Política de Privacidade.
- Discussão e aprovação em Conselhos Superiores.

Responsáveis: José Alfredo Ferreira Costa / Elias Jacob de Menezes Neto
Unidades vinculadas: CT / Ouvidoria

Previsão de entrega: 06/2022

ENTREGA 07

Análise de processos, riscos e Relatório de Impacto de Dados Pessoais.

Objetivo: Identificar a melhor estratégia de mapeamento dos processos de negócio que envolvam grande volume de tratamento de dados pessoais, além de desenvolver a metodologia de construção de Relatórios de Impacto de Dados Pessoais para os processos organizacionais críticos. Isso envolverá:

- Aprendizado da equipe na elaboração de Relatório de Impacto;
- Confecção de Relatório de Impacto de processos-piloto;
- Capacitação da equipe na construção desses relatórios;
- Desenvolvimento de estratégia de criação de relatórios dos processos de negócio quanto ao seu risco e importância para os objetivos estratégicos da instituição.

Responsáveis: Manoel Bezerra da Costa Neto
Unidades vinculadas: SINFO

Previsão de entrega: 06/2022

ENTREGA 08

Estruturação de mecanismos de governança e monitoramento de dados pessoais.

Objetivo: Operacionalizar um conjunto de responsabilidades, conformidade e monitoramento de variáveis relacionadas a proteção de dados pessoais após a implementação das diretrizes da LGPD na instituição. Isso envolve:

- Estruturação de eventuais mecanismos de governança (Comitês) a serem criados por novas resoluções criadas pelo projeto;
- Geração de relatórios periódicos e estatísticas de número de usuários (titulares) com dispensa de consentimento, usuários com consentimento, volume de dados tratados, entre outros;
- Criação de dashboard de acompanhamento dos processos críticos quanto ao processamento de dados pessoais, focalizando nos seus riscos e medidas de mitigação;
- Estabelecimento de procedimentos de comunicação ao usuário sobre incidentes de segurança e comunicação a Autoridade Nacional de Proteção de Dados.

Responsáveis: Luan David Pereira do Nascimento
Unidades vinculadas: SGP

Previsão de entrega: 12/2023

LGPD NA UFRN

PLANO DE AÇÃO

CRONOGRAMA PREVISTO

O diagrama de GANTT apresenta, em ordem cronológica, a previsão de entrega das ações planejadas para implementação das diretrizes da LGPD na UFRN. Os requisitos referentes à garantia dos direitos dos titulares dos dados - art. 18 da LGPD - foram priorizados, com previsão de entrega até dezembro de 2021. As demais entregas, especialmente aquelas relacionadas à governança, mudança de cultura organizacional e legislação infralegal, mais complexas e que demandam um maior tempo de análise e construção, terão prazo de entrega até os anos de 2022 e 2023, acompanhando a data limite do Plano de Gestão 2019-2023 da instituição.

GANTT - LGPD NA UFRN

		2021				2022	2023
nº	Entregas	1° Trimestre	2° Trimestre	3° Trimestre	4° Trimestre		
1	Diagnóstico de unidades que realizam tratamento de dados						
2	Mudanças nos sistemas organizacionais						
3	Capacitação da comunidade de servidores						
4	Campanha de comunicação e conscientização						
5	Melhorias de governança na área de tecnologia da informação						
6	Criação e revisão de normativos						
7	Análise de processos, riscos e Relatório de Impacto de Dados Pessoais						
8	Estruturação de mecanismos de governança e monitoramento						

O cronograma poderá sofrer alterações em virtude das restrições elencadas no planejamento do projeto, especialmente a disponibilidade de recursos orçamentários, a capacidade de conciliação das tarefas da equipe do projeto com seus processos diários, além do nível de complexidade técnica na implementação de mudanças nos sistemas integrados da universidade e no nível de maturidade na mudança de comportamento organizacional pela comunidade de servidores e colaboradores da instituição.

LGPD NA UFRN

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Universidade Federal do Rio Grande do Norte

UFRN.BR