CRCRN
CONSELHO REGIONAL DE CONTABILIDADE
DO RIO GRANDE DO NORTE

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

Julho de 2023.

Av. Nevaldo Rocha, 4545 – Tirol – Natal/RN – Cep: 59015-450
Telefone: (84) 3211-8505
crcrn@crcrn.org.br – www.crcrn.com.br

Histórico de Revisões

Data	Versão	Descrição	Autor
17/07/2023	1.0	Conclusão da primeira versão do relatório	Geovane Martins de Oliveira

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO	
Controlador	
Conselho Regional de Contabilidade do Rio Grande do Norte, representado pelo Contador Anailson Marcio Gomes.	
Operador	
Spiderware Consultoria em Informática Ltda	
Encarregado	
Geovane Martins de Oliveira	
E-mail Encarregado	**Telefone Encarregado**
dpo@crcrn.org.br	(84) 3211-8505

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

A Lei Geral de Proteção de Dados estabelece uma série de exigências e critérios às empresas ou entidades que tratam dados pessoais, dentre eles, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) objetivando assegurar que as atividades sejam conduzidas em conformidade com as normas aplicáveis.

Neste contexto, o RIPD cumpre a função de demonstrar que o Conselho Regional de Contabilidade do Rio Grande do Norte (CRCRN), avaliou e mapeou os riscos existentes nas operações de tratamento de dados pessoais e verificou a adoção de medidas para mitigá-los, melhorá- los ou eliminá-los dentro das áreas.

Esclarece-se que risco é um cenário em que pode se descrever o evento e suas respectivas consequências, calculando o impacto e a probabilidade. A gestão de riscos,

por outro lado, pode ser definida como as atividades voltadas ao controle sobre o risco pela organização.

Considerando os fundamentos da proteção de dados pessoais (art. 2º e incisos, LGPD), a boa-fé e os demais princípios a serem observados nas atividades de tratamento de dados pessoais o Conselho Regional de Contabilidade do Rio Grande do Norte (CRCRN), dispõe de sistemas de controles internos, que variam de acordo com a natureza do dado pessoal, para mitigar eventuais riscos de falha na proteção de dados pessoais. Entretanto, podem ser aprimorados a fim de que ocorra a redução dos riscos existentes na entidade. Em assim sendo, o RIPD tem por função avaliar os riscos e reduzi-los ao máximo possível evitando incidentes envolvendo dados de pessoas físicas.

3 – DESCRIÇÃO DO TRATAMENTO

A Política de Segurança da Informação (PSI) da entidade está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 reconhecidas mundialmente como um código de prática para a gestão da segurança da informação, tem por objetivo definir os princípios e diretrizes gerais sobre a preservação da segurança da informação, segundo os princípios de auditabilidade, confidencialidade, disponibilidade, integridade, autenticidade, bem como legalidade dos processos que amparam a operacionalização e gestão das atividades da entidade. Ela evita que os riscos aos quais estão sujeitos os ativos de informação comprometam vitalmente as atividades do Conselho Regional de Contabilidade do Rio Grande do Norte – CRCRN, e impeçam o cumprimentode sua missão institucional.

No que se refere especificamente às informações de caráter pessoal, os sistemas de controle interno implantados no Conselho Regional de Contabilidade do Rio Grande do Norte – CRCRN variam de acordo com o tipo de suporte (físico ou digital – em sua maioria), bem como com a natureza da informação (comum ou sensível).

3.1 – NATUREZA DO TRATAMENTO

No Conselho Regional de Contabilidade do Rio Grande do Norte – CRCRN, de forma geral, são adotadas algumas medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Com relação aos Projetos: 1001 1003, 2001,2002 e 2013 alusivos às áreas de registro e fiscalização da profissão contábil e área de recursos de recursos humanos, em que se verificou maior risco/probabilidade de ofensa aos direitos fundamentais do titular, em razão da qualidade do dado pessoal circulante, percebeu-se a necessidade de realização do RIPD.

Isso porque os dados pessoais identificados na fase de diagnóstico mostram-se na qualidade de sensíveis, podendo causar discriminação caso ocorra o uso inadequado ou em um incidente de vazamento de dados, acarretará prejuízos ao titular, merecendo maior atenção por parte do Controlador.

3.1.2 Tratamento dos dados

Existem diversas formas de tratamento dos dados pessoais no Conselho Regional de Contabilidade do Rio Grande do Norte – CRCRN, relacionados aos Projetos: 1001 1003, 2001, 2002 e 2013 , considerando a definição da LGPD:

Área de Registro - Projeto 1001

a. A coleta dos dados é realizada pelos CRCs e não pelo CFC.
b. Os dados são retidos e armazenados na base de dados do CFC.
c. Os dados são processados e usados nos cadastros do CNAI, CNPC, CNAI PJ, Carteira de Identidade Profissional e Comunicação do Exercício Profissional em outra jurisdição.
d. Os dados são compartilhados no portal do CFC e nos cadastros do CNAI, CNPC, CNAI PJ, Carteira de Identidade Profissional e Comunicação do Exercício Profissional em outra jurisdição e SPW. e Receita Federal do Brasil
e. Os dados não são eliminados.

Área de Registro - Projeto 1003

a. Os dados são coletados na Receita Federal do Brasil com base no pedido de informações dos CRCs.
b. Os dados são retidos e armazenados na rede interna do CFC.
c. São processados e usados na rede interna do CFC.
d. São compartilhados via e-mail a cada CRC para fins de atualização da base cadastral e tomar as medidas cabíveis.
e. Os dados são eliminados.

Área de Fiscalização - 2001

a. A coleta é realizada por meio de dados do registro do profissional ou procedimento fiscalizatório anterior e convênios, por meio físico e ou formulario eletrônico.
b. A retenção é realizada em arquivo físico dos registros, banco de dados (interno ou externo), Sistema de Fiscalização Eletrônico da SPW, Sistema Decore do CFC, Sistema de Ouvidoria, Sistema de Denúncia da SPW e servidor de e-mail.
c. O processamento pode ser realizado em arquivo físico e digital (word, excel, pdf e etc) , banco de dados (interno ou externo), Sistema de Fiscalização Eletrônico da SPW (local e Web), Sistema Decore do CFC, Sistema de Ouvidoria VOX, Sistema de Denúncia da SPW e servidor de e-mail. As Unidades Organizacionais que possuem acesso aos dados são a área de Fiscalização, Presidência e Jurídico do CRC.
d. O compartilhamento é realizado por meio de arquivo físico e digital (word, excel, pdf e etc) ,banco de dados (interno ou externo), Sistema de Fiscalização Eletrônico da SPW (local e Web), Sistema Decore do CFC, Sistema de Ouvidoria VOX, Sistema de Denúncia da SPW e servidor de e-mail. As Unidades Organizacionais que possuem acesso aos dados são a área de Fiscalização e Jurídico do CRC. Envio de

   dados pessoais de profissionais ou leigos para as autoridades competentes tais como: Ministério Público, Polícia Civil, Tribunal de Contas, Defensoria e Tribunais gerais.
e. Os dados serão eliminados, conforme tabela de temporalidade. Os processos com penalidade aplicada são de guarda permanente.

Área de Fiscalização - 2002

a. A coleta é realizada por meio de dados do registro do profissional ou procedimento fiscalizatório anterior e convênios, por meio físico e ou formulario eletrônico.
b. A retenção é realizada em arquivo físico dos registros, banco de dados (interno ou externo), Sistema de Fiscalização Eletrônico da SPW, Sistema Decore do CFC, Sistema de Ouvidoria, Sistema de Denúncia da SPW e servidor de e-mail.
c. O processamento pode ser realizado em arquivo físico e digital (word, excel, pdf e etc) , banco de dados (interno ou externo), Sistema de Fiscalização Eletrônico da SPW (local e Web), Sistema Decore do CFC, Sistema de Ouvidoria VOX, Sistema de

Denúncia da SPW e servidor de e-mail. As Unidades Organizacionais que possuem acesso aos dados são a área de Fiscalização, Presidência e Jurídico do CRC.

d. O compartilhamento é realizado por meio de arquivo físico e digital (word, excel, pdf e etc) ,banco de dados (interno ou externo), Sistema de Fiscalização Eletrônico da SPW (local e Web), Sistema Decore do CFC, Sistema de Ouvidoria VOX, Sistema de Denúncia da SPW e servidor de e-mail. As Unidades Organizacionais que possuem acesso aos dados são a área de Fiscalização e Jurídico do CRC. Envio de dados pessoais de profissionais ou leigos para as autoridades competentes tais como: Ministério Público, Polícia Civil, Tribunal de Contas, Defensoria e Tribunais gerais.
e. Os dados serão eliminados, conforme tabela de temporalidade. Os processos com penalidade aplicada são de guarda permanente.

Área de Pessoal - 2013

a. coleta - Os dados pessoais dos funcionários são coletados pelo empregado do Setor Pessoal. Para a contratação de estagiários a coleta é realizada por meio de currículo, fornecido pelo candidato (a) interessado na vaga via e-mail.
b. retenção - Os dados pessoais dos colaboradores contratados são retidos e armazenados no banco de dados do CRCRN e na pasta física de cada colaborador, num armário que possui chave (a responsável pelos recursos humanos e o estagiário da aréa possuem acesso as pastas, em um armário específico para guarda de documentos) e alguns dos dados são armazenados na rede interna. As informações são acessadas na rede interna pelo responsável pelo Setor Pessoal e pela área de tecnologia da informação.
c. processamento - Os dados dos colaboradores são processados e usados no Sistema FORTES, Sistema SEI, IFOOD BENEFÍCIOS E SERVIÇOS LTDA, Sefip, Caged, RAIS, DIRF, Caixa (conectividade social), CRCRN (portal da transparência), E-social, Ciee e rede interna do CRCRN (arquivos em excel e word).
d. compartilhamento - Os dados dos colaboradores são compartilhados no Sistema MASTERMAQ, Sistema SEI, IFOOD BENEFÍCIOS E SERVIÇOS LTDA, Sefip, Caged, RAIS, DIRF, Caixa (conectividade social), CRCRN (portal da transparência), E-social, Ciee e rede interna do CRCRN (arquivos em excel e word).

e. eliminação- Os dados não serão eliminados, tendo em vista a necessidade da criação de comissão interna para promover a análise para descarte de documentos, seguindo a tabela de temporalidade do CFC.

3.2 – ESCOPO DO TRATAMENTO

O CRCRN oferece diversos serviços à sociedade que exigem autenticação para acesso e tratamento de dados pessoais.

São eles:

- Identidade profissional
- Negociação de anuidades, multas e emolumentos;
- Acesso a cursos e eventos;
- Assinatura de conteúdo do portal;
- Emissão de DECORE;
- Prestação de contas do Programa de Educação Profissional Continuada (PEPC);
- Prestação de contas do COAF;
- Processo de fiscalização;
- Cadastro nacional de auditores independentes (CNAI);
- Cadastro Nacional de Auditores Independentes – Pessoa Jurídica (CNAI- PJ);
- Cadastro Nacional de Peritos Contábeis;
- Consultas a profissionais e organizações contábeis;
- Emissão de Certidão de Aprovação no Exame de Suficiência;
- Relação de aprovados nas edições do Exame de Suficiência;
- Canais de denúncia;
- Solicitações ouvidoria; e
- Pedidos de acesso à informação.

Para acessar os serviços supramencionados é necessário efetuar o cadastro no CRCRN, ocasião em que são solicitados dados como nome, e-mail, CPF, endereço, telefone, qualificação profissional, cópia de documento de identidade, entre outros, para que o usuário seja corretamente identificado e receba login e senha de autenticação.

Alguns dados pessoais podem ser obtidos por meio de fontes disponíveis em outros cadastros de governo e disponibilizados ao CFC/CRCs, de acordo com a legislação aplicável.

Contudo, o usuário poderá se desejar, ter acesso aos dados, editá-los e retificá-los sempre que estiverem incompletos desatualizados ou inexatos (conforme reza o art. 18 da LGPD).

3.3 – CONTEXTO DO TRATAMENTO

O Conselho Regional de Contabilidade do Rio Grande do Norte é uma Autarquia Especial Corporativa dotada de personalidade jurídica de direito público, criado por legislação específica, o Decreto-Lei nº 9.295, de 27 de maio de 1946.

O Conselho Regional de Contabilidade do Rio Grande do Norte trata os dados pessoais de acordo com os propósitos legítimos e específicos de modo compatível com a sua finalidade, cujo caráter é de interesse público, e objetivo executar as competências legais ou cumprir as atribuições legais e execuções contratuais/preliminares ao contrato.

Porém, algumas ações humanas verificadas no diagnóstico, na análise geral dos Projetos do CRCRN, colocam em risco os dados pessoais tratados pela entidade.

São elas:

- Utilização de PC/Notebook profissional para realização de atividades pessoais e particulares;
- Utilização de e-mail pessoal ou particular dentro do CRCRN;
- Utilização de Skype ou outras plataformas de comunicação on-line, vinculadas a contas particulares dentro da entidade;
- Utilização de dispositivos de armazenamento externo;
- Utilização de recursos para armazenamento de arquivos em nuvem vinculado a conta particular;
- Uso da impressora com frequência;
- Frequência no descarte de arquivos impressos;
- Acesso de e-mail corporativo em equipamento de uso pessoal;
- Utilização de e-mail profissional para tratar assuntos pessoais;
- Ausência de tratamento diferenciado para dados pessoais sensíveis;
- Ausência de tratamento diferenciado para dados de crianças e de adolescentes;
- Armazenamento e exclusão de dados.

4 – PARTES INTERESSADAS CONSULTADAS

Para confecção deste Relatório, Colaboradores de diversos projetos do Conselho

Regional de Contabilidade do Rio Grande do Norte (CRCRN) foram analisados. Realizaram-se avaliações de conformidade à LGPD, sob os aspectos culturais, operacionais e nos sistemas informatizados, segundo padrão metodológico baseado nas melhores práticas de proteção de dados. Foram mapeados todos os projetos constantes do Plano de Trabalho, destacando aqueles que possuem atividades fins de Conselho.

5 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Dentre os tipos de risco operacional verificados no diagnóstico, destacam-se os riscos à proteção de dados e informações armazenadas pela entidade, em especial aos dados pessoais sensíveis e dados de criança e adolescente.Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o ti- tular de dados pessoais e sobre o CRCRN.

Apresentam-se a seguir exemplos iniciais, não exaustivos, de riscos identificados e mensurados, de acordo com a metodologia de gerenciamento de riscos operacionais à proteção de dados pessoais:

a. vazamento de dados pessoais;
b. alteração de dados pessoais;
c. acesso indevido a dados pessoais;
d. perda de dados pessoais.

Seguindo as evidências de fragilidades listadas acima, a Matriz de Probabilidade de Impacto, ajuda na tomada de decisão com relação às sugestões de melhoria que serão disponibilizadas para adequação a LGPD. Esta ferramenta se mostra muito importante para a manutenção da entidade dentro da legislação, também utilizada pelo DPO/Encarregado e para atualização do DPIA, conforme exigência da Lei.

Parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Classificação	**Valor**
Baixo	5
Moderado	10

Alto	15

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a

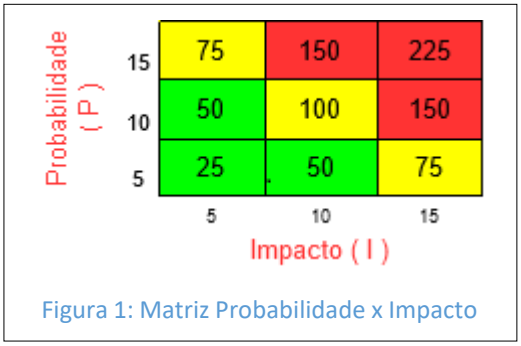

Figura 1: Matriz Probabilidade x Impacto

definição dos critérios de classificação do nível de risco.

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

- verde, é entendido como baixo;

- amarelo, representa risco moderado; e

- vermelho, indica risco alto.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**.

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	Retenção prolongada de dados pessoais sem necessidade, sem utilização de Tabela de Temporalidade oficial da entidade, especialmente em razão do tratamento de dados pessoais sensíveis.	10	15	150
R02	Bloqueio de PC/Notebook durante ausências	10	15	150
R03	Armazenamento de senhas.	10	15	150
R04	'Repasse' de senhas do PC/Notebook.	5	5	25
R05	Utilização de PC/Notebook profissional para realização de atividades pessoais e particulares.	15	15	225
R06	Utilização de e-mail pessoal ou particular dentro da empresa.	15	15	225

R07	Utilização de Skype ou outras plataformas de comunicação online, vinculadas a contas particulares dentro da empresa	15	15	225
R08	Utilização de dispositivos de armazenamento externo	15	15	225
R09	Utilização de recursos para armazenamento de arquivos em nuvem vinculado a conta particular.	15	15	225
R10	Costuma utilizar impressora? Com que frequência?	15	15	225
R11	Falta de recolhimento de arquivos impressos na bandeja das impressoras.	5	10	50
R12	Descarte de arquivos impressos	5	5	25
R13	Conhecimento sobre políticas de proteção de dados da empresa.	10	10	100
R14	Conhecimento sobre LGPD (Lei Geral de Proteção de Dados).	10	15	150
R15	Nível de acesso à rede	5	10	50
R16	Utilização de usuários próprios e 'repasse' de senhas para acesso à rede	5	15	75
R17	Repasse de senhas para acesso a softwares e sistemas	5	15	75

Id	**Risco referente ao tratamento de dados pessoais**	**P[1]**	**I[2]**	**Nível de Risco (P x I) [3]**
R18	Utilização de ferramentas de comunicação online	10	15	150
R19	Conhecimento sobre dados sensíveis	15	15	225
R20	Tratamento de dados de crianças e adolescentes sem necessidade e/ou dados de crianças e adolescentes não anonimizado	5	15	75
R21	Armazenamento e exclusão de dados	15	15	225

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

6 – MEDIDAS PARA TRATAR OS RISCOS

Para tratar os riscos acima mencionados é necessário que o Conselho Regional de Contabilidade do Rio Grande do Norte realize medidas de segurança técnicas e

administrativas de forma contínua.

Nesse sentido, pode a entidade decidir que alguns riscos são aceitáveis - até um risco de nível alto- devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação.

No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

Quanto às medidas de segurança administrativas, tem-se que as mesmas servem para garantir a efetiva proteção dos dados pessoais, não bastando a utilização de medidas técnicas, sendo imprescindível também a adoção de medidas de ordem administrativa, como a realização de treinamentos periódicos acerca da temática proteção de dados pessoais na entidade. Até mesmo porque nem todo vazamento decorre de violação do sistema de segurança, assim como nem todo tratamento incide sobre os dados pessoais on-line/digitais, mas também off-line/físicos, sendo possível, portanto, a causa decorrente de culpa ou dolo dos próprios colaboradores/usuários.

Isso reflete a necessidade de aplicação das regras de *Compliance*, visando alterar a cultura dos colaboradores, para fins de assegurar a observância das novas exigências legais. Isso corresponde ao incentivo ao desenvolvimento da cultura da privacidade e da proteção de dados pessoais dentro das entidades analisadas.

Para isso, é indispensável garantir internamente a difusão das Políticas e Normativas do Conselho Regional de Contabilidade do Rio Grande do Norte, especialmente voltada à gestão de dados pessoais, bem como a de privacidade do CRCRN. Tais regramentos devem ser seguidos, por meio da adoção de mecanismos de *Compliance* e implementação de boas práticas no tratamento dos dados pessoais, com a aplicação de treinamentos regulares com intervalos regrados a ser elaborado e definido pela *DPO*, de modo a garantir a fixação de controles internos e, via de consequência, a prevenção de condutas dos colaboradores emdesacordo com os comandos da LGPD.

Quanto às medidas técnicas voltadas a Segurança de Informação, faz-se necessária as seguintes implementações, consoante a Análise do Ambiente Tecnológico: Instalação e operacionalização do **firewall** no qual como dispositivo de segurança da rede que monitorará o tráfego de rede de entrada e saída e decide permitirá ou bloqueará tráfegos específicos de acordo com um conjunto definido de regras de segurança, deve ser aplicados testes de vulnerabilidade e intrusão periodicamente; análise periódica e verificação da necessidade de melhorias nas regras ou tratamento de ameaças; procedimentos e plano de resposta a incidentes de segurança documentados devem ser analisados se o procedimento segue os controles previstos no item 16 da ISO 27002; notificação de incidentes de segurança a clientes/consumidores adequado ao previsto na LGPD e controles previstos no item 16.1.2 da ISSO 27002.

Além disso, é necessário manter um cronograma periódico de verificação de vulnerabilidades e testes de instrução e na realização dos testes. No processo para remediação de vírus detectados não proativamente/automaticamente resolvidos pelos sistemas AV, sugere-se um procedimento formalizado para a prevenção e remediação em caso de ataques de códigos maliciosos, conforme previsto no item 5.1.1 da ISO 27002.

Ainda realizar procedimentos para que as transferências de informações sejam criptografadas, mascaradas ou anonimizadas, conforme descrito na LGPD, bem como as diretrizes da ISO 27002 em seu item 13.2.

Existem ferramentas do tipo "Security Information and Event Management (SIEM)" que podem ser configuradas para manter a gestão de logs e o gerenciamento de informações de segurança e de eventos para automatizar o processo de auditoria (a ISO 27002 no seu item 12.4 - Registros e monitoramento traz sugestões de boas práticas que podem ser adotadas para gestão de logs e incidentes).

É necessário que os sistemas bloqueiem o acesso após um número máximo de 5 tentativas de acesso, garantindo assim a proteção contra-ataques de força bruta.

É prudente que os usuários estejam cientes de que procedimentos básicos devem ser seguidos em uma emergência. Buscar treinamento, focado nas tecnologias disponíveis no CRCRN para os administradores de segurança.

Da mesma forma, mostra-se adequada a utilização de ferramenta de classificação das informações e que bloqueie o envio de documentos ou informação privadas para um distribuidor de e-mail não autorizado.

Dessa forma, o incremento de medidas técnicas a exemplo de um cadeado mais forte em uma janela que pode ser invadida; rotina de escaneamento de máquinas por meio de antivírus para a redução de riscos.

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	**ENCARREGADO**
Geovane Martins de Oliveira **Diretor Adm. Operacional** Natal/RN, 17/07/2023	Geovane Martins de Oliveira **DPO do CRCRN** Natal/RN, 17/07/2023

AUTORIDADE REPRESENTANTE DO CONTROLADOR	**AUTORIDADE REPRESENTANTE DO OPERADOR**
CONSELHO REGIONAL DE CONTABILIDADE DO RIO GRANDE DO NORTE Natal/RN, 17/07/2023	SPIDERWARE CONSULTORIA EM INFORMÁTICA LTDA Natal/RN, 17/07/2023