



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

MAPA DE GERENCIAMENTO DE RISCOS - LGPD

1. INTRODUÇÃO

A matriz ou mapa de riscos é uma ferramenta de gerenciamento que permite de forma visual identificar quais são os principais riscos e ameaças de segurança, e que devem receber mais atenção para a sua prevenção.

A avaliação deve ser recorrente e focada em tecnologia, nos processos e nas pessoas da instituição, e também, é importante que essa avaliação seja realizada após todos os processos serem mapeados.

A matriz de risco tem como características, entre outras: melhorar a conformidade evitando sanções por descumprimento da lei, ajuda a implementar medidas de segurança da informação, diminuir a probabilidade de incidentes e seus resultados negativos e trazer informações objetivas nas decisões estratégicas.

A **matriz de gerenciamento de riscos** prevista pela LGPD irá identificar, analisar e avaliar que fatores podem expor os dados que são tratados, sendo portanto primordial a proteção desses dados coletados, armazenados e processados digitalmente.

Elaborada de forma correta, identifica qual será a prioridade em esforços de proteção para evitar que riscos ocorram, podendo também corrigir falhas em segurança, em sistemas e acessos não autorizados.

Em uma instituição, o Encarregado de Dados tem a missão de contribuir e adotar medidas que estejam de acordo com os preceitos da LGPD.

A matriz de risco também compõe as etapas de elaboração do RIPD (Relatório de impacto à proteção de dados) .



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

2.FUNDAMENTAÇÃO

A Lei Geral de Proteção de Dados (LGPD 13709/2018) estabelece as bases legais para o tratamento de dados pessoais no Brasil, incluindo os princípios, direitos dos titulares, deveres dos controladores e operadores, e as penalidades aplicáveis em caso de descumprimento.

3. IDENTIFICAÇÃO DOS RISCOS E AÇÕES

Neste Mapa de Gerenciamento de Riscos vislumbram-se alguns riscos e ameaças que possam vir a comprometer a efetividade da proteção dos dados pessoais dos profissionais e demais indivíduos com os quais o Conselho Regional de Administração do Estado do Rio de Janeiro se relaciona.

Etapas para a elaboração do Mapa de Riscos:

1. Identificar os dados sensíveis: dados pessoais, profissionais, empresariais, etc
2. Identificar onde estão os dados: sistemas, nuvens, etc.
3. Identificar quais são os riscos: perda de dados, acesso não autorizado, uso indevido, etc.
4. Criar uma matriz de monitoramento, incluindo ações imediatas para pontos críticos e pontos de atenção;
5. Implementar medidas de prevenção;
6. Acompanhamento contínuo e revisão da matriz de riscos;



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.

DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.

DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.

DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

3.1 Avaliação de riscos de segurança e privacidade

Tipo de Risco	Descrição	Medidas Mitigadoras	Impacto x Probabilidade
1	Acesso não autorizado no Sistema	Fortalecimento de senhas, firewalls, segurança de rede	3
2	Perda de dados	Back up regulares	3
3	Falhas no processo de armazenamento e monitoramento de dados	Criptografias, controles de acesso	6
4	Necessidade de permitir acesso ao banco de dados	Criptografia	6
5	Falta de análise periódica sobre os dados coletados	Estabelecer cronograma periódico	2
6	Falta de conscientização dos colaboradores da instituição quanto a privacidade dos dados coletados	Treinamento de pessoal	3
7	Fornecer dados para órgão de pesquisa	Anonimização de dados	3
8	Falha ou falta de backup e criptografia em dados do Sistema	Testar periodicamente a restauração dos backups para garantir sua integridade e funcionalidade.	3
9	Roubo de dados	Senhas fortes, Criptografia, políticas de segurança	3
10	Compartilhamento de dados não realizados por meio criptografado	Treinamento de pessoal, criptografia e gerenciamento de acessos.	2



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

3.2 ESTIMATIVA DE RISCOS

Legenda de cores referente a riscos:

Verde : **Baixo**

Amarelo : **Moderado**

Vermelho : **Alto**

Matriz impacto x probabilidade

Impacto X Probabilidade	Riscos com ocorrência significativamente Baixas 1	Riscos com ocorrências significativamente Medianas 2	Riscos com ocorrências significativamente Altas 3
Baixa probabilidade 1	1	2	3
Media probabilidade 2	2	4	6
Alta probabilidade 3	3	6	9

Escala de Impacto

Diretriz	Nível
Alto	3
Médio	2
Baixo	1

Escala de Probabilidade

Diretriz	Nível
Alto	3
Médio	2
Baixo	1



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

4. MEDIDAS DE SEGURANÇA

As medidas de segurança visam proteger tanto os sistemas quanto os dados armazenados pelo CRA-RJ.

Considerando a infraestrutura disponível no CRA-RJ pode-se relacionar as seguintes ações:

4.1 Segurança de Rede e Infraestrutura:

Uso de Firewalls e VPNs : Garantia de proteção de dados durante a transmissão, especialmente para acessos remotos ao SIFA e sistemas corporativos. A implementação de uma VPN (Rede Privada Virtual) pode ser essencial para conexões externas.

Monitoramento de Rede : Uso de ferramentas de monitoramento para identificar e bloquear tentativas de acessos não autorizados ou invasões aos servidores.

Segurança na Nuvem (AWS) : A AWS oferece uma série de certificações e medidas de segurança, como criptografia de dados em trânsito e segurança, detecção de anomalias, gerenciamento de identidade e acesso (IAM) para controle granular de permissões, e backups automáticos e replicação de dados.

4.2 Proteção de Dados Armazenados:

Criptografia de Dados Sensíveis : Tanto no ERP SIFA quanto no sistema da Alterdata, dados pessoais e financeiros devem ser criptografados. Isso garante que, mesmo em caso de violação, as informações sejam ilegíveis sem as chaves de descriptografia.

Controle de Acesso Baseado em Funções (RBAC) : Implementação de acesso restrito aos dados, conforme a necessidade da carga ou função. Apenas funcionários do RH, por exemplo, devem ter acesso aos dados pessoais armazenados no Alterdata.

Segurança dos Arquivos Físicos : A empresa GRM deve adotar medidas de segurança física, como controle de acesso a arquivos físicos e monitoramento de seu movimento. O armazenamento deve seguir protocolos de integridade e auditoria.

4.3 Segurança de Sistemas:

Atualizações e Patches Regulares : Tanto o ERP SIFA quanto os sistemas de Alterdata e o armazenamento na AWS precisam ser mantidos atualizados sempre com os últimos patches de segurança, garantindo proteção contra vulnerabilidades conhecidas.

Antivírus e Antimalware : Todos os dispositivos que acessam os sistemas devem estar protegidos por soluções de antivírus e antimalware, e devem ser feitas varreduras regulares em busca de ameaças.



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

4.4 Plano de Recuperação de Desastres (DRP) e Continuidade de Negócios (BCP):

Backups Regulares e Armazenamento Seguro : Implementação de políticas específicas de backup de dados, com cópias armazenadas de maneira segura na AWS e, se necessário, fora do ambiente de produção.

Plano de Recuperação : Desenvolvimento de um plano detalhado para restauração rápida dos sistemas em caso de falhas ou ataques cibernéticos, como ransomware.

4.5 Treinamento e Conscientização:

Capacitação de Funcionários : Programas regulares de treinamento para conscientizar todos os funcionários sobre boas práticas de segurança cibernética, como reconhecimento de demonstração de phishing e gerenciamento de senhas

5. SISTEMA E PRIVACIDADE

O sistema de privacidade refere-se ao tratamento seguro e adequado dos dados pessoais, conforme regulamentações como a LGPD (Lei Geral de Proteção de Dados).

Neste contexto, podemos relacionar as seguintes medidas:

5.1 Conformidade com a LGPD:

Tratamento de Dados Pessoais : O sistema da Alterdata, que contém dados de funcionários e conselheiros, e o ERP SIFA, que processa informações administrativas e financeiras, deve estar em conformidade com a LGPD, garantindo que os titulares de dados tenham ciência sobre a coleta, processamento e armazenamento de suas informações.

Bases Legais para o Tratamento : Todos os dados pessoais (de pessoas físicas) devem ter uma base legal justificada para o tratamento, como o consentimento explícito, a execução de contratos ou a obrigação legal/regulatória.

Gerenciamento de Consentimento : O CRA-RJ precisa obter o consentimento adequado dos titulares de dados para as especificações específicas de uso, especialmente ao tratar de dados sensíveis.



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

5.2 Privacidade e Segurança de Dados:

Proteção de Dados Pessoais na Nuvem : A AWS oferece uma série de soluções para atender às exigências de privacidade da LGPD, como segregação de dados, criptografia e ferramentas de auditoria para verificar quem acessa as informações e nesse contexto.

Gerenciamento de Incidentes : Procedimentos claros para relatar incidentes de segurança que possam comprometer a privacidade dos dados, garantindo uma notificação às autoridades competentes e aos titulares de dados em tempo hábil, conforme exigido pela LGPD.

5.3 Retenção e Descarte de Dados:

Política de Retenção : Estabelecimento de uma política de retenção de dados que garante que as informações pessoais sejam armazenadas apenas pelo tempo necessário para o cumprimento de suas finalidades.

Descarte Seguro : Os dados pessoais, tanto digitais quanto físicos (armazenados pela GRM), devem ser eliminados de forma segura, no tempo adequado e por ordem formal do Presidente ou pessoa por ele designada, assegurando que as informações confidenciais sejam completamente inacessíveis, prevenindo qualquer uso indevido.

5.3.1 Metodologia de Descarte :

Dados Físicos:

Trituração (Shredding): Papéis, documentos e mídias físicas podem ser triturados em fragmentos pequenos, tornando impossível a reconstrução e leitura.

Dados Digitais:

- Formatação Segura (Secure Erasure): Apagar arquivos de discos rígidos ou SSDs por meio de software especializado que sobrescreve os dados diversas vezes, garantindo que não possam ser recuperados.
- Criptografia Irrecuperável (Cryptographic Erasure): Destruição das chaves de criptografia, tornando os dados criptografados permanentemente inacessíveis.
- Destruição Física de Mídias: Para discos rígidos e outros dispositivos de armazenamento, métodos como perfuração, trituração ou incineração podem ser utilizados para garantir que os dados não possam ser recuperados.

Cada método deve ser escolhido de acordo com o nível de sensibilidade dos dados e a conformidade com normas de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD).



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.
DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DO RIO DE JANEIRO / CRA-RJ

Autarquia Federal de fiscalização profissional (Lei nº4.769/65)
Rua Professor Gabizo, 197, Ed. Belmiro Siqueira, Tijuca – Rio de Janeiro/RJ CEP 20271-064
Site: www.cra-rj.org.br

5.4 Gestão de Contratos com Terceiros:

Acordos de Confidencialidade : Contratos firmados com terceiros que armazenam dados, como AWS, Alterdata e GRM, devem incluir cláusulas específicas de proteção de dados e confidencialidade, garantindo que essas empresas estejam em conformidade com a LGPD e ofereçam as devidas proteções.

5.5 Direitos dos Titulares de Dados:

Atendimento às Solicitações : Implementação de um processo para atender às obrigações dos titulares de dados, que podem querer acessar, corrigir, remover ou transferir suas informações. O sistema da Alterdata e o ERP SIFA devem ser capazes de responder a essas demandas com eficiência.

Elaboração :

Adm Paulo Coelho

CRA _RJ 20-17518

Chefe de Ouvidoria e

Encarregado de Proteção de Dados (DPO).

Adm. Leonardo Fuerth

CRA-RJ 20-22222

Superintendente Geral

Adm. Rafaela Ferreira

CRA-RJ 20-101867

Administradora- Superintendência

Apresentado e referendado na Sessão Plenária CRA-RJ 4206 de 07.10.24



DOCUMENTO ASSINADO POR RAFAELA MAIA DE LIMA FERREIRA EM 14/10/2024 ÀS 15:59:03 DO HORÁRIO DE BRASÍLIA.

DOCUMENTO ASSINADO POR PAULO CESAR CARVALHO COELHO EM 14/10/2024 ÀS 16:41:14 DO HORÁRIO DE BRASÍLIA.

DOCUMENTO ASSINADO POR LEONARDO RIBEIRO FUERTH EM 14/10/2024 ÀS 16:05:37 DO HORÁRIO DE BRASÍLIA.

DOCUMENTO ASSINADO POR LOGIN E SENHA, PARA VALIDAR ACESSO <http://sistemacrarj.com.br/assinaturas/validarAssinatura/YV284271> OU UTILIZE O QR CODE.