

TERMO DE NOMEAÇÃO DE ENCARGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

VEROCHEQUE REFEIÇÕES LTDA., pessoa jurídica devidamente inscrita no CNPJ sob o n.º 06.344.497/0001-41, localizada na Avenida Presidente Vargas, 2001, Conjunto 174, Jardim Santa Ângela, CEP n.º 14.020 525, Ribeirão Preto, São Paulo neste ato representada por seu CEO e, ora, membro executivo, Sr. NICOLAS TEIXEIRA VERONEZI, doravante denominada simplesmente "EMPRESA";

CONSIDERANDO o disposto no art. 41 da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), que determina a nomeação de um Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO);

CONSIDERANDO a Resolução CD/ANPD nº 18, de 16 de julho de 2024, que aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais;

RESOLVE:

Art. 1º Nomear **Caio Gonzalez y Gonzalez**, para exercer a função de Encarregado(a) pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO) do(a) CONTROLADOR(A).

*Parágrafo único. As informações de contato profissional do(a) Encarregado(a) são:

- **E-mail:** caio@verocard.com.br
- **Telefone:** 16 4009-9543
- **Endereço:** Avenida Presidente Vargas, 2001, Conjunto 174, Jardim Santa Ângela, CEP n.º 14.020 525, Ribeirão Preto, São Paulo

Art. 2º São atribuições do(a) Encarregado(a), sem prejuízo de outras que venham a ser estabelecidas em normas complementares:

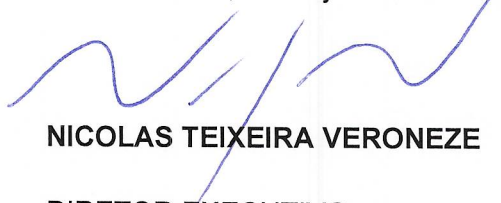
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas da ANPD, em especial as atividades descritas no art. 16 do Regulamento aprovado pela Resolução CD/ANPD nº 18, de 16 de julho de 2024.

Art. 3º O(A) Encarregado(a) atuará com autonomia e independência no exercício de suas funções, reportando-se diretamente à [alta administração/diretoria] do(a) CONTROLADOR(A).

Art. 4º Na ausência, impedimentos e vacâncias do(a) Encarregado(a), a função será exercida interinamente por Suelen Palareto Maciel.

Art. 5º Este Termo de Nomeação entra em vigor na data de sua publicação, devendo ser divulgado publicamente, de forma clara e objetiva, no sítio eletrônico do(a) CONTROLADOR(A), em conformidade com o § 1º do art. 41 da LGPD.

Ribeirão Preto, 18 de janeiro de 2024.



NICOLAS TEIXEIRA VERONEZE

DIRETOR EXECUTIVO

VEROCHEQUE REFEIÇÕES LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – (“PSI”) **Verocheque Refeições Ltda. (Verocard)**

1. Objetivo

Essa política tem como objetivo formalizar aos colaboradores da Verocheque Refeições Ltda (Verocard) as diretrizes aqui estabelecidas e conscientizar a todos quanto ao bom uso das informações, boa conduta e aderência a PSI, garantindo aderência às normas legais, em especial à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), bem como às diretrizes internas de governança, segurança da informação e compliance corporativo.

Seu propósito é assegurar que todos os dados sob custódia da Verocheque Refeições Ltda (Verocard) sejam mantidos em segurança.

2. Comitê de Segurança da Informação

O Comitê de Segurança da Informação (CSI), ora constituído no presente instrumento, terá como objetivo maior a função de manter e aprimorar a PSI e bem como elevar a maturidade da organização quanto aos assuntos referentes a SI. Este comitê é multidisciplinar e capaz de apoiar todos os colaboradores no esclarecimento e aderência aos assuntos relacionados à SI.

Todos os informativos e reportes ao CSI se faz pelo e-mail:

- privacy@verocard.com.br

2.1. O comitê é formado por representantes das áreas:

- Tecnologia da Informação (Governança, Infraestrutura e Segurança da Informação);
- Jurídico;
- Compliance;

2.2. Responsabilidades

- Garantir que as diretrizes definidas na PSI sejam compreendidas por todos;
- Avaliar e definir novos controles e serem aplicados a PSI;

- Apoiar a SI na definição de ações para contornar possíveis incidentes de segurança;
- Avaliar a aplicabilidade de sanções administrativas para os casos de não cumprimento da PSI e demais normas relacionadas.

2.3. Colaboradores:

- Todos os colaboradores terão conhecimento pleno das diretrizes definidas na PSI, e, todos deverão praticá-las;
- Tratar todas as informações conforme o seu tipo e a sua classificação; Reportar qualquer violação da PSI a SI através do e-mail privacy@verocard.com.br
- Disseminar a cultura da Segurança da Informação para todos os outros colaboradores;

2.4. Diretores:

- Aprovar a PSI e demais documentos relacionados;
- Promover a melhoria contínua da PSI;
- Validar e aprovar as diretrizes definidas pelo CSI;
- Avaliar a aplicabilidade de sanções administrativas para os casos de não cumprimento da PSI e demais normas relacionadas.
- Cumprir e fazer cumprir os controles definidos na PSI para seus pares; Dar o exemplo no cumprimento das diretrizes estabelecidas.

2.5. Gestores:

- Garantir e/ou fiscalizar as diretrizes definidas na PSI, para que sejam cumpridas por todos;
- Promover a melhoria contínua da PSI;
- Dar o exemplo no cumprimento das diretrizes estabelecidas.

2.6. Contratados, parceiros e fornecedores:

- Estar aderente a PSI e aos demais controles estabelecidos;
- Reportar qualquer violação ou não conformidade com a PSI.

2.7. Gestão de Gente

- Atuar visando dar ciência de todos os colaboradores quanto ao conteúdo da PSI;
- Aplicar sanções administrativas aos colaboradores pelo não cumprimento da PSI, quando aplicável.

2.8. Jurídico

- Avaliar a PSI no âmbito jurídico para que ela esteja sempre aderente as leis e regulamentações;
- Apoiar na definição de diretrizes para a PSI.

2.9. Segurança da Informação

- Apoiar o CSI na definição de diretrizes e continuidade da PSI;
- Avaliar juntamente com o CSI as medidas de contorno dos incidentes reportados;
- Realizar trabalhos focados na divulgação da PSI;
- Analisar incidentes de segurança da informação reportados;
- Auditar os processos e ativos de TIC no âmbito de segurança.

2.10. Tecnologia da Informação

- Atuar proativamente reportando e analisando falhas de SI;
- Apoiar o CSI e SI na implementação de controles.

3. **Classificação da Informação**

Considera-se que as informações sendo elas físicas, digitais ou faladas, devem possuir a sua devida classificação feita pelos seus proprietários, pois garante o acesso ou limita-o de pessoas não autorizadas. Tais informações, que foram criadas, armazenadas ou alteradas são definitivamente de propriedade da Veroqueque Refeições Ltda (Verocard) e devem ser manuseadas da forma correta.

4. **Confidencial**

As informações de caráter confidencial devem ser preservadas devido a sua alta criticidade e por conter informações estratégicas, podendo ser acessada por um número restrito de pessoas.

Tais informações possuem sérios impactos sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

Entende-se como documentos Confidenciais: Documentos pessoais de clientes/usuários, Objetivos estratégicos, contratos, holerites, relatórios gerenciais, código fonte, relatório de transações e dados pessoais.

5. Restrita

As informações rotuladas como restrita, estão limitadas apenas a um grupo de pessoas, departamento ou segregadas por um assunto.

O acesso de pessoas não autorizadas pode gerar conflitos internos, impacto de imagem ou perda de competitividade.

Entende-se como documentos restritos: Pasta de arquivos departamentais, planejamento estratégico, planilhas contábeis, controles.

6. Interna

São as informações que estão disponíveis a todos os colaboradores, mas sem a previa autorização para divulgação externa.

A divulgação das informações internas pode afetar a imagem da organização e/ou também dos colaboradores.

Entende-se como documentos internos: Lista de ramais, Lista de aniversariantes, Eventos internos, metas departamentais.

7. Pública

São informações sem restrições de acesso e disponíveis para visualização através dos canais de comunicação.

Estas informações podem ser compartilhadas caso necessário obedecendo a fonte que define a sua origem.

Entende-se como documentos públicos: Textos informativos sobre eventos,

informações contidas no site ou redes sociais.

8. Backup

O backup das informações é realizado periodicamente conforme a política estabelecida, incluindo os principais sistemas, arquivos departamentais e de usuários, e, ainda, nos exatos termos da Política de Retenção e Descarte, além do constante na Política de Privacidade de Dados, tudo sob deliberação do Comitê de Dados e do Comitê de segurança da Informação.

9. Conformidade

A Verocheque Refeições Ltda (Verocard), através dessa política, definiu suas diretrizes com embasamento nas melhores práticas de mercado e no conjunto de normas específicas da Segurança da Informação, e logo atendendo as conformidades de leis e regulamentações que implicam a essa organização.

10. Aderência da PSI

Todos os colaboradores devem ter o conhecimento das diretrizes estabelecidas na PSI e demais normas relacionadas.

Para os eventuais casos de violação das diretrizes da PSI, estas serão avaliadas pelo CSI em que julgara a necessidade de se aplicar sanções administrativas ou medidas legais.

11. Incidente de segurança

Os incidentes relacionados à SI devem ser reportados via e-mail privacy@verocard.com.br para que seja analisado pela área de SI. Fica a critério da área de SI eleger estes incidentes para a pauta do CSI para discussão e direcionamentos.

12. Monitoramento

A Verocheque Refeições Ltda (Verocard) monitora os serviços principais que atribuem o direito aos colaboradores de alterarem as suas informações, visando preservar os direitos sobre as informações derivadas da sua atuação empresarial e garantir um ambiente mais seguro. Diante disso poderá auditar a qualquer momento os serviços de e-mail, conta telefônica, Internet, sistemas,

dentre outros, gerando evidências para comprovação de algum incidente de segurança.

A auditoria deve ser realizada perante a aprovação da Diretoria.

13. Revisão da PSI

As revisões da PSI, são feitas a cada 1 ano ou sempre em que houver alterações no ambiente atual, e, ainda, conforme definido no Comitê de Dados e/ou de Segurança da Informação.

14. Normas Gerais

Uso do e-mail

O uso do e-mail deve ser praticado por todos de forma consciente para que não traga danos ao ambiente e não seja penalizado pelo uso indevido da ferramenta. A utilização do e-mail corporativo é permitida a todos os colaboradores e alguns terceiros, tendo como domínio principal **@VEROCARD.com.br**. Outros domínios podem ser criados conforme a necessidades do negócio.

Não é permitido:

- Utilizar o e-mail para armazenar e/ou compartilhamento mensagens de correntes, difamatórias, eróticas, ofensivas, racistas, dentre outros;
- Utilizar o e-mail corporativo para cadastro em sites, e-commerce, campanhas promocionais, dentre outros;
- Alterar a estrutura (histórico) dos e-mails ao respondê-lo;
- Se passar ou responder por outro colaborador nos e-mails;
- Enviar e-mails com usuário e senha no mesmo e-mail;
- Compartilhar caixas de e-mail com outros colaboradores;
- O bom uso do e-mail cabe a todos e pode ser melhor entendido através do manual de boas práticas do uso do e-mail.

Uso da Internet

A Internet é uma ferramenta de trabalho e deve ser utilizada por todos os colaboradores e terceiros de forma consciente. O acesso é liberado para todos os colaboradores através de perfis específicos para cada função. O ambiente é monitorado com o objetivo de identificar acessos indevidos e obter

rastreabilidade do tráfego. Caso for identificado o uso indevido da Internet o responsável pelo acesso será penalizado após a análise do CSI e RH.

Não é permitido:

- Utilizar de mecanismos para burlar as políticas de acesso à Internet;
- Utilizar a internet para entretenimento, como rádios, jogos online e filmes;
- Efetuar downloads que impactem o bom funcionamento da rede;
- Utilizar o upload de arquivos para ambientes que não sejam os homologados pela TI do Grupo Verocheque Refeições Ltda (Verocard). Devem ser utilizadas ferramentas disponíveis e homologada pela Verocheque Refeições Ltda (Verocard);

As exceções devem ser avaliadas e aprovadas.

Mesa e tela limpa

As informações quando físicas (impressas) ou até mesmo em formato digital, devem ser posicionadas de maneira organizada para impossibilitar o acesso indevidos. A classificação da informação deve ser considerada para que o tratamento seja adequado.

Todos os colaboradores devem:

- Fora do expediente de trabalho todos os documentos como documentos impressos, mídias eletrônicas e demais objetos sejam guardados em local seguro, como armários com chave, cofres, ou qualquer tipo de mobília;
- Todas as estações de trabalho devem ser desligadas no final do expediente;
- Sempre que se ausentar da estação de trabalho a tela deve ser bloqueada através da combinação de teclas (Win + L);
- Sempre que possível evitar a impressão de documentos sensíveis. Caso necessário retirá-las imediatamente da impressora.

Recursos computacionais

Todos os recursos computacionais são fornecidos aos colaboradores para desempenho das atividades profissionais e devem ser manuseados de forma adequada. Por esse motivo a Verocheque Refeições Ltda (Verocard) não permite a utilização de recursos computacionais particulares.

O colaborador e / ou terceiro através dos recursos computacionais não devem infringir os controles de SI aplicados.

Software

A Verocheque Refeições Ltda (Verocard) apoia e respeita a propriedade intelectual, portanto não é permitida a pirataria. A instalação de software não homologados está passível de aprovação.

Toda nova instalação ou remoção de aplicativos devem ser tratados via chamado pela TI.

Antivírus

O antivírus é uma ferramenta que minimiza os riscos de infecções provenientes do uso inadequado da Internet ou dispositivos externos. Deste modo todas as estações de trabalho devem possuir este controle de segurança ativo e atualizado.

A tentativa de desativação é considerada violação da PSI.

Redes sociais

O uso de redes sociais utilizando recursos corporativos é permitido apenas como ferramenta de trabalho.

Cabe a todos os colaboradores:

- Não publicar qualquer tipo de informações da Verocheque Refeições Ltda (Verocard), como fotos internas, eventos, reuniões;
- A publicação é permitida apenas com a autorização da área de RH.
- Não participar de fóruns de discussão ou debates que tratem assuntos pornográficos, racistas, dentre outros, de denigrem a imagem e conduta;
- É permitido o compartilhamento de informações apenas que foram postadas pelas áreas autorizadas pela comunicação interna;
- Qualquer ação que viole essa política identificado nas redes sociais devem ser reportados para privacy@verocard.com.br para que seja avaliado.

Uso de senhas

- As senhas de acessos são condições mínimas para acessar qualquer ambiente de informação e devem ser asseguradas individualmente por todos.

- As senhas devem conter no mínimo 8 caracteres, dentre letras maiúsculas, letras minúsculas, números, e caractere especial;
- As senhas expiram em 60 dias;
- Não utilização das últimas 3 senhas;
- As senhas devem ser alteradas sempre em que houver suspeita de violação;
- A senha é pessoal e intransferível, por isso não deve ser passado a outra pessoa;
- Evitar salvar a senha (memorizada) em navegadores;
- Portais disponibilizados a clientes externos (alunos, professores, pais e outros) deve seguir um mínimo esforço, tendo ao menos 2 combinações acima.

Contratação e rescisão de contratos

O processo de contratação e rescisão devem ser feitos de forma segura para todos os candidatos, conforme a ética, regulamentações e leis vigentes, para que evite riscos, principalmente aos casos em que o colaborador ou terceiro acesse informações sensíveis ou tenha contato direto com os processos críticos.

Rescisão do contrato

- A comunicação deve ser feita com antecedência a TI para que as devidas medidas de segurança sejam tomadas;
- Os acessos aos sistemas e demais ambientes devem ser revogados e as informações devem ser contidas e asseguradas;

Trabalho remoto

O trabalho remoto sempre que acordado deve ser realizado de forma segura, seguindo todos os procedimentos e uso de tecnologias homologadas pela Verocheque Refeições Ltda (Verocard).

Todos devem:

- Avaliar a segurança física do local de onde será realizado o acesso;
- Evitar a utilização de redes públicas para acesso remoto;
- Utilizar sempre a VPN para acesso remoto;
- Utilizar apenas máquinas homologadas e de propriedade da Verocheque Refeições Ltda (Verocard) para acesso remoto;
- O acesso remoto deve ser realizado a partir de máquinas com firewall e

- antivírus ativo e atualizado;
- O acesso remoto deve ser realizado somente para suporte ou consulta ao sistema, mudanças devem ser evitadas;
- Caso seja realizado o empréstimo de notebook, telefone móvel, o qualquer outro dispositivo eletrônico para a realização de atividades externas, o mesmo deve ser devolvido imediatamente;
- Aplica-se aos terceiros:
- Os acessos devem ser feitos conforme os procedimentos padrão;
- Devem ser feitos apenas em horário comercial; ou,
- Acesso fora do horário comercial, finais de semana ou feriados, devem ser solicitados através do processo de aprovação;
- Os acessos aos sistemas, base de dados, devem ser feitos apenas em ambiente de homologação;
- As mudanças realizadas por terceiros devem ser evitadas;
- Todo terceiro deve possuir seu login de acesso a VPN individual;

Descarte de informações

O descarte correto das informações que contém conteúdo sensíveis ou não, devem ser feitos de forma segura e controlada nos termos da referida política e guia procedimental.

Casos em as informações estejam armazenadas em mídias, estas devem ser feitas pela TI.

As informações impressas devem ser descartadas pelos donos da informação.

Para que o descarte seja feito de forma segura deve-se:

- Todas as mídias assim que tornar-se em desuso devem ser destruídas através de incineração ou trituração;
- Caso as mídias sejam reutilizadas, deve-se fazer a cópia segura das informações atuais e reutilizada para o mesmo fim, nunca deve ser direcionada para outra unidade;
- O descarte deve ser registrado para que se tenha rastreabilidade;
- Os documentos sensíveis, que foram impressos devem ser descartados através de desfragmentadoras de papel;
- As informações escritas em lousas devem ser apagadas após o uso;
- Os materiais físicos utilizados em reuniões devem ser retirados das salas ou descartado.

Mudanças

A formalização das mudanças que visam atender os requisitos do negócio, sendo elas em sistemas ou de infraestrutura, ajudam a minimizar os riscos no negócio como indisponibilidades por longos períodos.

Para atender os requisitos de mudança todos devem:

- Utilizar o formulário padrão de mudanças;
- As requisições de mudanças devem passar por um processo de aprovação;
- Um planejamento prévio deve ser realizado e formalizado;
- A comunicação deve ser efetiva e envolver as pessoas chave.

Nomeação

Nomear os seguintes colaboradores para compor o Comitê de Segurança da Informação:

NOME COMPLETO DO MEMBRO	CARGO	ÁREA DE REPRESENTAÇÃO
Nicolas Teixeira Veronezi	Diretor Executivo	Diretoria
José Francisco Clemente	Diretor de TI	TI
Caio Gonzalez y Gonzalez	DPO	Compliance

A atuação dos membros no Comitê é considerada de relevante interesse para a ORGANIZAÇÃO e não será remunerada adicionalmente, sendo as atividades desenvolvidas em horário de expediente normal.

O mandato dos membros ora nomeados será de 2 anos, permitida a recondução, entrando em vigor na data de sua assinatura e, na ausência de qualquer documento em sentido contrário, os nomeados acima poderão ter a nomeação renovada sucessivamente, ficando o colaborador, abaixo indicado, como responsável pela gestão e administração do comitê ora nomeado;

Caio Gonzalez y Gonzalez, para exercer a função de Responsável pelo Comitê de Segurança da Informação, órgão gestor da presente PSI.

*Parágrafo único. As informações de contato profissional do(a) colaborador(a)

são:

- **E-mail:** caio@verocard.com.br
- **Telefone:** 16 4009-9543
- **Endereço:** Avenida Presidente Vargas, 2001. Conj 174. Jd. Santa Ângela. 14020-525. Ribeirão Preto/SP.

Data de aprovação: 17 de janeiro de 2025

Documento controlado – uso interno restrito à Verocheque Refeições Ltda (Verocard).

TERMO DE NOMEAÇÃO DE MEMBROS DO COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

VEROCHEQUE REFEIÇÕES LTDA., pessoa jurídica devidamente inscrita no CNPJ sob o n.º 06.344.497/0001-41, localizada na Avenida Presidente Vargas, 2001, Conjunto 174, Jardim Santa Ângela, CEP n.º 14.020 525, Ribeirão Preto, São Paulo neste ato representada por seu CEO e, ora, membro executivo, Sr. NICOLAS TEIXEIRA VERONEZI, doravante denominada simplesmente “EMPRESA”;

CONSIDERANDO a instituição do Comitê de Privacidade e Proteção de Dados Pessoais, por meio do(a) termo de instituição, datado de 18/01/2025;

CONSIDERANDO a necessidade de designar os representantes das áreas que comporão o referido Comitê, conforme o Art. 3º do mencionado ato de instituição;

RESOLVE:

Art. 1º Nomear os seguintes colaboradores para compor o Comitê de Privacidade e Proteção de Dados Pessoais da ORGANIZAÇÃO:

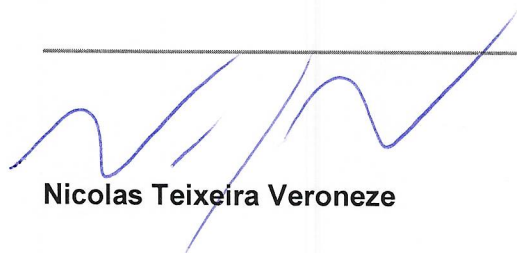
NOME COMPLETO DO MEMBRO	CARGO	ÁREA DE REPRESENTAÇÃO
Nicolas Teixeira Veronezi	Diretor Executivo	Diretoria
José Francisco Clemente	Diretor de TI	TI
Caio Gonzalez y Gonzalez	DPO	Compliance

Art. 2º A atuação dos membros no Comitê é considerada de relevante interesse para a ORGANIZAÇÃO e não será remunerada adicionalmente, sendo as atividades desenvolvidas em horário de expediente normal.

Art. 3º O mandato dos membros ora nomeados será de 1 (hum) ano, permitida a recondução.

Art. 4º Este Termo de Nomeação entra em vigor na data de sua publicação.

Ribeirão Preto, 18 de janeiro de 2025.



Nicolas Teixeira Veroneze

Diretor Executivo
VEROCHEQUE REFEIÇÕES LTDA.

TERMO DE INSTITUIÇÃO DO COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

VEROCHEQUE REFEIÇÕES LTDA., pessoa jurídica devidamente inscrita no CNPJ sob o n.º 06.344.497/0001-41, localizada na Avenida Presidente Vargas, 2001, Conjunto 174, Jardim Santa Ângela, CEP n.º 14.020 525, Ribeirão Preto, São Paulo neste ato representada por seu CEO e, ora, membro executivo, Sr. NICOLAS TEIXEIRA VERONEZI, doravante denominada simplesmente "EMPRESA";

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais para proteger os direitos fundamentais de liberdade e de privacidade;

CONSIDERANDO a necessidade de estabelecer uma estrutura de governança em privacidade e proteção de dados para garantir a conformidade com a LGPD e outras regulamentações aplicáveis;

CONSIDERANDO a importância de promover uma cultura de proteção de dados em toda a ORGANIZAÇÃO, por meio de orientação, conscientização e supervisão contínua;

RESOLVE:

Art. 1º Fica instituído o Comitê de Privacidade e Proteção de Dados Pessoais (doravante denominado Comitê), órgão consultivo e deliberativo, de caráter permanente, com o objetivo de assessorar a alta administração e supervisionar a implementação das ações necessárias ao cumprimento da LGPD no âmbito da ORGANIZAÇÃO.

Art. 2º Compete ao Comitê:

I - Propor, revisar e acompanhar a implementação do Programa de Governança em Privacidade e da Política de Proteção de Dados Pessoais da ORGANIZAÇÃO; II - Avaliar os mecanismos de tratamento e proteção de dados existentes e propor ações voltadas ao seu aperfeiçoamento; III - Orientar as áreas de negócio e de apoio sobre as melhores práticas de privacidade e proteção de dados; IV - Promover a disseminação da cultura de proteção de dados, por meio de treinamentos, comunicados e outras ações de conscientização; V - Monitorar o cumprimento das obrigações estabelecidas na LGPD e nas políticas internas, em colaboração com o Encarregado pelo Tratamento de Dados Pessoais (DPO); VI - Analisar relatórios de impacto à proteção de dados pessoais (RIPD) e opinar sobre as medidas de mitigação de riscos propostas; VII - Assessorar a alta administração na tomada de decisões estratégicas que envolvam o tratamento

de dados pessoais; VIII - Propor a elaboração e a revisão de normas internas relacionadas à privacidade e proteção de dados.

Art. 3º O Comitê será composto por membros titulares e suplentes, representantes das seguintes áreas:

- Diretoria Executiva
- Encarregado pelo Tratamento de Dados Pessoais (DPO)
- Tecnologia da Informação (TI)

Parágrafo único. A nomeação dos membros do Comitê será formalizada em termo próprio, que especificará os representantes de cada área.

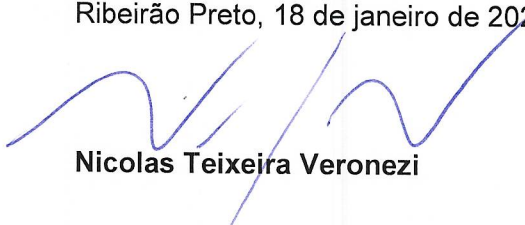
Art. 4º O Comitê será coordenado pelo Encarregado pelo Tratamento de Dados Pessoais (DPO).

Art. 5º O Comitê se reunirá ordinariamente a cada três meses e, extraordinariamente, sempre que convocado por seu Coordenador ou pela maioria de seus membros.

Parágrafo único. As deliberações e os encaminhamentos das reuniões serão registrados em atas.

Art. 6º Este Termo de Instituição entra em vigor na data de sua publicação.

Ribeirão Preto, 18 de janeiro de 2025.



Nicolas Teixeira Veronezi

Diretor Executivo

VEROCHEQUE REFEIÇÕES LTDA.

Registro de Operações de Tratamento de Dados Pessoais (ROPA)

Controlador: Verocard / Verocheque Refeições LTDA

CNPJ: 06.344.497/0001-41

Endereço: Ribeirão Preto/SP

Encarregado de Dados (DPO): Caio Gonzalez y Gonzalez

E-mail do DPO: privacy@verocard.com.br

Data de Elaboração: 18 de janeiro de 2025

Versão: 1.0

Introdução

Este Registro de Operações de Tratamento de Dados Pessoais (ROPA) foi elaborado em conformidade com o artigo 37 da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que determina que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

O ROPA tem como objetivo documentar de forma clara e organizada todas as operações de tratamento de dados pessoais realizadas pela Verocard no âmbito da prestação de serviços de administração, gerenciamento, emissão, distribuição e fornecimento de cartões de Vale-Alimentação/Refeição, permitindo o controle, a transparência e a conformidade com a LGPD.

Este ROPA deve ser revisado e atualizado periodicamente, especialmente quando houver:

- Novas operações de tratamento de dados pessoais
- Alterações nas finalidades ou bases legais
- Mudanças nos destinatários de compartilhamento
- Atualizações na legislação aplicável
- Incidentes de segurança que impactem o tratamento de dados

A manutenção atualizada do ROPA é fundamental para demonstrar a conformidade com a LGPD e facilitar o atendimento a solicitações da ANPD ou dos titulares de dados.

OPERAÇÃO 1: Cadastramento de Beneficiários

Identificação da Operação

Nome da Operação: Cadastramento de Beneficiários de Vale-Alimentação/Refeição

Área Responsável: Cadastro e Gestão de Benefícios

Responsável pela Operação: Suelen Palareto

Papel da Verocard: Controlador

Finalidade do Tratamento

Cadastrar os colaboradores do Cliente como beneficiários do vale-alimentação/refeição para viabilizar a emissão dos cartões e a prestação do serviço contratado.

Base Legal (LGPD)

Art. 7º, V - Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados Cadastrais	Nome completo, CPF, nome do pai, nome da mãe, data de nascimento	Não
Dados de Contato	Telefone, celular, e-mail	Não
Dados Profissionais	Nome da empresa empregadora (Organização Estadual do Cliente), cargo/função	Não

Origem dos Dados

- **Fonte:** Cliente (contratante)
- **Forma de Coleta:** Fornecimento pela empresa contratante por meio de arquivo eletrônico ou sistema integrado

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Operadora Contábil	Cumprimento de obrigações fiscais e trabalhistas	Brasil	Art. 7º, II (cumprimento de obrigação legal)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Prazo indeterminado, com prazo mínimo de 5 (cinco) anos contados após o fim da relação de consumo, conforme artigos 12 e 34 do Código de Defesa do Consumidor. Os dados podem ser mantidos por período superior quando houver motivo legal, ordem judicial, prevenção à fraude ou outros interesses legítimos.

Medidas de Segurança

- Controle de acesso baseado em perfis (apenas colaboradores autorizados)
- Login individual com senhas alfanuméricas
- Logs de acesso
- Firewall e antivírus
- Termo de Sigilo e Confidencialidade assinado pelos colaboradores
- Armazenamento em servidores seguros (data center no Brasil)

Forma de Eliminação

- Eliminação definitiva do software da Verocard
- Trituração de documentos físicos (quando aplicável)
- Possibilidade de anonimização para fins estatísticos

OPERAÇÃO 2: Emissão de Cartões

Identificação da Operação

Nome da Operação: Emissão de Cartões de Vale-Alimentação/Refeição

Área Responsável: Operações e Produção de Cartões

Responsável pela Operação: Suelen Palareto

Papel da Verocard: Controlador

Finalidade do Tratamento

Emitir cartões eletrônicos personalizados com chip e tarja magnética para os beneficiários cadastrados, viabilizando o uso do benefício na rede credenciada.

Base Legal (LGPD)

Art. 7º, V - Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados Cadastrais	Nome completo, CPF, nome dos pais, data de nascimento	Não
Dados do Cartão	Número do cartão, 4 últimos dígitos	Não

Origem dos Dados

- **Fonte:** Base de dados interna da Verocard (cadastro de beneficiários)
- **Forma de Coleta:** Processamento interno a partir dos dados cadastrados

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Fornecedor de Cartões (se aplicável)	Produção física dos cartões	Brasil	Art. 7º, V (execução de contrato)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Prazo indeterminado, com prazo mínimo de 5 (cinco) anos contados após o fim da relação de consumo. Os dados podem ser mantidos por período superior quando houver motivo de lei, ordem judicial, prevenção à fraude ou outros interesses legítimos.

Medidas de Segurança

- Controle de acesso restrito à área de produção
- Sistema de câmeras CFTV
- Criptografia de dados sensíveis do cartão
- Logs de produção e emissão
- Firewall e antivírus

Forma de Eliminação

- Eliminação definitiva do software da Verocard
- Destruição segura de cartões não utilizados ou cancelados



OPERAÇÃO 3: Autenticação no Aplicativo/Portal

Identificação da Operação

Nome da Operação: Autenticação de Beneficiários no Aplicativo/Portal Web

Área Responsável: Tecnologia da Informação

Responsável pela Operação: José Francisco Clemente

Papel da Verocard: Controlador

Finalidade do Tratamento

Autenticar os beneficiários no aplicativo móvel ou portal web para permitir acesso seguro às funcionalidades de consulta de saldo, extrato, bloqueio/desbloqueio de cartão e troca de senha.

Base Legal (LGPD)

Art. 7º, V - Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados de Contato	Telefone, e-mail	Não
Dados de Autenticação	Senha de acesso (criptografada)	Não
Dados de Navegação	Endereço IP, logs de acesso, dispositivo utilizado	Não

Origem dos Dados

- **Fonte:** Cadastro pelo próprio titular no aplicativo/portal
- **Forma de Coleta:** Cadastro voluntário pelo beneficiário

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Provedor de Infraestrutura aplicável (se)	Hospedagem do aplicativo/portal	Brasil	Art. 7º, V (execução de contrato)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Logs de acesso: 6 meses

Dados de autenticação: Prazo indeterminado, enquanto o beneficiário mantiver conta ativa, com prazo mínimo de 5 anos após o encerramento.

Medidas de Segurança

- Criptografia de senhas (hash)
- Autenticação segura (HTTPS)
- Logs de acesso para auditoria
- Firewall e proteção contra ataques (DDoS, SQL Injection)
- Monitoramento de tentativas de acesso não autorizado

Forma de Eliminação

- Eliminação definitiva dos logs após o prazo de retenção
- Eliminação da conta e dados de autenticação mediante solicitação do titular ou após o prazo de retenção

OPERAÇÃO 4: Processamento de Transações

Identificação da Operação

Nome da Operação: Processamento de Transações de Compra na Rede Credenciada

Área Responsável: Operações e Processamento de Pagamentos

Responsável pela Operação: Daniel Lopes Ramos

Papel da Verocard: Controlador



Finalidade do Tratamento

Processar as transações de compra realizadas pelos beneficiários na rede credenciada de supermercados, restaurantes e similares, autorizando ou negando a transação conforme saldo disponível e regras do PAT.

Base Legal (LGPD)

- **Art. 7º, V** - Execução de contrato
- **Art. 7º, II** - Cumprimento de obrigação legal (PAT)
- **Art. 7º, IX** - Legítimo interesse (prevenção à fraude)

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados do Cartão	Número do cartão, senha de acesso	Não
Dados Transacionais	Nome do estabelecimento, data e hora da transação, valor, localização geográfica, tipo de produto/serviço	Não
Dados Financeiros	Saldo disponível, histórico de créditos	Não

Origem dos Dados

- **Fonte:** Captura automática no momento da transação
- **Forma de Coleta:** Sistema de ponto de venda (POS) do estabelecimento credenciado

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Estabelecimentos Credenciados	Processamento da transação	Brasil	Art. 7º, V (execução de contrato)
Processadores de Pagamento / Bandeira	Liquidação financeira da transação	Brasil	Art. 7º, V (execução de contrato)



Destinatário	Finalidade	Localização	Base Legal
Cliente (contratante)	Relatórios gerenciais e comprovação do serviço	Brasil	Art. 7º, V (execução de contrato)
Receita Federal	Cumprimento de obrigações do PAT	Brasil	Art. 7º, II (cumprimento de obrigação legal)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Prazo indeterminado, com prazo mínimo de 5 (cinco) anos contados após o fim da relação de consumo. Dados fiscais podem ser mantidos conforme legislação tributária (até 5 anos após a declaração).

Medidas de Segurança

- Criptografia de dados em trânsito (TLS/SSL)
- Tokenização de dados sensíveis do cartão
- Sistema de detecção de fraudes (análise de padrões)
- Logs de transações para auditoria
- Firewall e antivírus
- Monitoramento em tempo real

Forma de Eliminação

- Eliminação definitiva do software após o prazo de retenção
- Possibilidade de anonimização para fins estatísticos

OPERAÇÃO 5: Atendimento ao Titular

Identificação da Operação

Nome da Operação: Atendimento ao Titular (SAC, Bloqueio, Desbloqueio, 2ª Via, Extrato, Troca de Senha)

Área Responsável: Atendimento ao Cliente

Responsável pela Operação: Thais Helena Albino

Papel da Verocard: Controlador



Finalidade do Tratamento

Atender às solicitações dos titulares relacionadas ao uso do cartão, incluindo bloqueio e desbloqueio, emissão de 2ª via, fornecimento de extrato, troca de senha e esclarecimento de dúvidas.

Base Legal (LGPD)

Art. 7º, V - Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados Cadastrais	CPF, nome completo, nome dos pais, data de nascimento	Não
Dados do Cartão	4 últimos dígitos do cartão	Não
Dados Profissionais	Nome da empresa empregadora	Não
Dados Transacionais	Último estabelecimento utilizado, estabelecimento frequente	Não
Dados de Contato	Telefone, e-mail	Não

Origem dos Dados

- **Fonte:** Fornecimento pelo próprio titular no momento do atendimento
- **Forma de Coleta:** Telefone, e-mail, chat, aplicativo

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Não há compartilhamento externo nesta operação.

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Registros de atendimento: 5 anos



Dados cadastrais utilizados: Prazo indeterminado (já armazenados na operação de cadastramento)

Medidas de Segurança

- Validação de identidade do titular antes de fornecer informações ou realizar operações
- Gravação de chamadas (quando aplicável, com aviso prévio ao titular)
- Controle de acesso aos sistemas de atendimento
- Logs de atendimento para auditoria
- Treinamento de atendentes sobre LGPD e proteção de dados

Forma de Eliminação

- Eliminação definitiva dos registros de atendimento após o prazo de retenção
- Exclusão de gravações de chamadas conforme política de retenção

OPERAÇÃO 6: Mudança de Domicílio Bancário

Identificação da Operação

Nome da Operação: Mudança de Domicílio Bancário do Beneficiário

Área Responsável: Cadastro e Gestão de Benefícios

Responsável pela Operação: Suelen Palareto

Papel da Verocard: Controlador

Finalidade do Tratamento

Processar solicitações de mudança de domicílio bancário dos beneficiários, atualizando os dados bancários para crédito de eventuais reembolsos ou devoluções.

Base Legal (LGPD)

Art. 7º, V - Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados de Identificação	Foto de identificação com documento (selfie), CPF, RG	Não



Categoria	Dados Específicos	Sensível?
Dados Bancários	Banco, agência, conta, tipo de conta, comprovante de conta (folha de cheque, foto do cartão, extrato, certificado de MEI ou contrato social)	Não
Dados de Contato	Telefone de contato	Não

Origem dos Dados

- **Fonte:** Fornecimento pelo próprio titular
- **Forma de Coleta:** Formulário eletrônico, e-mail ou aplicativo

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Instituição Financeira	Processamento de pagamentos/reembolsos	Brasil	Art. 7º, V (execução de contrato)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Prazo indeterminado, com prazo mínimo de 5 (cinco) anos contados após o fim da relação de consumo.

Medidas de Segurança

- Validação de identidade por meio de foto com documento (selfie)
- Criptografia de dados bancários
- Controle de acesso restrito
- Logs de alterações cadastrais
- Armazenamento seguro de documentos

Forma de Eliminação

- Eliminação definitiva do software após o prazo de retenção
- Trituração de documentos físicos (quando aplicável)



OPERAÇÃO 7: Gestão de Créditos Mensais

Identificação da Operação

Nome da Operação: Gestão e Creditação de Valores Mensais nos Cartões

Área Responsável: Financeiro e Gestão de Benefícios

Responsável pela Operação: Suelen Palareto

Papel da Verocard: Controlador

Finalidade do Tratamento

Processar os valores mensais a serem creditados nos cartões dos beneficiários conforme contrato firmado entre Verocard e Cliente.

Base Legal (LGPD)

Art. 7º, V - Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados Cadastrais	Nome completo, CPF	Não
Dados Financeiros	Valor do benefício mensal, histórico de créditos, saldo disponível	Não
Dados do Cartão	Número do cartão	Não

Origem dos Dados

- **Fonte:** Cliente (contratante) e base de dados interna da Verocard
- **Forma de Coleta:** Arquivo eletrônico fornecido pelo contratante

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Operadora Contábil	Registro contábil e fiscal	Brasil	Art. 7º, II (cumprimento de obrigação legal)
Cliente (contratante)	Relatórios de créditos realizados	Brasil	Art. 7º, V (execução de contrato)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Prazo indeterminado, com prazo mínimo de 5 (cinco) anos contados após o fim da relação de consumo. Dados fiscais podem ser mantidos conforme legislação tributária.

Medidas de Segurança

- Controle de acesso restrito à área financeira
- Criptografia de dados financeiros
- Logs de operações de crédito
- Conciliação bancária periódica
- Firewall e antivírus

Forma de Eliminação

- Eliminação definitiva do software após o prazo de retenção
- Possibilidade de anonimização para fins estatísticos

OPERAÇÃO 8: Prevenção à Fraude e Segurança

Identificação da Operação

Nome da Operação: Monitoramento e Prevenção à Fraude

Área Responsável: Compliance e Segurança da Informação

Responsável pela Operação: Caio Gonzalez y Gonzalez

Papel da Verocard: Controlador



Finalidade do Tratamento

Monitorar transações e padrões de uso dos cartões para identificar e prevenir fraudes, protegendo os titulares e a Verocard de prejuízos financeiros.

Base Legal (LGPD)

Art. 7º, IX - Legítimo interesse do controlador, desde que não prevaleçam direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados Transacionais	Histórico de compras, padrões de uso, localização geográfica, horários, valores, estabelecimentos	Não
Dados do Cartão	Número do cartão, 4 últimos dígitos	Não
Dados de Navegação	Endereço IP, logs de acesso	Não

Origem dos Dados

- **Fonte:** Captura automática de transações e acessos
- **Forma de Coleta:** Sistemas de processamento de transações e aplicativo/portal

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Autoridades Policiais/Judiciárias	Investigação de fraudes (quando solicitado)	Brasil	Art. 7º, II (cumprimento de obrigação legal)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Logs de monitoramento: 6 meses a 1 ano



Registros de fraudes identificadas: 5 anos (para fins de defesa em processos)

Medidas de Segurança

- Sistema de detecção de anomalias e padrões suspeitos
- Alertas automáticos para transações atípicas
- Bloqueio preventivo de cartões em caso de suspeita de fraude
- Logs de auditoria
- Equipe treinada em análise de fraudes

Forma de Eliminação

- Eliminação definitiva dos logs após o prazo de retenção
- Anonimização de dados para análise estatística de padrões de fraude

OPERAÇÃO 9: Relatórios Gerenciais e Cumprimento do PAT

Identificação da Operação

Nome da Operação: Geração de Relatórios Gerenciais e Cumprimento de Obrigações do PAT

Área Responsável: Financeiro e Compliance

Responsável pela Operação: Caio Gonzalez y Gonzalez

Papel da Verocard: Controlador

Finalidade do Tratamento

Gerar relatórios gerenciais para o Cliente (contratante) e relatórios para cumprimento das obrigações do Programa de Alimentação do Trabalhador (PAT) junto à Receita Federal.

Base Legal (LGPD)

- **Art. 7º, V** - Execução de contrato (relatórios ao Cliente)
- **Art. 7º, II** - Cumprimento de obrigação legal (relatórios ao PAT/Receita Federal)

Dados Pessoais Tratados

Categoria	Dados Específicos	Sensível?
Dados Cadastrais	Nome, CPF (quando exigido pela legislação)	Não

Categoria	Dados Específicos	Sensível?
Dados Financeiros	Valor do benefício, total de créditos	Não
Dados Transacionais	Histórico de uso, estabelecimentos, valores (agregados ou individualizados conforme exigência legal)	Não

Origem dos Dados

- **Fonte:** Base de dados interna da Verocard (operações anteriores)
- **Forma de Coleta:** Processamento interno

Titulares dos Dados

Colaboradores do Cliente beneficiários do vale-alimentação/refeição.

Compartilhamento de Dados

Destinatário	Finalidade	Localização	Base Legal
Cliente (contratante)	Relatórios gerenciais e comprovação do serviço	Brasil	Art. 7º, V (execução de contrato)
Receita Federal	Cumprimento de obrigações do PAT	Brasil	Art. 7º, II (cumprimento de obrigação legal)

Transferência Internacional

Não há transferência internacional de dados.

Período de Retenção

Prazo indeterminado, com prazo mínimo de 5 (cinco) anos. Relatórios fiscais podem ser mantidos conforme legislação tributária (até 5 anos após a declaração).

Medidas de Segurança

- Controle de acesso restrito aos sistemas de relatórios
- Criptografia de dados em trânsito
- Logs de geração e envio de relatórios
- Anonimização ou agregação de dados quando possível



Forma de Eliminação

- Eliminação definitiva após o prazo de retenção legal
- Anonimização para fins estatísticos

Controle de Versões

Versão	Data	Responsável	Descrição das Alterações
1.0	15/01/2025	Caio Gonzalez y Gonzalez (DPO)	Versão inicial do ROPA

Assinaturas:



Encarregado de Dados (DPO):

Caio Gonzalez y Gonzalez

E-mail: privacy@verocard.com.br

Data: 18/01/2025



Responsável Legal:

Nicolas Veronezi

Cargo: Diretor Executivo

Data: 18/01/2025

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

1. Sumário Executivo

Este Relatório de Impacto à Proteção de Dados Pessoais (RIPD) foi elaborado para analisar o tratamento de dados pessoais no âmbito da prestação de serviços de administração, gerenciamento, emissão, distribuição e fornecimento de cartões de Vale-Alimentação/Refeição promovido pela O objetivo é descrever o fluxo de dados, identificar e avaliar os riscos aos direitos e liberdades dos titulares e detalhar as medidas de mitigação adotadas, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. O tratamento de dados é essencial para a execução do contrato e para o cumprimento de obrigações legais, como as do Programa de Alimentação do Trabalhador (PAT).

2. Descrição do Tratamento de Dados Pessoais

2.1. Natureza e Finalidade do Tratamento

O tratamento de dados pessoais tem como finalidade principal a operacionalização do benefício de vale-alimentação/refeição para os colaboradores do Cliente. As operações de tratamento incluem:

- **Coleta e Cadastro:** Recebimento dos dados dos colaboradores para emissão dos cartões e criação de contas.
- **Gerenciamento de Créditos:** Processamento dos valores mensais a serem creditados nos cartões.
- **Processamento de Transações:** Autorização e registro de compras realizadas na rede credenciada.
- **Atendimento e Suporte:** Utilização de dados para atender a solicitações dos titulares (consulta de saldo, bloqueio, etc.).
- **Prevenção à Fraude:** Monitoramento de transações para identificar atividades suspeitas.
- **Cumprimento de Obrigações Legais:** Geração de relatórios e informações exigidas pela legislação do PAT e outras normas fiscais e trabalhistas.

2.2. Agentes de Tratamento e Compartilhamento de Dados

- **Controlador:** A Verocard (Verocheque Refeições LTDA, CNPJ 06.344.497/0001-41) atua como controladora dos dados pessoais, sendo responsável pelas decisões referentes às finalidades e meios de tratamento.
- **Operadores:** A Verocard se utiliza de operadores para viabilizar o serviço, incluindo:
 - **Rede Credenciada:** Supermercados, restaurantes e similares que recebem os pagamentos.

- **Processadores de Pagamento e Bandeiras:** Empresas que liquidam as transações.
- **Provedores de Tecnologia:** Empresas que fornecem a infraestrutura de TI (servidores, nuvem, etc.).
- **Compartilhamento:** Os dados são compartilhados com o Cliente (relatórios gerenciais), com a rede credenciada (para efetivar a transação) e, quando necessário, com autoridades governamentais para cumprimento de obrigações legais.

2.3. Tipos de Dados Pessoais Tratados

Categoria de Dados	Exemplos de Dados Tratados
Dados Cadastrais	Nome completo, CPF, RG, data de nascimento, endereço, telefone, e-mail.
Dados Profissionais	Matrícula, cargo, unidade de lotação (Organização Estadual do Cliente).
Dados Financeiros	Valor do benefício, histórico de créditos, saldo do cartão.
Dados de Autenticação	Senha de acesso (criptografada).
Dados Transacionais	Histórico de compras, nome do estabelecimento, data, hora, valor e localização da transação.
Dados de Navegação	Endereço IP, logs de acesso ao portal/aplicativo.

2.4. Ciclo de Vida dos Dados

- **Coleta:** Os dados são fornecidos pelo Cliente no momento da contratação e adesão dos colaboradores.
- **Armazenamento:** Os dados são armazenados em ambiente de nuvem seguro, com criptografia e controles de acesso rigorosos.
- **Retenção:** Os dados são mantidos durante a vigência do contrato e, após o término, pelo prazo necessário para cumprimento de obrigações legais e regulatórias (pelo menos 5 anos, considerando prazos prescricionais trabalhistas e fiscais).
- **Eliminação:** Findo o prazo de retenção e a necessidade legal, os dados são eliminados definitivamente do software da Verocard. Documentos físicos, quando existentes, são triturados. Os dados podem ser utilizados de forma anonimizada para fins estatísticos, caso em que não mais se caracterizam como dados pessoais.

3. Bases Legais para o Tratamento

O tratamento de dados pessoais realizado pela Verocard está fundamentado nas seguintes bases legais da LGPD:

- **Execução de Contrato (Art. 7º, V):** É a base legal primária, pois o tratamento é indispensável para fornecer o benefício de vale-alimentação/refeição conforme acordado entre a Verocard e o Cliente, em favor dos titulares.
- **Cumprimento de Obrigação Legal ou Regulatória (Art. 7º, II):** O tratamento é necessário para cumprir as exigências do Programa de Alimentação do Trabalhador (PAT), regulamentado pelo Decreto nº 10.854/2021, e outras obrigações fiscais e trabalhistas.
- **Legítimo Interesse (Art. 7º, IX):** Utilizado para atividades de prevenção à fraude e garantia da segurança das operações, sempre em equilíbrio com os direitos e liberdades dos titulares.
- **Exercício Regular de Direitos em Processo (Art. 7º, VI):** Os dados podem ser mantidos para defesa da Verocard em eventuais processos judiciais, administrativos ou arbitrais.

4. Avaliação da Necessidade e Proporcionalidade

O tratamento de dados é considerado **necessário** para a finalidade proposta, uma vez que sem os dados cadastrais, financeiros e transacionais, seria impossível emitir os cartões, creditar os valores e processar as compras. A coleta de dados é **proporcional**, limitando-se ao mínimo indispensável para a prestação do serviço. Não são coletados dados sensíveis, a menos que estritamente necessário e com base legal apropriada, o que não se aplica ao escopo padrão deste serviço. As medidas de segurança implementadas são adequadas à natureza e à sensibilidade dos dados tratados. O período de retenção, embora indicado como "prazo indeterminado" na política interna, respeita o prazo mínimo legal de 5 anos e pode ser estendido apenas quando houver fundamento legal ou legítimo interesse devidamente justificado.

5. Análise de Riscos e Medidas de Mitigação

A avaliação de riscos foi realizada considerando a probabilidade de ocorrência de cada evento de risco e o impacto potencial sobre os direitos e liberdades dos titulares. A metodologia adotada classifica a probabilidade em três níveis (Baixa, Média e Alta) e o impacto em quatro níveis (Baixo, Médio, Alto e Crítico). O nível de risco é calculado multiplicando-se a probabilidade pelo impacto, resultando em uma escala de 1 a 12, classificada em Risco Baixo (1-2), Risco Moderado (3-4), Risco Alto (6-8) e Risco Crítico (9-12).

Para cada risco identificado, foram analisadas as consequências potenciais para os titulares e documentadas as medidas de mitigação implementadas pela Verocard. A avaliação considerou tanto riscos técnicos (relacionados à segurança da informação) quanto riscos organizacionais (relacionados a processos e governança).

A tabela abaixo resume os principais riscos identificados, a avaliação de seu impacto e probabilidade, e as medidas adotadas para mitigá-los.

Risco	Nível	Descrição	Medidas de Mitigação Implementadas
1. Acesso Não Autorizado	Alto	Acesso indevido a dados por pessoas não autorizadas, internas ou externas.	- Controle de acesso baseado em função (RBAC) - Autenticação multifator (MFA) - Criptografia de dados em trânsito e em repouso - Monitoramento contínuo de logs de acesso - Testes de invasão periódicos
2. Uso Inadequado de Dados	Alto	Utilização dos dados para finalidades distintas das informadas, como marketing não consentido.	- Política de Privacidade clara - Treinamento sobre LGPD para colaboradores - Segregação de dados por finalidade - Auditorias internas de conformidade
3. Compartilhamento Inadequado	Alto	Transferência de dados para terceiros sem as devidas garantias contratuais e de segurança.	- <i>Due diligence</i> de fornecedores - Cláusulas contratuais de proteção de dados - Compartilhamento do mínimo de dados necessário (minimização)

Risco	Nível	Descrição	Medidas de Mitigação Implementadas
			- Monitoramento da conformidade de parceiros
4. Vazamento de Dados	Moderado	Exposição accidental ou criminosa de dados pessoais em larga escala.	- Plano de Resposta a Incidentes - Sistemas de detecção de intrusão (IDS/IPS) - Notificação à ANPD e aos titulares, se necessário - Seguro de responsabilidade cibernética
5. Retenção Excessiva	Moderado	Manutenção de dados por tempo superior ao legalmente permitido ou necessário.	- Política de Retenção e Descarte de Dados - Processos automatizados para eliminação de dados - Revisão periódica dos prazos de retenção
6. Falha no Atendimento aos Direitos Titulares	Moderado	Demora ou falha em responder às solicitações dos titulares (acesso, correção, etc.).	- Canal de comunicação dedicado ao titular - Procedimentos internos para atendimento em até 15 dias - Designação de um Encarregado de Dados (DPO)

6. Direitos dos Titulares

A Verocard garante aos titulares o pleno exercício de seus direitos, conforme o Art. 18 da LGPD. Um canal de comunicação direto com o Encarregado de Dados (DPO) está disponível para que os titulares possam solicitar:

- Confirmação da existência do tratamento.
- Acesso aos seus dados.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários.
- Portabilidade dos dados a outro fornecedor.
- Informação sobre o compartilhamento de seus dados.
- Revogação do consentimento, quando aplicável.

7. Medidas de Segurança Implementadas

A Verocard adota medidas de segurança de dados, tanto internas quanto externas, físicas e digitais, para garantir aos titulares o máximo de proteção quanto às suas informações pessoais. As medidas implementadas incluem:

Segurança Física: Sistema de câmeras de segurança CFTV nas instalações, controle de acesso físico às áreas restritas, armários com fechadura para armazenamento de documentos físicos, e trituração de documentos ao final do prazo de retenção.

Segurança Lógica: Sistema de servidor interno e sistema de servidor externo em data center localizado no Brasil, firewall e antivírus atualizados, logs de acesso para rastreabilidade de operações, login individual para cada colaborador com senhas alfanuméricas, controle de acesso baseado em perfis e privilégios, e criptografia de senhas de acesso dos titulares.

Segurança Organizacional: Política de Privacidade e Proteção de Dados documentada, Política de Segurança da Informação específica, Termo de Sigilo e Confidencialidade assinado por todos os colaboradores, treinamento sobre LGPD e proteção de dados, procedimentos internos para tratamento de dados, e Encarregado de Dados (DPO) designado.

As normas de segurança da informação e prevenção contra incidentes de dados pessoais são detalhadas na Política de Segurança da Informação da Verocard e nas normativas internas e documentos concernentes ao tema.

8. Direitos dos Titulares

A Verocard reforça seu compromisso de respeito aos direitos dos titulares de dados pessoais, conforme o artigo 18 da LGPD. Os titulares podem exercer seus direitos por meio do canal de

comunicação com o Encarregado de Dados (DPO) no e-mail privacy@verocard.com.br. Os direitos assegurados são:

Confirmação da Existência do Tratamento: O titular pode questionar se há a realização de operações de tratamento relativos aos seus dados pessoais.

Acesso aos Dados: O titular pode solicitar e receber cópia de todos os dados pessoais coletados e armazenados pela Verocard.

Correção de Dados: O titular pode requisitar a correção de dados pessoais que estejam incompletos, inexatos ou desatualizados.

Anonimização, Bloqueio ou Eliminação: O titular pode requisitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, salvo se houver motivo legítimo para sua manutenção, como obrigação legal de retenção ou necessidade para execução do contrato.

Portabilidade dos Dados: O titular pode requisitar que seus dados pessoais sejam disponibilizados a outro fornecedor de serviço, respeitados os limites técnicos da infraestrutura.

Informação sobre Compartilhamento: O titular tem direito de obter informações sobre as entidades públicas e privadas com as quais a Verocard compartilhou seus dados.

Revogação do Consentimento: Quando o tratamento for baseado em consentimento, o titular tem direito a revogá-lo a qualquer momento, sem afetar a legalidade do tratamento realizado anteriormente. A Verocard informará as consequências da revogação.

Oposição ao Tratamento: Nas hipóteses de tratamento não baseadas em consentimento, o titular poderá apresentar oposição, que será analisada a partir dos critérios presentes na LGPD.

9. Conclusão e Parecer do Encarregado

O tratamento de dados pessoais para a prestação do serviço de vale-alimentação/refeição é realizado de forma a cumprir com as obrigações contratuais e legais, buscando sempre o equilíbrio com a proteção da privacidade dos titulares. Os riscos identificados são endereçados por um conjunto robusto de medidas técnicas, administrativas e organizacionais.

Recomenda-se a implementação e o monitoramento contínuo das medidas de mitigação descritas, bem como a revisão periódica deste RIPD, especialmente em caso de mudanças significativas no escopo do tratamento. Com as salvaguardas atuais, o tratamento é considerado adequado e em conformidade com a LGPD.

Parecer: Favorável à continuidade do tratamento, com a condição de que as medidas de mitigação sejam mantidas e aprimoradas continuamente.

Encarregado pela Proteção de Dados (DPO): Caio Gonzalez y Gonzalez
caio@verocard.com.br

Aprovação: Nicolas Teixeira Veronezi em 18 de janeiro de 2025

POLÍTICA DE RETENÇÃO DE DADOS

Verocheque Refeições Ltda (Verocard)

1. OBJETIVO

A presente Política de Retenção de Dados estabelece os critérios, procedimentos e responsabilidades aplicáveis ao armazenamento, à conservação, à revisão e à eliminação de dados pessoais, sensíveis e corporativos tratados pela Verocheque Refeições Ltda (Verocard), garantindo aderência às normas legais, em especial à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), bem como às diretrizes internas de governança, segurança da informação e compliance corporativo.

Seu propósito é assegurar que todos os dados sob custódia da Verocheque Refeições Ltda (Verocard) sejam mantidos apenas pelo período estritamente necessário ao atendimento das finalidades legítimas para as quais foram coletados, resguardando-se, simultaneamente, os direitos dos titulares, a segurança jurídica da empresa e a rastreabilidade de suas operações.

2. ABRANGÊNCIA

Esta política é aplicável a todos os departamentos, colaboradores, prestadores de serviço, parceiros comerciais, fornecedores e terceiros que, sob qualquer forma, realizem o tratamento de dados em nome ou por determinação da Verocheque Refeições Ltda (Verocard), abrangendo todas as operações que envolvam coleta, produção, recepção, classificação, utilização, acesso, transmissão, armazenamento, eliminação, avaliação ou controle da informação, tanto em meio físico quanto digital.

3. PRINCÍPIOS E FUNDAMENTOS

A Verocheque Refeições Ltda (Verocard) observa, no tratamento e retenção de dados, os seguintes princípios institucionais:

Finalidade e adequação: todo tratamento deve possuir propósito legítimo, explícito e compatível com as atividades empresariais e com o contexto de coleta.

Necessidade e proporcionalidade: devem ser armazenados apenas os dados estritamente indispensáveis à execução da finalidade proposta.

Temporalidade limitada: os dados serão conservados apenas pelo tempo necessário ao cumprimento da finalidade ou das obrigações legais e contratuais.

Segurança e integridade: o armazenamento deve ocorrer sob padrões de proteção técnica e administrativa capazes de impedir perda, alteração, acesso indevido, vazamento ou qualquer forma de tratamento irregular.

Transparência e governança: todos os titulares têm direito à informação clara e acessível quanto aos prazos e critérios de retenção adotados.

Responsabilização: os agentes de tratamento devem adotar medidas preventivas e corretivas para garantir o cumprimento integral desta política.

4. CLASSIFICAÇÃO DOS DADOS

Para fins de gestão e aplicação desta política, as informações tratadas pela Verocheque Refeições Ltda (Verocard) são classificadas da seguinte forma:

Dados pessoais: informações relacionadas a pessoa natural identificada ou identificável, como nome, CPF, e-mail, telefone, endereço e dados bancários.

Dados sensíveis: dados referentes à origem racial ou étnica, convicções religiosas, opiniões políticas, saúde, vida sexual, dados genéticos ou biométricos.

Dados corporativos: registros operacionais, contratos, comunicações comerciais, relatórios de auditoria, documentos contábeis e fiscais.

Dados técnicos e de autenticação: logs de acesso, identificadores eletrônicos, registros de uso de sistema e metadados associados a transações.

5. DIRETRIZES GERAIS DE RETENÇÃO

Os dados deverão ser armazenados apenas pelo período necessário à execução da finalidade que motivou sua coleta, acrescido dos prazos prescricionais aplicáveis para eventual defesa de direitos da Verocheque Refeições Ltda (Verocard).

Decorrido o prazo de retenção, os dados deverão ser eliminados ou anonimizados de forma segura, observadas as restrições legais, regulatórias ou contratuais vigentes.

Em caso de litígio, investigação ou auditoria, os dados poderão ser retidos até a conclusão do procedimento, mediante justificativa formal e registro de retenção extraordinária.

6. TABELA DE PRAZOS DE RETENÇÃO

Categoria de Dados	Finalidade / Base Legal	Prazo de Retenção	Destinação Final
Dados cadastrais de clientes, usuários e beneficiários	Execução contratual, prevenção à fraude e atendimento pós-venda	5 anos após o encerramento da relação contratual	Eliminação definitiva ou anonimização segura
Registros de transações financeiras e operacionais	Processamento de pagamentos, controle contábil e obrigações fiscais	10 anos após a operação	Arquivamento seguro e eliminação após decurso do prazo prescricional

Categoria de Dados	Finalidade / Base Legal	Prazo de Retenção	Destinação Final
Dados de colaboradores e ex-colaboradores	Execução de obrigações trabalhistas, previdenciárias e fiscais	10 anos após o término do vínculo	Arquivamento obrigatório e eliminação após o período legal
Documentos fiscais, contábeis e societários	Cumprimento de obrigações tributárias e auditoria externa	5 a 10 anos conforme a natureza do documento	Descarte controlado e registro de eliminação
Logs de sistemas e registros de acesso	Segurança da informação, rastreabilidade e prevenção de incidentes	6 meses a 1 ano	Exclusão ou sobrescrita automatizada
Dados de marketing, prospecção e relacionamento comercial	Envio de comunicações mediante consentimento	3 anos ou até revogação do consentimento	Eliminação imediata após expiração do prazo ou solicitação do titular
Dados sensíveis tratados em procedimentos específicos	Cumprimento de obrigação legal, regulatória ou de saúde ocupacional	Pelo prazo legalmente exigido	Anonimização ou destruição definitiva após o cumprimento da finalidade

7. ARMAZENAMENTO E CONTROLE DE ACESSO

Todos os dados deverão ser armazenados exclusivamente em ambientes autorizados e monitorados, com autenticação multifator e registro de logs de acesso.

Os repositórios digitais devem ser criptografados, com cópias de segurança gerenciadas sob política de backup corporativo.

Documentos físicos devem permanecer em arquivos lacrados, com controle de empréstimo, rastreabilidade e restrição de acesso a pessoal autorizado.

A transferência ou compartilhamento de dados com terceiros somente ocorrerá mediante contrato formal contendo cláusulas de confidencialidade e obrigações equivalentes às previstas nesta política.

8. PROCEDIMENTO DE DESCARTE E ANONIMIZAÇÃO

Eliminação de dados digitais: realizada mediante sobrescrita múltipla, exclusão segura ou destruição de mídias, garantindo impossibilidade técnica de recuperação.

Descarte de documentos físicos: realizado por trituração, descaracterização ou incineração supervisionada.

Anonimização: sempre que possível, dados serão convertidos em informações não identificáveis, mantendo valor estatístico ou histórico, sem violar a privacidade dos titulares.

Registro de descarte: toda operação de exclusão deve ser documentada, indicando data, método utilizado, responsável técnico e autorização formal.

9. RESPONSABILIDADES

Controlador (Verocard): definir finalidades, prazos de retenção e meios de eliminação; supervisionar o cumprimento das obrigações legais.

Encarregado de Proteção de Dados (DPO): atuar como ponto de contato com titulares e autoridades, monitorar o cumprimento desta política e propor melhorias contínuas.

Gestores de área: zelar pelo cumprimento das diretrizes em seus respectivos departamentos, realizando revisões periódicas e reportando inconsistências.

Colaboradores e prestadores de serviço: observar integralmente esta política e as normas complementares de segurança da informação.

Terceiros contratados: adotar padrões de proteção e retenção compatíveis, sob pena de responsabilização solidária em caso de violação.

10. DIREITOS DOS TITULARES

A Verocheque Refeições Ltda (Verocard) assegura aos titulares de dados o exercício dos seguintes direitos: confirmação da existência de tratamento, acesso, correção, anonimização, portabilidade, eliminação e revogação do consentimento.

As solicitações deverão ser encaminhadas ao Encarregado de Proteção de Dados, que providenciará resposta em prazo razoável, observadas as limitações decorrentes de obrigações legais ou regulatórias de retenção.

11. MONITORAMENTO, AUDITORIA E REVISÃO

Esta política será revisada anualmente ou sempre que houver alteração significativa nas normas legais, nos sistemas de informação ou nos processos internos da Verocheque Refeições Ltda (Verocard).

A conformidade com os prazos e procedimentos de retenção será objeto de auditorias periódicas conduzidas pela área de Compliance e pelo DPO.

Os resultados das auditorias deverão ser registrados, acompanhados de plano de ação corretiva quando identificadas não conformidades.

12. DISPOSIÇÕES FINAIS

O descumprimento das normas previstas nesta política constitui infração disciplinar e poderá ensejar medidas administrativas, civis e contratuais cabíveis.

A presente política integra o conjunto normativo de governança e compliance da Verocheque Refeições Ltda (Verocard) e deve ser observada em conjunto com o Código de Conduta, a Política de Privacidade e a Política de Segurança da Informação.

Todos os colaboradores e parceiros deverão manifestar ciência e compromisso com as diretrizes aqui estabelecidas, mediante assinatura eletrônica ou física do termo de adesão interno.

Data de aprovação: 17 de janeiro de 2025

Responsável pela aprovação: toda política e revisão será instituída pelo comitê nomeado

Documento controlado – uso interno restrito à Verocheque Refeições Ltda (Verocard).

DECLARAÇÃO E PROCEDIMENTO DE DEVOLUÇÃO E DESCARTE DE DADOS PESSOAIS

Verocheque Refeições LTDA (Verocard)

1. OBJETIVO E ESCOPO

O presente documento tem como finalidade formalizar os procedimentos adotados pela Verocheque Refeições Ltda. (Verocard) para devolução, eliminação definitiva ou anonimização de dados pessoais e sensíveis tratados no curso de contratos, convênios, parcerias, operações comerciais e serviços tecnológicos prestados.

Esta política aplica-se a todas as áreas corporativas da Verocard, abrangendo as informações armazenadas em sistemas internos, servidores, nuvem, mídias externas, arquivos físicos e plataformas de terceiros sob responsabilidade da empresa.

A medida visa garantir conformidade integral com os princípios de necessidade, finalidade, transparência, segurança e responsabilização, conforme previstos na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), e reforçar o compromisso institucional da Verocard com a ética, a confidencialidade e a proteção das informações pessoais de clientes, usuários, colaboradores e parceiros.

2. DIRETRIZES GERAIS

Todos os dados pessoais tratados pela Verocheque Refeições Ltda. (Verocard) serão objeto de devolução ou descarte quando cessar a finalidade que motivou sua coleta, ou após o término da relação contratual, salvo hipóteses legais de conservação.

A devolução e a eliminação serão conduzidas de forma planejada, controlada e auditável, mediante registro documental e validação pelo Encarregado de Proteção de Dados (DPO).

O processo obedecerá aos princípios de segurança da informação, integridade e rastreabilidade, assegurando que nenhuma informação permaneça armazenada além do período autorizado.

Qualquer exceção deverá ser formalmente aprovada pela Diretoria de Compliance e pelo DPO, com justificativa legal expressa e prazo determinado para guarda extraordinária.

3. PROCEDIMENTO DE DEVOLUÇÃO DOS DADOS PESSOAIS

3.1. Solicitação e autorização

A devolução poderá ocorrer mediante solicitação formal do controlador dos dados (cliente ou parceiro contratante) ou por determinação legal/regulatória.

A solicitação deverá ser encaminhada ao canal oficial de privacidade da Verocard, contendo a identificação do solicitante, a base contratual e o escopo do retorno.

3.2. Extração e exportação controlada

A equipe técnica realiza a extração dos dados a partir de bases originais, garantindo a integridade e a completude das informações.

Os dados são convertidos para formato interoperável e seguro (CSV criptografado, JSON, XML ou outro formato acordado), compatível com os sistemas do controlador.

O arquivo é submetido à criptografia de 256 bits e enviado por canal autenticado com duplo fator de verificação.

Cada transferência é documentada em Relatório de Entrega de Dados, que contém:

1. Data e hora da exportação;
2. Nome do responsável técnico;
3. Hash de verificação de integridade;
4. Identificação do contrato ou projeto;
5. Confirmação de recebimento pelo destinatário autorizado.

3.3. Pós-entrega e eliminação subsequente

Após a confirmação do recebimento, a Verocheque Refeições Ltda. (Verocard) procede com a eliminação completa das cópias locais, incluindo:

Bases temporárias utilizadas no processo de exportação;

Registros intermediários de sistemas;

Backups relacionados ao período contratual, observadas eventuais obrigações legais de retenção fiscal ou contábil.

Um Termo de Conclusão de Devolução e Descarte é emitido e arquivado por prazo mínimo de cinco anos.

4. PROCEDIMENTO DE ELIMINAÇÃO E DESCARTE DEFINITIVO

4.1. Identificação dos conjuntos de dados

Encerrado o vínculo contratual ou a finalidade do tratamento, o gestor da área identifica os bancos de dados e documentos físicos que contêm informações pessoais, classificando-os conforme:

1. Natureza do dado (pessoal, sensível, corporativo);
2. Meio de armazenamento (digital, físico, nuvem, backup);

3. Prazo legal aplicável (trabalhista, fiscal, contratual, contábil).

Essas informações compõem o Inventário de Descarte, controlado pela área de Compliance.

4.2. Métodos de descarte

a) Dados digitais:

Eliminação por sobrescrita múltipla (método DOD 5220.22-M ou equivalente);

Criptografia total e destruição de chaves;

Destruição física de mídias, quando aplicável.

b) Documentos físicos:

Trituração mecânica em fragmentos inferiores a 6 mm;

Descaracterização completa com incineração supervisionada;

Certificação por empresa especializada, sob contrato de confidencialidade.

4.3. Registro e auditoria

Cada operação de descarte é documentada em Relatório de Eliminação de Dados, contendo:

- 1.** Código de referência do processo ou contrato;
- 2.** Quantidade e tipo de registros eliminados;
- 3.** Data e hora da execução;
- 4.** Método técnico utilizado;
- 5.** Nome e assinatura do responsável;
- 6.** Validação do DPO e do gestor da área.

Esses relatórios são armazenados digitalmente em ambiente segregado e auditável, garantindo evidência de conformidade para inspeções internas, externas ou regulatórias.

5. PROCEDIMENTO DE ANONIMIZAÇÃO

Em situações em que a manutenção parcial dos dados se mostre necessária para fins estatísticos, de auditoria, estudo de desempenho ou melhoria de sistemas, a Verocheque Refeições Ltda. (Verocard) adota processo de anonimização técnica controlada, que envolve:

Remoção ou substituição de identificadores diretos (nome, CPF, e-mail, etc.);

Perturbação de valores identificáveis (hashing, generalização ou mascaramento);

Armazenamento em ambiente segregado sem vínculo com bases ativas;

Auditoria de irreversibilidade para garantir que o dado não possa ser reidentificado.

Esses dados anonimizados não são mais considerados pessoais e passam a ser utilizados apenas em contexto legítimo e proporcional ao interesse empresarial.

6. SUPERVISÃO, GOVERNANÇA E CONTROLE

O processo de devolução e descarte é coordenado pela Diretoria de Compliance, sob supervisão direta do Encarregado de Proteção de Dados (DPO), e executado em conjunto com as áreas de Tecnologia da Informação, Jurídico e Segurança da Informação.

As atribuições específicas incluem:

DPO: validar solicitações, aprovar métodos de eliminação e emitir relatórios de conformidade.

TI: executar tecnicamente os procedimentos de exportação, destruição e anonimização.

Compliance: manter o inventário de dados eliminados, acompanhar prazos legais e garantir rastreabilidade.

Jurídico: avaliar hipóteses de retenção legal e emitir parecer em casos de guarda extraordinária.

Reuniões de verificação e auditorias internas são realizadas trimestralmente, com emissão de relatório de acompanhamento e plano de ação corretiva, quando aplicável.

7. SEGURANÇA E CONFIDENCIALIDADE

Durante todas as etapas de devolução ou descarte, aplicam-se controles de segurança equivalentes aos utilizados no tratamento ativo dos dados, incluindo:

1. Criptografia de ponta a ponta em todas as transmissões;
2. Controle de acesso baseado em privilégios mínimos;
3. Registro de logs de atividade e monitoramento contínuo;
4. Autenticação multifatorial e segregação de ambientes;
5. Política de senhas e tokens de acesso;
6. Monitoramento de integridade de arquivos e trilhas de auditoria.

A Verocheque Refeições Ltda. (Verocard) mantém contratos de confidencialidade com todos os colaboradores e fornecedores envolvidos, assegurando o sigilo absoluto das informações manipuladas durante o processo.

8. COMPROVAÇÃO E RASTREABILIDADE

Para cada operação de devolução, eliminação ou anonimização, é emitido um Termo de Conclusão, contendo:

1. Descrição detalhada do procedimento;
2. Identificação do conjunto de dados afetado;
3. Referência contratual e responsável técnico;
4. Data de execução e hash criptográfico de validação;
5. Assinatura do DPO e do Diretor de Compliance.

Esses termos são arquivados eletronicamente, com versionamento automático e controle de integridade, garantindo accountability e plena rastreabilidade perante auditorias ou autoridades competentes.

9. DECLARAÇÃO DE CONFORMIDADE

A Verocheque Refeições Ltda. (Verocard) reafirma seu compromisso com a governança de dados, assegurando que:

Todos os processos de devolução, eliminação e anonimização seguem protocolos seguros, rastreáveis e auditáveis;

Não são mantidos dados pessoais além dos prazos ou finalidades autorizadas;

Qualquer solicitação de titulares, controladores ou autoridades será atendida dentro dos prazos legais;

A empresa mantém estrutura técnica e procedimental compatível com as melhores práticas nacionais e internacionais de proteção de dados.

Data de aprovação: 17 de janeiro de 2025

Responsável pela aprovação: toda política e revisão será instituída pelo comitê nomeado

Documento controlado – uso interno restrito à Verocard Administradora de Benefícios Ltda.

PLANO DE CONTINUIDADE DE NEGÓCIOS E DISASTER RECOVERY (BCP/DRP)

Verocheque Refeições Ltda (Verocard)

1. OBJETIVO

O presente Plano tem por finalidade estabelecer a estrutura corporativa de Continuidade de Negócios (Business Continuity Plan – BCP) e Recuperação de Desastres (Disaster Recovery Plan – DRP) da Verocheque Refeições Ltda (Verocard), assegurando a resiliência operacional, a redundância de sistemas e a capacidade de recuperação completa dos ambientes tecnológicos e processos críticos em situações de interrupção, incidente cibernético, falha sistêmica ou desastre físico.

O documento visa garantir que a Verocheque Refeições Ltda (Verocard) mantenha suas operações essenciais de forma ininterrupta, protegendo os dados de clientes, usuários, parceiros e colaboradores, preservando a confiança institucional e a conformidade com as obrigações legais e regulatórias.

2. ABRANGÊNCIA

Este plano aplica-se a todas as operações, unidades, departamentos e sistemas sob gestão direta ou indireta da Verocheque Refeições Ltda (Verocard), abrangendo:

- Ambientes de produção, homologação e contingência;
- Infraestrutura de servidores, bancos de dados e redes corporativas;
- Plataformas de gestão de benefícios, transações financeiras e APIs integradas;
- Ambientes em nuvem e provedores de infraestrutura tecnológica (AWS Cloud);
- Processos administrativos, financeiros e de atendimento ao cliente;
- Parceiros e prestadores de serviço que suportem a cadeia operacional crítica.

3. REFERÊNCIAS E BASE NORMATIVA

A Verocheque Refeições Ltda (Verocard) estrutura seu Plano de Continuidade e Disaster Recovery conforme os seguintes referenciais e boas práticas internacionais:

1. **Lei nº 13.709/2018 – LGPD**, quanto à integridade e disponibilidade de dados pessoais;
2. **Resolução BACEN nº 4.658/2018**, sobre política de segurança cibernética e continuidade operacional;
3. **ISO 22301:2019** – Business Continuity Management Systems;
4. **ISO/IEC 27031:2022** – Guidelines for ICT Readiness for Business Continuity;
5. **ISO/IEC 27001:2022** – Information Security Management System (SGSI);
6. **PCI DSS – Payment Card Industry Data Security Standard**, aplicável ao ambiente de transações;
7. **AWS Well-Architected Framework** – Pilares de segurança, confiabilidade e desempenho;
8. **NIST SP 800-34 Rev.1** – Contingency Planning Guide for Federal Information Systems.

4. PRINCÍPIOS FUNDAMENTAIS

A Verocheque Refeições Ltda (Verocard) adota os seguintes princípios na gestão de continuidade e recuperação:

1. **Resiliência** – garantir capacidade de resistir e recuperar-se de incidentes sem perda significativa de desempenho.
2. **Redundância Total** – replicação de sistemas, dados e recursos críticos em múltiplas zonas e regiões geográficas.

3. **Alta Disponibilidade (HA)** – manter disponibilidade contínua dos serviços essenciais com *uptime* mínimo de 99,9%.
4. **Integridade e Consistência** – assegurar que os dados restaurados sejam completos e não corrompidos.
5. **RTO e RPO Controlados** – tempo máximo de recuperação (RTO) e ponto máximo de perda (RPO) definidos e testados.
6. **Automação e Escalabilidade** – recuperação automatizada com orquestração em nuvem e monitoramento 24/7.
7. **Transparência e Responsabilidade** – comunicação clara a todas as partes interessadas durante contingências.
8. **Melhoria Contínua** – revisão e teste periódico do plano, com base em simulações reais e auditorias.

5. INFRAESTRUTURA TECNOLÓGICA E REDUNDÂNCIA

5.1. Arquitetura em Nuvem – AWS Cloud

A infraestrutura da Verocheque Refeições Ltda (Verocard) é hospedada integralmente na Amazon Web Services (AWS), que fornece arquitetura distribuída e resiliente, baseada em múltiplas Zonas de Disponibilidade (Multi-AZ) e Regiões Geográficas (Multi-Region).

As principais medidas implementadas incluem:

- **Replicação síncrona** entre zonas de disponibilidade, garantindo resiliência a falhas locais;
- **Failover automático** em caso de indisponibilidade de uma zona ou instância;
- **Backup e snapshots automatizados** de bancos de dados (RDS, S3, EBS);
- **Armazenamento redundante** no Amazon S3 com durabilidade de 99,999999999%;

- Criptografia em repouso e em trânsito (AES-256 e TLS 1.2+);
- Serviços balanceados via AWS Elastic Load Balancer;
- **Monitoramento proativo e alertas via Amazon CloudWatch e Security Hub;**
- **Multi-factor authentication (MFA)** para administração de ambientes críticos;
- **Cross-region replication** de dados para ambientes de contingência remotos.

5.2. Ambientes e Segmentação Operacional

A Verocheque Refeições Ltda (Verocard) mantém três ambientes segregados:

- **Produção:** operação ativa dos sistemas corporativos e transacionais.
- **Homologação/Teste:** ambiente isolado para validação de novas versões.
- **Contingência (DR Site):** infraestrutura espelhada com atualização contínua, apta para assumir o tráfego em até **2 horas (RTO máximo)** em caso de falha.

5.3. Conectividade e Comunicação

- **VPN redundante** com múltiplos provedores de link;
- **Failover de DNS e IP elástico** para redirecionamento automático de requisições;
- **Serviços de mensageria e autenticação** (SES, Cognito, SNS) com replicação e contingência;
- **Monitoramento contínuo de performance e latência** via AWS CloudWatch e métricas internas.

6. GOVERNANÇA DE CONTINUIDADE

A governança do Plano de Continuidade é centralizada no Comitê de Segurança da Informação.

1. Esse comitê tem autoridade para:
2. Avaliar riscos e priorizar processos críticos;

3. Acionar o plano de contingência e disaster recovery;
4. Autorizar comunicações externas;
5. Coordenar ações conjuntas entre as áreas técnicas, operacionais e jurídicas;
6. Aprovar relatórios de recuperação e planos de melhoria.

6.1. Papéis e Responsabilidades

Função	Responsabilidades
Diretoria Executiva	Aprovar e financiar o plano; supervisionar a execução e relatórios pós-incidente.
Diretoria de TI	Implementar medidas técnicas, supervisionar backups e gerenciar a infraestrutura AWS.
Comitê de Segurança da Informação.	Deliberar sobre acionamento do plano e comunicação institucional.
Compliance e DPO	Avaliar impactos regulatórios e de proteção de dados; supervisionar conformidade LGPD.
Suporte Técnico / Operações	Executar os procedimentos de failover, restauração e validação de integridade.
Usuários-Chave (Key Users)	Validar a restauração funcional dos sistemas e apoiar o retorno às atividades.

6.2. Definições e Diretrizes Complementares

Todas as definições, conceitos, parâmetros, responsabilidades, planos de ação, métricas e atualizações atinentes ao Plano de Continuidade de Negócios (BCP) e às políticas correlatas de Recuperação de Desastres (DRP) serão objeto de análise, deliberação e aprovação formal pelo Comitê de Segurança da Informação da Verocheque Refeições Ltda (Verocard).

O Comitê de Segurança da Informação, é responsável por:

1. Definir critérios, indicadores e métricas de continuidade de negócios (RTO, RPO e níveis de severidade);
2. Estabelecer metodologias e padrões de classificação de criticidade de processos e sistemas;
3. Deliberar sobre revisões e ajustes nas definições estratégicas do BCP;
4. Garantir a integração das políticas de continuidade com a Política de Segurança da Informação, a Política de Retenção de Dados e o Programa de Governança em Privacidade;
5. Assegurar o alinhamento das decisões de continuidade com as boas práticas das normas ISO 22301, ISO 27031 e ISO 27701;
6. Emitir pareceres técnicos sempre que houver necessidade de atualização, ampliação ou redefinição de parâmetros de resiliência operacional.

Toda definição aprovada pelo Comitê de Segurança da Informação será registrada em ata, incorporada à versão vigente do Plano e comunicada às áreas envolvidas por meio de memorando interno controlado, garantindo rastreabilidade e governança sobre cada alteração de diretriz.

7. PROCEDIMENTO DE ACIONAMENTO DO PLANO

7.1. Detecção e Avaliação do Evento

1. O incidente é detectado por sistemas de monitoramento automatizado ou por comunicação interna.
2. Comitê de Segurança da Informação é notificado e avalia o impacto conforme classificação: **Baixo, Médio, Alto ou Crítico.**

7.2. Decisão de Ativação

Em caso de falha crítica, a Direção de TI autoriza a ativação imediata do **Plano de Disaster Recovery (DRP)**.

São acionados as réplicas e os mecanismos de failover da AWS; os sistemas passam a operar no ambiente secundário.

7.3. Recuperação e Restauração

Restauração das instâncias e volumes a partir dos últimos snapshots válidos;

Sincronização dos dados transacionais e revalidação dos sistemas integrados;

Verificação de integridade e checagem dos logs de auditoria.

Parâmetros operacionais definidos:

- **RTO (Recovery Time Objective):** até 2 horas;
- **RPO (Recovery Point Objective):** até 15 minutos;
- **Disponibilidade mínima garantida:** 99,9%.

7.4. Comunicação e Escalonamento

- A comunicação de contingência segue o **Protocolo de Comunicação de Crise**, coordenado pela Diretoria Executiva.
- Clientes e parceiros são informados formalmente sobre o status e o tempo estimado de recuperação, caso o impacto ultrapasse 30 minutos.
- Caso envolva dados pessoais, o DPO acompanha o processo para garantir observância ao art. 48 da LGPD.

7.5. Encerramento e Revisão Pós-Evento

Após normalização, é elaborado o **Relatório Final de Continuidade (RFC)**, contendo:

1. Descrição do evento;
2. Tempo de resposta e de restauração;
3. Dados de RTO e RPO alcançados;
4. Impactos técnicos e financeiros;
5. Ações corretivas e preventivas.

O relatório é apresentado à Diretoria Executiva e arquivado por prazo mínimo de 5 (cinco) anos.

8. TESTES, SIMULAÇÕES E AUDITORIAS

A Verocheque Refeições Ltda (Verocard) realiza testes formais semestrais de continuidade e disaster recovery, com simulações completas de falhas críticas, perda total de ambiente, indisponibilidade de rede e corrupção de banco de dados.

Esses testes têm como objetivos:

1. Validar tempos de resposta e integridade dos dados restaurados;
2. Verificar conformidade dos ambientes de contingência;
3. Testar a comunicação interna entre times técnicos e executivos;
4. Avaliar o nível de aderência às normas ISO 22301 e 27031.

Os resultados são consolidados em relatórios de desempenho (RTO/RPO reais) e revisados pelo Comitê de Segurança da Informação.

9. GESTÃO DE CRISES E COMUNICAÇÃO EXTERNA

O **Protocolo de Gestão de Crises** define os fluxos de comunicação interna e externa durante eventos de grande impacto.

- A comunicação pública é centralizada pela **Diretoria Executiva e pelo Jurídico**, assegurando consistência e sigilo.
- Em casos de impacto a parceiros, os mesmos são notificados com relatório técnico e plano de mitigação.
- As decisões de divulgação são registradas em ata e arquivadas pelo Compliance.

10. REVISÃO, MELHORIA CONTÍNUA E CONFORMIDADE

Este Plano é revisado **anualmente**, ou sempre que houver:

- Mudança na infraestrutura tecnológica;
- Inclusão de novos sistemas críticos;
- Alteração significativa na arquitetura AWS;
- Ocorrência real de incidente de alta severidade.

As melhorias são documentadas em **Planos de Ação de Continuidade (PACs)**, auditadas internamente e aprovadas pela Diretoria Executiva.

11. DECLARAÇÃO DE CONFORMIDADE E CAPACIDADE OPERACIONAL

A Verocheque Refeições Ltda (Verocard) declara que:

1. Possui Plano de Continuidade de Negócios (BCP) e Plano de Disaster Recovery (DRP) formalmente aprovados, documentados e testados;
2. Toda sua infraestrutura tecnológica é hospedada em ambiente AWS Cloud, com redundância multi-regional, replicação contínua e failover automático;

3. Mantém RTO máximo de 2 horas e RPO máximo de 15 minutos, com monitoramento 24/7;
4. Garante alta disponibilidade (99,9%) dos serviços essenciais, mesmo em caso de falhas locais ou regionais;
5. Adota processos contínuos de backup, auditoria, testes e verificação de integridade;
6. Realiza testes semestrais de restauração e simulações de contingência, com relatórios documentados;
7. Possui equipe técnica, Comitê de Segurança da Informação e processos formalizados para resposta coordenada a desastres e retomada integral de operações;
8. Atua em plena conformidade com as normas de governança, privacidade, cibersegurança e continuidade operacional vigentes.

Data de aprovação: 17 de janeiro de 2025

Responsável pela aprovação: toda política e revisão será instituída pelo Comitê de Segurança da Informação.

Documento controlado – uso interno restrito à Verocheque Refeições Ltda (Verocard).