POLÍTICA DE DESCARTE E ANONIMIZAÇÃO DE DADOS

Código: POL-TI-006
Revisão: 01
Data: 05/01/2023

1. OBJETIVO

Orientar e estabelecer as diretrizes corporativas da DMS LOGISTICS para o descarte e anonimização adequados de dados.

2. CAMPO DE APLICAÇÃO

Todos os colaboradores, prestadores de serviços e usuários internos e externos das informações pertencentes/custodiadas pela DMS LOGISTICS.

3. DOCUMENTOS DE REFERÊNCIA

Esta política se aplica a todos os documentos que são ativos de informação ou não e que estão sob posse da DMS LOGISTICS. Para fins de referência foram utilizados a Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/18 e a ABNT NBR ISO/IEC 27001:2022.

4. PROCEDIMENTOS DE REGRAS

4.1. Definições

4.1.1. Aplicabilidade

Neste documento, quando houver menções de atribuições e/ou responsabilidades à DMS LOGISTICS, a abrangência a ser considerada será a DMS LOGISTICS e todas as suas Subsidiárias.

4.1.2. Anonimização

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

4.1.3. Dado anonimizado

Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

4.1.4. Descarte de dados

Processo de eliminar ou deletar um registro de dados sem a possibilidade de reversão ou reconstrução da informação.

4.1.5. Mapeamento de Dados Pessoais (ROPA)

Documento com a identificação do fluxo dos dados pessoais utilizados nos processos da organização. Ele contém o detalhamento sobre o tratamento desses dados, dentre os quais como e de onde eles são coletados, e de que forma eles são utilizados, armazenados, compartilhados e descartados.

4.1.6. Lei Geral de Proteção de Dados (LGPD)

Lei brasileira de regulamentação para uso, proteção e transferência de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado.

4.1.6.1. Titular de Dados

Pessoa natural a quem se referem os dados pessoais.

4.1.6.2. Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

4.1.6.3. Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

4.1.6.4. Tratamento de Dados

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4.1.6.5. Autoridade Nacional de Proteção de Dados (ANPD)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

4.1.6.6. Finalidade

A partir da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados.

4.1.7. Equipamentos de TI

Computadores, smartphones, notebooks, tablets ou qualquer outro equipamento móvel que possua acesso à rede e a informações da organização.

4.1.8. Data Protection Officer (DPO)

É o encarregado, figura principal da Governança de Dados Pessoais. É uma pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Dentre suas atribuições, estão:

• Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

• Receber comunicações da ANPD e adotar providências;

• Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção dos dados pessoais;

• Executar demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

4.2. Siglas

ROPA – Record of Processing Activities

LGPD – Lei Geral de Proteção de Dados

ANPD – Autoridade Nacional de Proteção de Dados

4.3. Descarte e Destruição de Dados

O descarte é a última fase do ciclo de vida dos dados em uma organização. É uma prática que ajuda a reduzir custos de armazenamento de dados e contribuem para um gerenciamento mais eficiente da Segurança da Informação. Além disso, com a chegada da LGPD, o descarte de dados deixa de ser apenas uma boa prática e passa a ser, também, uma prática obrigatória em determinados contextos, como está exposto adiante neste documento.

Em síntese, o descarte de dados tem como principais objetivos:

• Ser parte fundamental da gestão da capacidade de armazenamento de dados; • Reduzir custos relacionados ao armazenamento de dados;

• Reforçar a garantia de boas práticas de Segurança da Informação e governança de dados;

• Seguir as diretrizes da LGPD para as condições de tratamento de dados pessoais, atendendo aos direitos do titular garantidos pela Lei.

4.3.1. Critérios para Descarte

Em geral há duas razões para se manterem dados armazenados em uma organização: ou eles têm valor regulatório legal, ou geram resultados efetivos ao negócio. Por meio de um processo de análise do fluxo de informações é possível identificar em qual dessas divisões elas se encontram. Se não estiverem adequadas a nenhuma dessas categorias, as informações podem ser descartadas.

Para verificar os dados que geram resultados ao negócio, é preciso ter um alinhamento da área de TI, que é a área responsável pelos sistemas de informação eletrônicos, com as áreas de negócio. Para isso, é importante que o processo de manutenção do ROPA, descrito na Política de Governança da LGPD, seja seguido, garantindo que o ROPA esteja sempre atualizado. Assim, os dados que não têm mais utilização e não serão mais utilizados no futuro, poderão ser identificados para um possível descarte.

Para a avaliação do valor regulatório legal das informações, é importante destacar que as normas seguidas pela organização não são estáticas, e sim estão em constante transformação. Portanto, a área de TI deve ter um processo contínuo de comunicação com a área jurídica para que se estabeleçam e se atualizem os critérios de definição dos dados que precisam ser armazenados e dos dados que podem ser descartados.

Seguindo essas diretrizes, a DMS LOGISTICS adota requisitos para descarte de dados, seguindo os processos de tratamento de dados identificados no ROPA. Busca-se garantir que apenas os dados necessários sejam tratados e armazenados pela DMS LOGISTICS,

Todos os dados pessoais tratados pela DMS LOGISTICS serão retidos pelo tempo necessário ao cumprimento do objetivo para que foram coletados, com finalidades lícitas, específicas e informadas.

Alguns dados deverão ser guardados para cumprimento de obrigação legal, como os de natureza tributária, trabalhista e previdenciária. Nesses casos, os dados serão armazenados até o fim do prazo estipulado pela legislação.

Outros, relacionados a contratos e operações de cunho comercial e logístico, serão armazenados pelo tempo necessário, seguindo um prazo coerente com as práticas de mercado e com a natureza do tratamento.

Os dados pessoais que atingirem sua finalidade e prazo de armazenamento serão eliminados através dos seguintes métodos:

Método	Descrição	Aplicável a
Destruição física	Destruição física da mídia de armazenamento com o uso de picotadores especializados, pulverizadores ou incineradores. Este método destrói completamente a mídia de todos os dados.	Discos rígidos, discos removíveis. CD, CDR, DVD, DVDR. Este método também é válido para material em suporte físico como impressos e similares;
Criptografia de caminho único (one way)	Uso de um hash do tipo one-way para criptografar a informação de forma irrecuperável, mesmo que de posse da chave de criptografia. Este método não afeta a mídia e pode ser usado para o	Discos rígidos, discos removíveis, CDR, DVDR e similares;

	descarte seletivo de informações.	

Esta política determina as diretrizes para eliminação, descarte ou anonimização dos dados pessoais.

4.3.2. A LGPD E Descarte de Dados

Elaborar relatório de impacto à proteção a dados pessoais mediante solicitação da ANPD, que deverá conter, no mínimo:

• Descrição dos tipos de dados coletados;

• Metodologia utilizada para a coleta e para a garantia da segurança das informações; • Análise do controlador com relação a medidas, salvaguardas e mecanismos de risco adotados.

A ANPD irá solicitar, quando julgar necessário, um relatório de impacto à proteção de dados pessoais ao controlador de dados. Portanto, a DMS LOGISTICS deve estar preparada para elaborar o relatório sempre que necessário. Para isso, é importante que a organização esteja a par das informações que a ANPD poderá solicitar e que essas informações estejam facilmente disponíveis.

Para auxiliar na elaboração do relatório de impacto à proteção de dados, a DMS LOGISTICS irá utilizar o seu modelo deste relatório, com base nas principais diretrizes da LGPD.

4.3.3. Boas Práticas para o Descarte Seguro

Os procedimentos de descarte de informações considerados seguros não precisam ser os mesmos para as diferentes classificações de informação – para informações sobre a classificação das informações, consultar a Política de Classificação das Informações. Assim, os descartes seguros para cada tipo de informação devem ser procedidos conforme descritos a seguir.

• Sigilosa (NC1) ou restrita (NC2): a informação deve ser destruída de modo que não seja possível sua recuperação, independente do meio disponível. Quando a

informação está localizada nos parceiros, este deve ser orientado quanto à forma correta de descarte.

• Informação Interna (NC3): a informação deve ser destruída de modo que não seja possível sua recuperação, independente do meio disponível;

• Informação Pública (NC4): não há restrição quanto à forma para o descarte.

É importante ressaltar que deve existir um processo para que o descarte de dados possa ser documentado de forma adequada, sendo os registros feitos em sistemas confiáveis e seguros.

4.3.4. Sistemas de TI

Na DMS LOGISTICS, os dados armazenados nos seus sistemas de TI podem estar hospedados em servidores locais próprios ou em servidores em nuvem de empresas parceiras.

Para os casos de armazenamento de dados em nuvem, é especialmente importante que as responsabilidades sobre os dados sejam compartilhadas e bem definidas entre a DMS LOGISTICS e a empresa prestadora do serviço. A DMS LOGISTICS deve exigir que boas práticas de segurança da informação e de descarte de dados sejam seguidas pela empresa parceira, ponto que deve estar reforçado em contrato.

A LGPD, no Artigo 39, determina que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador. Além disso, o Artigo 42 da Lei diz que o operador responde solidariamente pelos danos causados pelo tratamento quando não tiver seguido as instruções lícitas do controlador. Portanto, o compartilhamento de responsabilidades e as exigências lícitas em relação à segurança da informação da DMS LOGISTICS para com os parceiros é fundamental para o descarte seguro de dados no contexto da LGPD, implicando em abrandamento de sanções em caso de infrações à Lei.

Para os dados armazenados em servidores locais próprios, o descarte seguro de dados é reforçado pelo cumprimento das Boas Práticas de Segurança Física, que mantêm os servidores livres de acessos não autorizados.

4.3.5. Equipamentos de TI e Mídias Móveis de Armazenamento

O descarte dos dados dos equipamentos de TI e das mídias de armazenamento deverão acontecer frente às seguintes hipóteses:

• Troca da atribuição de um equipamento ou mídia entre colaboradores da DMS LOGISTICS ou terceiros;

• Devolução do ativo uma vez em posse de um colaborador ou terceiro para a DMS LOGISTICS.

• Devolução do ativo para o fornecedor em caso de equipamento alugado; • Dispositivos de mídia móveis de armazenamento não mais necessários ou danificados. Estes devem ser descartados com segurança, sendo necessariamente devolvidos à TI para descarte seguro, que realizará o processo de descarte em ambientes apropriados.

Em qualquer hipótese, a responsabilidade pelo processo de descarte seguro das informações será da área de TI, ficando o usuário do ativo responsável por comunicar à área de TI qualquer necessidade de descarte seguro de dados não previstos.

Em casos críticos, devem ser utilizadas técnicas mais extremas para destruição da informação, entre as quais a desmagnetização, a sobrescrita ou até mesmo a destruição física. Para isso, devem ser usados equipamentos e serviços que fazem a eliminação segura dos dispositivos para que nenhum dado seja recuperado.

4.3.6. Documentos Físicos

Uma vez verificada a necessidade ou quando o descarte de documentos físicos for conveniente para a DMS LOGISTICS, observadas as condições presentes nesta Política, esses documentos devem ser destruídos, sem a possibilidade de reconstrução, antes de serem descartados.

Muitas vezes, um mesmo registro pode existir tanto no formato eletrônico quanto no formato físico. Nesses casos, a DMS LOGISTICS deve definir qual é o formato oficial para que a versão não oficial possa ser descartada com segurança.

4.3.7. Anonimização de Dados

O Artigo 12 da LGPD estabelece que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Portanto, quando a LGPD trouxer a obrigatoriedade de exclusão de dados pessoais, conforme as hipóteses dispostas neste documento no item “A LGPD E O DESCARTE DE DADOS”, e quando os dados em questão ainda forem úteis para a DMS LOGISTICS, uma alternativa à exclusão poderá ser a anonimização desses dados.

Além disso, a anonimização de dados também pode ser utilizada como reforço para a Segurança da Informação na organização de forma geral. Em síntese, a anonimização de dados é conveniente nos seguintes contextos:

• Para evitar danos e sanções em caso de vazamento de dados pessoais, caso essas informações sejam úteis para a DMS LOGISTICS mesmo nas suas formas anonimizadas;

• Quando, mediante obrigatoriedade de exclusão pela LGPD, a DMS LOGISTICS julgar que as informações ainda são úteis de alguma forma para a geração de valor na organização;

• Para armazenamento, transferência e compartilhamento seguros de dados pessoais.

4.3.8. Boas Práticas de Anonimização de Dados

Um ponto de atenção é que a garantia de uma anonimização efetiva de dados, em um cenário de forte evolução tecnológica, pode não ser simples. Para que a Lei seja cumprida em sua plenitude, portanto, a DMS LOGISTICS deve avaliar o grau de segurança que é aplicado nos seus processos de anonimização.

Diante desse cenário, é bastante provável que, conforme autoriza o 3º parágrafo do Artigo 12 da LGPD, venha a ser editado regulamento dispondo sobre os padrões e técnicas a serem empregados em processos de anonimização. Assim, a anonimização de dados deverá ser realizada sob as seguintes condutas:

• Seguindo os padrões e técnicas que podem vir a ser estabelecidos pela a LGPD, garantindo, assim, alinhamento e respaldo frente à Lei;

• Aplicando técnicas que a DMS LOGISTICS avaliou como sendo seguras, utilizando, de preferência, técnicas de última geração e que sejam constantemente atualizadas. A responsabilidade, no que tange a execução, registro, controle e efetividade e avaliação dos processos de anonimização de dados eletrônicos deve ser da área de TI da DMS LOGISTICS. Ainda assim, a anonimização poderá ser terceirizada, sendo feita por empresa independente,

desde que certificado que a anonimização se utilizará das boas práticas e seguirá as eventuais diretrizes da LGPD em relação às técnicas e padrões aceitáveis.

HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	09/02/2023	Emissão do documento.
01	24/02/2023	Revisão geral para incluir novos compromissos com o meio ambiente, saúde e segurança dos colaboradores e segurança da informação e codificação no documento.

APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	CyberSecurity Team	
Revisado por:	Leonardo Sabbadim	
Aprovador por:	Victor Gonzaga	
Nível de Confidencialidade:	**X**	**Informação Pública**
		Informação Interna
		Informação Confidencial
		Informação Sigilosa

NUNCA COLOCAMOS EM RISCO A QUALIDADE E NEM A ÉTICA NOS NEGÓCIOS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM