POLÍTICA DE GESTÃO DE VULNERABILIDADES

Código: POL-TI-007
Revisão: 01
Data: 28/02/2023

1. INTRODUÇÃO

O avanço tecnológico trouxe grandes benefícios para as instituições e a informação é um dos ativos mais críticos. Por outro lado, incidentes de segurança da informação tornaram-se um dos grandes problemas para a área de Segurança da Informação e Comunicações.

Por isso, há uma necessidade em garantir soluções para precaver-se dos impactos causados por incidentes e uma das ações preventivas está ligada à gestão de vulnerabilidades dos ativos que suportam os sistemas e a infraestrutura de rede. gestão de vulnerabilidades leva em consideração a probabilidade de um incidente de segurança da informação ocorrer quando uma vulnerabilidade for explorada.

A Gestão de Vulnerabilidades Técnicas visa levar a DMS LOGISTICS ao nível de maturidade dos processos de segurança, minimizando os impactos no negócio.

O armazenamento e tratamento de dados pessoais são uma vulnerabilidade em potencial. Por isso, a normativa do Anexo A traz como os riscos devem ser gerenciados, avaliados e tratados.

No Anexo B são trazidos os prazos de retenção e descarte adotados pela DMS LOGISTICS.

2. PÚBLICO-ALVO

Esta Política tem como público-alvo todos os colaboradores da DMS LOGISTICS.

3. OBJETIVO

O objetivo deste documento é estabelecer práticas de gestão de vulnerabilidades e avaliação de impacto capazes de prevenir proativamente a exploração de eventuais vulnerabilidades e potencial perda de dados da DMS LOGISTICS.

A DMS LOGISTICS cria e documenta práticas sistemáticas, de forma transparente, para manter os programas de controle, avaliar a vulnerabilidade de novos softwares ou hardwares e mitigar outras vulnerabilidades técnicas e não-técnicas.

O objetivo desta iniciativa é implementar uma maior proteção aos recursos de SIC, garantir as melhores práticas de compliance e reduzir o impacto de ameaças à DMS LOGISTICS e às informações sob sua tutela.

4. CONCEITO

O processo de gestão de vulnerabilidades técnicas é o conjunto de atividades coordenadas que tem por objetivo a redução, a níveis aceitáveis, das vulnerabilidades de segurança encontradas durante o processo de "Análise de Segurança" ou "Análise de Vulnerabilidades" em um determinado ativo, conjunto de ativos ou ambiente.

Ele estabelece regras para o mapeamento, acompanhamento, verificação e revisão dos sistemas.
O processo de gestão de vulnerabilidades técnicas é apresentado na norma ABNT NBR ISO/IEC 27002.

5. BENEFÍCIOS PELA IMPLEMENTAÇÃO

É possível elencar diversos benefícios da implementação do processo da gestão de vulnerabilidades, como:

- Conhecimento do ambiente;
- Apoio no processo de Inventário de software e hardware (responsabilidade por ativos);
- Transparência;
- Informações claras sobre cada ativo e o que é necessário implementar;
- Auxílio para tomada de decisão;
- Priorização de ações.

6. REFERÊNCIAS NORMATIVAS

- ABNT NBR ISO/IEC 27001:2022 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;
- ABNT NBR ISO/IEC 27002:2022 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação;
- ABNT NBR ISO/IEC 27005:2019 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;
- ABNT NBR 16167:2020 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação;
- Resolução do BACEN 4658/18
- ABNT NBR ISO/IEC 31000: 2018 - Gerenciamento de Riscos
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.0709/2018

7. O PROCESSO DE GESTÃO DE VULNERABILIDADES

O processo de gestão de vulnerabilidades técnicas é realizado com o monitoramento do ambiente e é segmentado em várias etapas, conforme demonstrado abaixo:

- Notificação dos responsáveis;
- Definição do escopo a ser analisado;
- Notificação dos responsáveis e agendamento das análises;
- Execução das análises;
- Consolidação dos dados (classificação e validação dos resultados das análises);
- Processo de mitigação;
- Validação do ambiente (novo ciclo e/ou reteste);
- Liberação do ambiente;
- Elaboração de relatórios;
- Relatório final;
- Finalização.

8. USO DE ENDPOINT PROTECTION

Todos os equipamentos da DMS LOGISTICS que tenham acesso ao sistema precisam utilizar o endpoint protection aprovado e utilizado pela companhia.

A solução atualmente em uso é o CrowdStrike Falcon Endpoint Protection Pro.

É proibida a alteração ou desabilitação do software de endpoint protection. Apenas a área de TI, após análise da equipe de Segurança da Informação, poderá tomar qualquer providência neste sentido.

Todos os arquivos recebidos através de redes ou dispositivos de armazenamento externos devem ser escaneados contra malware antes de serem utilizados.

O serviço de e-mail corporativo possui regras anti-spam e anti-malware predeterminadas no servidor do serviço, e além disso, todos os anexos que forem salvos no computador local são verificados pela solução de Endpoint Protection instalada.

E-mails e conteúdos suspeitos passarão por quarentena para prevenir a disseminação ao sistema de e-mail ou redes da DMS LOGISTICS. E-mails suspeitos deverão ser reportados à área de SI da DMS LOGISTICS, para que se tomem as medidas de proteção cabíveis.

Caso o usuário suspeite de atividades suspeitas ou e-mails não confiáveis, deverá seguir os procedimentos descritos na Política de Tratamento de Não Conformidade e Gestão de Incidentes (POP-SGI-002).

Todos os colaboradores precisam seguir as regras para uso seguro do e-mail. Em caso de suspeita de phishing ou qualquer outra atividade suspeita deve ser reportada imediatamente à Equipe de Segurança da Informação. O colaborador que identificou a atividade suspeita deve preencher os formulários constantes nos Anexos A e B existentes na Política de Gerenciamento de Incidentes e seguir os trâmites lá descritos (vide Política de Gerenciamento de Incidentes).

Todos os arquivos recebidos de fonte externa ao Sistema DMS LOGISTICS devem ser escaneados para verificar a existência de vírus e malware antes de sua abertura e uso.

Qualquer dispositivo não pertencente e não autorizado pela DMS LOGISTICS, quando conectados à rede da organização, podem comprometer e trazer danos à segurança da rede. A fim de mitigar este risco, deve-se obter uma autorização específica com o departamento de SI antes de qualquer conexão à rede deste tipo.

Toda detecção de vírus e malware que não seja automaticamente identificado e colocado em quarentena pelo endpoint protection constitui um incidente de segurança e precisa ser reportado à Equipe de Segurança da Informação através do Formulário de Reporte de Incidentes de Segurança

A Equipe de Segurança da Informação deverá manter e atualizar um banco de dados com as vulnerabilidades encontradas e reportadas, assim como as iniciativas tomadas para remediá-las, como uma ferramenta de controle e transparência.

9. MONITORAMENTO E ALERTA

A DMS LOGISTICS adota soluções e ferramentas para proteger a Confidencialidade, Autenticidade e Integridade dos dados e ativos do Sistema DMS LOGISTICS, a fim de protegê-lo contra transferência não autorizada, modificação ou quebra de confidencialidade, de acordo com as diretrizes da Lei Geral de Proteção de Dados e boas práticas de mercado.

Para isso, o sistema DMS LOGISTICS utiliza os sistemas abaixo elencados:

- AWS GuardDuty
- AWS CloudWatch
- AWS CloudTrail
- AWS Trusted Advisor
- NewRelic

Essas ferramentas, descritas na Política de Gerenciamento de Redes, são o equivalente a um SIEM.

Com esse mesmo intuito, os usuários devem somente receber acesso à rede e aos serviços de rede que tenham sido autorizados a utilizar. Todas as permissões e métodos de acesso devem ser solicitados por chamado registrado no Jira, e dirigidos ao Gestor de Segurança da Informação da DMS LOGISTICS. Para maiores detalhes, ver a Política de Gerenciamento de Redes.

Todos os sistemas são acessados mediante autenticação e cada usuário deve estar devidamente identificado por uma identidade única e intransferível, possibilitando que seja vinculado e responsabilizado por seus atos dentro da organização.

10. GERENCIAMENTO DE PATCHES

A Equipe de Segurança da Informação da DMS LOGISTICS possui total responsabilidade para a implementação, operacionalização e procedimentos do gerenciamento de patches.

Todos os recursos de informação são monitorados regularmente para identificar atualizações disponíveis. O atraso na atualização de sistemas operacionais ou plataformas representa uma vulnerabilidade aos recursos de informação da companhia, de forma que a varredura e a implementação das atualizações existentes devem ser realizadas dentro de um período aceitável que represente o menor risco à integridade da companhia.

Atualização de softwares e mudanças na configuração de sistemas devem ser testados antes de serem aplicados e adotados de forma ampla nos dispositivos da DMS LOGISTICS, e devem ser conduzidas de acordo com as diretrizes de controle de mudanças.

Neste mesmo sentido, a equipe de Segurança da Informação realiza e mantém um inventário dos recursos de tecnologia da informação para registrar as marcas, modelos e versões de seus hardwares, assim como dos sistemas operacionais, bases de dados, servidores e demais softwares usados pela empresa. Este inventário é atualizado anualmente ou sempre que houver mudanças. Ele é encontrado no Anexo B da Política de Uso Aceitável de Ativos.

11. TESTES DE PENETRAÇÃO (PENTEST)

Testes de penetração das redes internas e externas serão conduzidos no mínimo anualmente ou após eventos significativos e mudanças no ambiente de segurança, além de poderem ser realizados a qualquer momento, caso seja identificada uma

necessidade.

A Empresa poderá contratar uma empresa terceirizada para tanto. Após a condução do referido processo, o Comitê Gestor de Segurança da Informação deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Empresa, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade de o evento acontecer.

Todas as vulnerabilidades identificadas durante os testes de penetração serão corrigidas, seguido da realização de novos testes para verificar se as vulnerabilidades foram corrigidas com sucesso.

12. CONSCIENTIZAÇÃO E TREINAMENTO SOBRE VULNERABILIDADE

Serão realizadas campanhas de conscientização de todos os colaboradores da DMS LOGISTICS, assim como treinamentos relativos às melhores práticas para uso de softwares e hardwares de propriedade da empresa ou externos, visando a proteção contra vulnerabilidades. Essa medida visa contribuir para a criação, desenvolvimento e manutenção de uma cultura de segurança da informação e comunicações dentro da companhia, como expresso na Política de Segurança.

13. ESCOLHA DA EQUIPE

A escolha da equipe responsável pela execução do processo no que tange às atividades de análise e varredura pode variar, de acordo com a necessidade.

14. ENCERRAMENTO DA POLÍTICA DE GESTÃO DE VULNERABILIDADE

Após o restabelecimento total dos sistemas e recursos tecnológicos essenciais, todos deverão ser comunicados, inclusive orientados quais os cuidados deverão ter para evitar reincidência.

Todas as informações referentes ao evento de vulnerabilidade devem ser coletadas e analisadas a fim de tornar o Plano de Continuidade de Negócio mais robusto com o conhecimento adquirido conforme a ABNT NBR ISO/IEC 27001, controle 5.27 Aprendendo com os incidentes de segurança da informação.

15. PENALIDADES

O não cumprimento das regras presentes nesta Política de Gestão de Vulnerabilidade sujeita o infrator às penalidades previstas em lei e nos regulamentos internos da DMS LOGISTICS.

16. IMPLEMENTAÇÃO E ATUALIZAÇÃO

Recomenda-se que o processo e suas atividades sejam revisados a cada seis meses, ou conforme descrito no sistema normativo da empresa, não se restringindo apenas a estes. Caso uma parte interessada identifique uma melhoria, ela deve ser implementada assim que possível.

17. ANEXO A - GERENCIAMENTO DE RISCOS

Descobrir vulnerabilidades em tempo hábil é importante, mas ser capaz de estimar o risco associado ao negócio é tão importante quanto.

No início do ciclo de vida, pode-se identificar problemas de segurança na arquitetura usando a modelagem de ameaças. Posteriormente, podemos encontrar problemas de segurança utilizando a revisão de código ou o teste de penetração.

Com essa abordagem é possível estimar a gravidade de todos esses riscos para o negócio e tomar uma decisão baseada nestes riscos. Ter uma gestão de riscos vai economizar tempo e eliminar a discussão sobre as prioridades. Este sistema auxiliará que a DMS LOGISTICS tome as medidas apropriadas levando em conta a gravidade do risco, seja riscos menores ou riscos mais graves, todos serão atendidos.

17.1. ABORDAGEM

Existem várias abordagens diferentes para a análise de risco. A abordagem OWASP aqui apresentada baseia-se em metodologias padrão e é personalizada para segurança de aplicativos. Um modelo de risco normal é apresentado abaixo:

Risco = Probabilidade * Impacto

Nas seções abaixo os fatores que compõem "probabilidade" e "impacto" para a segurança do aplicativo são discriminados.

17.1.1. IDENTIFICAR UM RISCO

O primeiro passo é identificar os riscos de segurança que devem ser avaliados. O analista precisa reunir informações sobre o agente de ameaça envolvido, o ataque que será usado, a vulnerabilidade envolvida, bem como o impacto de uma exploração bem-sucedida nos negócios. Pode haver vários grupos de possíveis atacantes, ou até mesmo múltiplos impactos de negócios possíveis. Em geral, a melhor abordagem é utilizar a opção de pior caso, que vai resultar em maior risco global.

17.1.2. FATORES PARA ESTIMAR PROBABILIDADE

Uma vez que o analista tenha identificado um risco potencial, classificado este risco em termos de gravidade, o primeiro passo é estimar a "probabilidade". No nível mais alto, esta é uma medida aproximada de quão provável esta vulnerabilidade particular é para ser descoberta e explorada por um invasor. Não é necessário ser mais preciso nesta estimativa. Em geral, a identificação da probabilidade entre baixa, média ou alta é suficiente.

Há uma série de fatores que podem ajudar a determinar a probabilidade. O primeiro conjunto de fatores está relacionado com o agente de ameaça envolvido. O objetivo é o de estimar a probabilidade de um ataque com êxito a partir de um grupo de possíveis atacantes. Nota-se que pode haver vários agentes de ameaças que podem explorar uma vulnerabilidade particular, por isso é geralmente melhor usar um cenário de pior caso. Por exemplo, uma fonte pode ser um invasor muito mais provável do que um intruso anônimo, mas depende de um número de fatores.

Nota-se que cada elemento possui um conjunto de opções, e cada opção tem uma probabilidade baixa, de 0 a 9 associada a ele. Estes números serão usados mais tarde para estimar a probabilidade global.

Fatores de Ameaça

- **Nível de habilidade**

Quão tecnicamente qualificado é este grupo de agentes de ameaça?

Habilidades de penetração de Segurança (9), habilidades de rede e de programação (6), usuário de computador avançado (5), algumas habilidades técnicas (3), sem habilidades técnicas (1)

- **Motivo**

Quão motivado é este grupo de agentes de ameaça de encontrar e explorar essa vulnerabilidade?

Pouca ou nenhuma recompensa (1), possível recompensa (4), alta recompensa (9)

- **Oportunidade**

Que recursos e oportunidades são necessários para este grupo de agentes de ameaça encontrar e explorar essa vulnerabilidade?

Acesso total ou recursos caros exigidos (0), acesso especial ou recursos são necessários (4), alguns acessos ou recursos são necessários (7), não tem acesso ou recursos necessários (9)

- **Tamanho**

Quão grande é este grupo de agentes de ameaça?

Programadores (2), administradores de sistema (2), usuários da intranet (4), parceiros (5), os usuários autenticados (6), os utilizadores da Internet anônimos (9)

- **Fatores de vulnerabilidade**

O próximo conjunto de fatores está relacionado com as vulnerabilidades envolvidas. O objetivo aqui é estimar a probabilidade de a vulnerabilidade particular envolvida ser descoberta e explorada.

- **Facilidade de descoberta**

Quão fácil é para este grupo de agentes de ameaça descobrir essa vulnerabilidade?
Praticamente impossível (1), difícil (3), fácil (7), ferramentas automatizadas disponíveis (9)

- **Facilidade de explorar**

Quão fácil é para este grupo de agentes de ameaça para realmente explorar essa vulnerabilidade?
Teórica (1), difícil (3), fácil (5), ferramentas automatizadas disponíveis (9)

- **Consciência**

Quão bem conhecido é essa vulnerabilidade para este grupo de agentes de ameaça?
Desconhecido (1), escondido (4), obvio (6), de conhecimento público (9)

- **Detecção de intruso**

Qual a probabilidade de um exploit ser detectado?

Detecção ativa na aplicação (1), Logado e analisado (3), Logado sem análise (8), não registradas (9).

17.1.3. FATORES PARA ESTIMAR IMPACTO

Ao considerar o impacto de um ataque bem-sucedido, é importante perceber que existem dois tipos de impactos. O primeiro é o "impacto técnico" sobre a aplicação, os dados que ela usa, e as funções que ela oferece. O outro é o "impacto nos negócios" sobre o negócio e empresa que opera a aplicação.

O impacto nos negócios é o mais importante, no entanto, você não pode ter acesso a todas as informações necessárias para descobrir as consequências nos negócios de uma exploração bem-sucedida. Neste caso, fornecendo o máximo de detalhes sobre o risco técnico permitirá que o representante de negócios tome uma decisão sobre o risco do negócio.

Mais uma vez, cada elemento possui um conjunto de opções, e cada opção tem um

índice de impacto, de 0 a 9 associada a ele. Nós vamos usar esses números depois de estimar o impacto global.

- **Fatores de Impacto técnicos**

O impacto técnico pode ser dividido em fatores alinhados com as áreas da segurança: confidencialidade, integridade, disponibilidade e prestação de contas. O objetivo é o de estimar a magnitude do impacto sobre o sistema se a vulnerabilidade fosse explorada.

- **Perda de confidencialidade**

Quantos dados poderiam ser divulgados e quão sensível é?

Dados não sensíveis minimamente divulgados (2), dados críticos minimamente divulgados (6), dados não sensíveis divulgados completamente (6), dados críticos divulgados completamente (7), todos os dados divulgados (9)

- **A perda de integridade**

A quantidade de dados pode ser corrompida e quão danificado é?

Dados minimamente corrompidos (1), dados significantes minimamente corrompidos (3), dados ligeiramente corrompidos, porém, extensivamente (5), dados significantes extensivamente corrompidos (7), todos os dados totalmente corrompidos (9)

- **A perda de disponibilidade**

Quanto o serviço poderia ser perdido e quão vital é?

Serviços secundários minimamente interrompidos (1), serviços primários minimamente interrompidos (5), serviços secundários extensivamente interrompidos (5), serviços primários extensivamente interrompidos (7), todos os serviços completamente interrompidos (9)

- **Perda de prestação de contas**

São as ações dos agentes de ameaça "feitas com base em um indivíduo?" Totalmente rastreável (1), possivelmente rastreável (7), completamente anônimo (9)

Fatores de Impacto de Negócios

O impacto nos negócios decorre do impacto técnico, mas exige uma profunda compreensão do que é importante para a empresa. Em geral, devemos suportar nossa análise de riscos com impacto nos negócios, especialmente se sua audiência é nível executivo. O risco do negócio é o que justifica o investimento em corrigir problemas de segurança.

Os fatores a seguir são áreas comuns para muitas empresas:

- **Prejuízo financeiro**

Quanto dano financeiro resultará de um exploit?

Menos do que o custo para consertar a vulnerabilidade (1), efeito menor sobre o lucro anual (3), efeito significativo sobre o lucro anual (7), a falência (9)

- **Danos à reputação**

Quanto uma exploração resultaria em danos à reputação a ponto de prejudicar o negócio?

Danos mínimos (1), perda de grandes contas (4), perda de clientela (5), danos à marca (9)

- **Não cumprimento**

Quanto um exploit pode afetar em compliance?
Violação menor (2), violação clara (5), violação de alto perfil (7)

- **Violação de privacidade**

Quantas informações pessoais podem ser divulgadas?

Um indivíduo (3), centenas de pessoas (5), milhares de pessoas (7), milhões de pessoas (9).

17.1.4. DETERMINANDO A GRAVIDADE DO RISCO

Nesta etapa a estimativa de probabilidade e a estimativa de impacto são colocadas juntas para calcular a gravidade global para este risco. Isso é feito para descobrir se a probabilidade é baixa, média ou alta e, em seguida, fazer o mesmo para o impacto. A escala de 0 a 9 é dividida em três partes:

Níveis de probabilidade	**Impacto**
0 até 3	Baixo
3 até 6	Médio
6 até 9	Alto

- **Método repetitivo**

Para se ter uma gestão de riscos mais eficiente é necessário passar por um processo mais formal de classificação dos fatores e calcular o resultado. Lembre-se que há um

monte de incertezas nestas estimativas e que esses fatores são destinados a ajudar o testador a chegar a um resultado razoável. Este processo pode ser suportado por ferramentas automatizadas para tornar mais fácil o cálculo.

A primeira etapa consiste em selecionar uma das opções associadas com cada um dos fatores e introduzir o número associado na tabela. Em seguida, basta fazer a média das pontuações para calcular a probabilidade global. Por exemplo:

Agente de ameaça					Fatores de vulnerabilidade			
Nível de Habilidade	Motivo	Oportunidade	Tamanho		Facilidade de Descoberta	Facilidade de Explorar	Consciência	Detecção de Intruso
5	2	7	1		3	6	9	2
Probabilidade Geral: 4.375 (Médio)								

Em seguida, o testador precisa descobrir o impacto global. O processo é semelhante aqui. Em muitos casos, a resposta será óbvia, mas o testador pode fazer uma estimativa com base nos fatores, ou eles podem calcular a média das pontuações para cada um dos fatores. Mais uma vez, inferiores a 3 é baixo, de 3 a menos do que 6 é médio, e 6 a 9 é alto. Por exemplo:

Impactos técnicos					Impactos no negócio			
Perda de confidencialidade	Perda de integridade	Perda de Disponibilidade	Perda de prestação de contas		Danos financeiros	Danos à reputação	Não Cumprimento	Violação de privacidade
9	7	5	8		1	2	1	5
Impacto técnico geral: 7.25 (Alto)					Impacto global de negócios: 2.25 (Baixo)			

- **Determinando a gravidade**

O analisador chega nas estimativas de probabilidade e de impacto, e ele agora pode

combiná-los para obter uma classificação de gravidade final para este risco. Caso tenha boas informações dos impactos de negócio ele vai usá-las ao invés das informações de impacto técnico. Mas se ele não tem informações sobre o negócio, então o uso do impacto técnico é a melhor escolha.

Gravidade do risco total				
Impacto	Alto	Médio	Alto	Crítico
	Médio	Baixo	Médio	Alto
	Baixo	Info	Baixo	Médio
		Baixo	Médio	Alto
	Probabilidade			

No exemplo acima, a probabilidade do impacto de negócio é média e o impacto técnico é alto, então, a partir de uma perspectiva puramente técnica verifica-se que a severidade global é alta. No entanto, note que o impacto nos negócios é realmente baixo, de modo que a gravidade geral é melhor descrita como baixa também. É por isso que a compreensão do contexto empresarial das vulnerabilidades que está sendo avaliada é tão crucial para tomar boas decisões de risco. A falha em entender este contexto pode levar à falta de confiança entre as equipes comerciais e de segurança que está presente em muitas organizações

17.1.5. DECIDINDO O QUE CONSERTAR

Depois que os riscos para a aplicação foram classificados haverá uma lista de prioridades do que corrigir. Como regra geral, os riscos mais graves devem ser corrigidos em primeiro lugar.

Lembre-se que nem todos os riscos valem a pena serem corrigidos e alguma perda não só é esperada, mas justificável com base no custo de corrigir o problema. Por exemplo, se custaria R$100.000,00 para implementar controles para conter R$ 2.000,00 de fraude por ano, levaria 50 anos para obter retorno sobre o investimento para acabar com a perda. Mas lembre-se de que pode haver danos à reputação da organização em decorrência da fraude, o que poderia custar à organização muito mais.

18. ANEXO B - POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS

A DMS LOGISTICS tem a responsabilidade de garantir o cumprimento à Lei Geral de Proteção de Dados Pessoais (LGPD) e seus requisitos relativos à coleta, armazenamento, recuperação e destruição de registros de dados pessoais e/ou dados sensíveis (“Dados Pessoais”).

Esta política complementa, e não substitui, a Política Geral de Privacidade de Dados e políticas afins.

O Sistema DMS LOGISTICS mantém conjuntos de Dados Pessoais armazenados (“Registros”) em conformidade com requisitos contratuais, regulatórios e demais bases legais aplicáveis às modalidades de tratamentos de Dados Pessoais.

É importante que esses Registros sejam protegidos contra perda, destruição, falsificação, acesso não-autorizado e liberação não-autorizada. Para isso, uma variedade de controles é usada, como backups, controle de acesso e criptografia.

Esse controle se aplica a todas as operações, pessoas e processos que constituem o sistema de informações do Sistema DMS LOGISTICS, incluindo colaboradores, membros do conselho, diretores, fornecedores, clientes e terceiros que têm acesso aos dados tratados pelo Sistema DMS LOGISTICS.

18.1. CLASSIFICAÇÃO DE RISCO

O Sistema DMS LOGISTICS classifica os registros em categorias que estabelecem os requisitos de retenção e de descarte para cada categoria.

Todos os Dados Pessoais serão retidos pelo tempo necessário ao cumprimento do objetivo para que foram coletados, com finalidades lícitas, específicas e informadas.

Há uma diversidade de tratamentos de Dados Pessoais cujo prazo de arquivamento não é determinado por lei, como, por exemplo, o tempo de guarda dos Dados Pessoais de um prospecto comercial. Para tais dados, o Sistema DMS LOGISTICS estipula um prazo de guarda que seja coerente com as práticas de mercado e com a natureza do tratamento, enquanto não houver determinação específica pela autoridade reguladora.

Para demais Registros, incluindo aqueles de ordem tributária, trabalhista e previdenciária, a DMS LOGISTICS se reserva o direito de mantê-los armazenados até o fim do prazo prescricional estipulado em lei.

18.1.1. CATEGORIA DE REGISTROS:

- Registros de Negócios: informações registradas em qualquer meio, criadas ou capturadas que reflitam circunstâncias, eventos, atividades, transações ou resultados criados ou mantidos como parte da condução de negócios do Sistema DMS LOGISTICS, como por exemplo, venda de produtos do portfólio do Sistema DMS LOGISTICS; celebração e execução de contratos; e análise e proteção do crédito.

- Registros de Marketing e Comunicação: informações pessoais obtidas pelo Sistema DMS LOGISTICS em (i) campanhas publicitárias, ações promocionais e pesquisas; (ii) redes sociais; e (iii) serviço de atendimento ao consumidor.

Os Registros que forem utilizados para fins de marketing ou de pesquisa permanecerão armazenados na base do sistema DMS LOGISTICS apenas enquanto perdurar o interesse do titular em receber esses materiais, sendo possibilitado a exclusão a qualquer tempo, o qual permite a revogação do consentimento, caso esta seja a base legal que fundamente a respectiva modalidade de tratamento.

- Registros de Recursos Humanos: Dados Pessoais coletados para (i) gestão do RH, como por exemplo, gerenciamento de tempo de trabalho, salários, benefícios, contribuições previdenciárias e impostos; férias, licenças, ausências; (ii) gestão de carreira, como treinamentos, avaliações, experiência profissional, mobilidade no Sistema DMS LOGISTICS; (iii) administração do RH para comunicação corporativa, trabalho em rede social da empresa e uso de ferramentas de computador e telefonia; organogramas, serviços corporativos, planejamento e orçamentos, relatórios, pesquisa, reorganizações, aquisições e cisões; (iv) saúde ocupacional, como atestados médicos, prontuário médico, atestados de saúde ocupacional e todos os demais relacionados à saúde do empregado; (v) recrutamento e seleção, como nome, gênero, estado civil, idade, dados de contato, RG, CPF, comprovante de endereço, dados bancários, informações de função, habilidades, experiências, qualificações, referências, currículo, dados de entrevista e avaliação, notas e registros da entrevista e qualquer outra informação que o candidato disponibilize para o Sistema DMS LOGISTICS; e (vi) gestão de viagens de negócios, como informações para organização de viagens (preferências, local etc.); CNH e despesas.

Alguns Dados Pessoais são retidos após o término do contrato de trabalho, estágio ou contrato de trabalho temporário para cumprir os períodos legais de armazenamento definidos pela legislação trabalhista ou tributária.

Os contratos de trabalho, as fichas de registro de empregados e os respectivos Perfis Profissiográficos Previdenciários (PPP) serão armazenados por período indeterminado, mesmo após a rescisão contratual.

- Registros de Segurança: informações coletadas para gerenciamento do acesso e permanência nas instalações do Sistema DMS LOGISTICS como nome, RG, CPF, foto, biometria, controle de crachá, instalações por CFTV, login e senha para acesso aos sistemas de informação do Sistema DMS LOGISTICS.

18.2. RETENÇÃO E DESCARTES DE DADOS PESSOAIS

Para cada um desses cenários, a tabela a seguir mostra o período máximo de retenção de Dados Pessoais pelo Sistema DMS LOGISTICS, por categoria de Registro, descrição, bem como o formato de descarte.

Tipo de Registro	**Descrição/Dados a serem excluídos**	**Período de Retenção**	**Formato de Descarte**
Negócios	Contato Comercial (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail)	05 anos após contato inicial sem resposta, ou prontamente, no caso de revogação do consentimento ou dá a manifestação de desinteresse em ser contatado	Eliminação pelo Sistema DMS LOGISTICS, opt-out, ou a qualquer tempo pelo titular
Negócios	Contratos Gerais (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail; conta bancária; dados de cobrança)	5 anos após o término do contrato	Eliminação pelo Sistema DMS LOGISTICS
Negócios	Documentos Tributários	5 anos a contar da data de emissão do documento	Eliminação pelo Sistema DMS LOGISTICS

Negócios	Proteção do Crédito (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail)	Durante relação comercial e mais 5 anos após o término ou prontamente, em caso de exaurimento da finalidade	Eliminação pelo Sistema DMS LOGISTICS
Marketing e Comunicação	Campanhas Publicitárias, Ações Promocionais e Pesquisas (nome, RG, CPF, endereço, país de origem, e-mail, telefone, respostas a pesquisas)	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou revogação do consentimento	Eliminação pelo Sistema DMS LOGISTICS ou Opt-out a qualquer tempo pelo titular
Marketing e Comunicação	Site e Redes Sociais (dados de geolocalização, endereço de IP, dados on line capturados, cookies)	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou revogação do consentimento	Eliminação pelo Sistema DMS LOGISTICS ou opt-out a qualquer tempo pelo titular

Marketing e Comunicação	Serviço de Atendimento ao Consumidor – SAC (nome, telefone, e-mail, endereço e CPF)	5 anos após o último atendimento	Eliminação pelo Sistema DMS LOGISTICS
Recursos Humanos	Gestão de RH	Durante Contrato de Trabalho e mais 5 anos após o término, exceto FGTS (30 anos) e Folha de Pagamento (10 anos) Armazenamento de Contrato de Trabalho: prazo indeterminado	Eliminação pelo Sistema DMS LOGISTICS

Recursos Humanos	Gestão de Carreira	Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pelo Sistema DMS LOGISTICS
Recursos Humanos	Administração do RH	Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pelo Sistema DMS LOGISTICS
Recursos Humanos	Saúde Ocupacional	Durante o contrato de trabalho e mais 20 anos após a rescisão contratual	Eliminação pelo Sistema DMS LOGISTICS
Recursos Humanos	Recrutamento e Seleção	Reprovação pré-entrevista: 15 dias Reprovação pós entrevista: 90 dias (nacional) ou 180 dias (internacional) Aprovação do candidato: Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pelo Sistema DMS LOGISTICS
Recursos Humanos	Recrutamento e Seleção	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou após revogação do consentimento Aprovação do candidato: Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pelo Sistema DMS LOGISTICS ou Opt-out a qualquer tempo pelo titular
Recursos Humanos	Gestão de Viagens de Negócios	Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pelo Sistema DMS LOGISTICS

Segurança	Acesso às instalações físicas do Sistema DMS LOGISTICS (dados biométricos, nome, foto, RG, CPF)	5 anos após o último acesso	Eliminação pelo Sistema DMS LOGISTICS
Segurança	Sistema CFTV (imagens)	3 meses após a gravação	Eliminação pelo Sistema DMS LOGISTICS
Segurança	Informações de Crachá (nome, cargo)	Durante Contrato de Trabalho	Eliminação pelo Sistema DMS LOGISTICS
Segurança	Acesso ao sistema de informação do Sistema DMS LOGISTICS (login e senha)	Durante Contrato de Trabalho	Eliminação pelo Sistema DMS LOGISTICS

18.3. ELIMINAÇÃO PELO SISTEMA DMS LOGISTICS

Assim que o período expirar, e desde que não haja uma razão válida para que os mantenhamos, os Dados Pessoais em cópia física serão destruídos como resíduo confidencial e aqueles mantidos eletronicamente serão excluídos dos sistemas da DMS LOGISTICS e de terceiros contratados.

Hipóteses de investigação em curso, processos administrativos e judiciais são razões válidas para manutenção dos Registros e, independentemente de consentimento, os períodos de armazenamento indicados acima poderão ser prorrogados nesses casos.

Se o titular dos dados optar por exercer seu direito de eliminação dessas informações, os Dados Pessoais serão descartados imediatamente pelo Sistema DMS LOGISTICS, exceto em hipóteses de cumprimento de obrigação legal ou regulatória.

18.4. CONTATO FACILITADO

As solicitações recebidas do titular de Registros para exercer seus direitos durante todo o período de tratamento serão respondidas da forma e dentro dos prazos exigidos pelas normas aplicáveis.

Para exercer seus direitos, o Titular pode enviar solicitações através do e-mail dpo@dmslog.com. O titular deve indicar claramente seu nome completo, inserir uma cópia de um documento de identificação e indicar o endereço para o qual a resposta deve ser enviada.

O Encarregado pode ser contatado em dpo@dmslog.com para responder dúvidas ou para obter mais informações sobre esta Política de Descarte e Anonimização de Dados.

19. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	06/02/2023	Emissão do documento.
01	28/02/2023	Revisão e padronização de todo o documento.

20. 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