POLÍTICA DE HARDENING

Código: POL-TI-008
Revisão: 01
Data: 24/02/23

WWW.DMSLOG.COM

1. PROPÓSITO

A Política de Hardening é uma declaração formal da DMS LOGISTICS acerca do seu compromisso com a proteção dos ativos de informação de sua propriedade e/ou sob sua guarda.

Seu objetivo principal é definir as diretrizes estratégicas para manter a Segurança da Informação e Comunicações, com o intuito de preservar a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações produzidos, adquiridos, armazenados, em trânsito, descartados, de propriedade ou sob controle ou operação do Sistema DMS LOGISTICS.

Ela busca prevenir ameaças, internas ou externas, minimizar eventuais riscos, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis.

Deverá, assim, ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

2. PRINCÍPIOS

São princípios básicos desta Política:

- A preservação da imagem da empresa e de seus empregados;
- A criação, desenvolvimento e manutenção de cultura de segurança da informação e comunicações;
- Que o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações sejam apropriados e adequados ao valor dos ativos da DMS LOGISTICS, considerando os impactos e a probabilidade de ocorrência de incidentes.
- A preservação da responsabilidade solidária para dados de outras empresas que trafegam nos ativos da DMS LOGISTICS.

3. ESCOPO

A Política de Hardening aplica-se a:

- Todos os ambientes físicos, incluindo-se a sede, filiais, unidades regionais, unidades de desenvolvimento, centros de processamento e quaisquer outros pertencentes ao patrimônio ou sob a custódia da DMS LOGISTICS.

- Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pela DMS LOGISTICS, o que inclui: computadores; roteadores e switches; banco de dados.

Todos os empregados, estagiários, jovens aprendizes e colaboradores de qualquer natureza da DMS LOGISTICS devem compreender e seguir as diretrizes desta política. Qualquer alteração nos sistemas e aplicações da DMS LOGISTICS devem seguir as normas.

3.1. REFERÊNCIAS NORMATIVAS

Este documento foi elaborado com base nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001, cláusulas A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5, A.8.7, A.8.8, A.8.15, A.8.17, A.8.18, A.8.19, A.8.24, A.8.25, A.8.27, A.8.29, A.8.30, A.8.31, A.8.32, A.8.33 e ABNT NBR ISO/IEC 27002, cláusulas 5.8, 5.15, 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.7, 8.8, 8.15, 8.17, 8.18, 8.19, 8.25, 8.26, 8.27, 8.29, 8.30, 8.31, 8.32, 8.33, todas reconhecidas mundialmente como códigos de práticas para a gestão da segurança da informação, bem como estão de acordo com as leis brasileiras vigentes.

3.2. HARDENING

Hardening é o procedimento que visa aprimorar a infraestrutura para enfrentar tentativas de ataques. Envolve a identificação de vulnerabilidades, mapeamento das ameaças, ações para mitigar ou minimizar os riscos e executar atividades corretivas.

O Hardening envolve a autenticação do usuário, sua autorização de acesso, manutenção de registros com vistas às auditorias, sincronização de relógios e técnicas de acesso à infraestrutura. Além destas ações, também envolve a manutenção de registros das operações, características de sistema, como por exemplo, manutenção de softwares atualizados e permissão de que fiquem ativos

somente os recursos efetivamente utilizados e requisitos de configuração como manutenção de backups, por exemplo. O não cumprimento desta política pode ter um efeito significativo no funcionamento eficiente da organização, sendo, portanto, da obrigação de todos os seus colaboradores, independente da hierarquia, seguir as orientações mencionadas neste documento.

4. PROCEDIMENTOS DE HARDENING

4.1. AUTENTICAÇÃO

Autenticação é o processo que busca verificar a identidade do usuário no momento em que este requisita o acesso. A ABNT NBR ISO/IEC 27000 define a autenticação como a garantia de que uma característica reivindicada de uma entidade está correta.

- Na DMS LOGISTICS, os procedimentos básicos de autenticação de usuários envolvem os seguintes requisitos:
- Deve ser criado um usuário para cada operador ativo, desativando contas antigas.
- Uma única conta padrão de administração não deve ser utilizada por usuários diferentes;
- As senhas de acesso devem ser fortes;
- As senhas não devem ser armazenadas em texto puro;
- O recurso de duplo fator de autenticação (MFA) deve ser utilizado.

4.2. AUTORIZAÇÃO

Ela tem a função de diferenciar os privilégios atribuídos aos usuários que foram autorizados para acessar os sistemas. Segue os princípios least privilege e need to know.

- Todos os usuários do Sistema DMS LOGISTICS devem obter permissão para acessar o equipamento de acordo com o seu trabalho.
- A senha de administrador não deve ser fornecida a todos os usuários, a fim de mitigar acidentes, agentes maliciosos ou sem a formação necessária para lidar com esses recursos internamente.
- Dispositivos externos, quando conectados à rede da DMS LOGISTICS, devem ser primeiramente autorizados pelo departamento de SI antes de ser conectado.

Os usuários devem estar classificados em um grupo de privilégio, funcionalidade que é permitida em vários sistemas.

4.3. AUDITORIA

O procedimento de auditoria é o acesso às informações relacionadas à utilização de recursos da infraestrutura pelos usuários.

Como procedimentos básicos, são necessários:

- Manter o registro de cada usuário com suas respectivas permissões.
- Registrar as ações dos usuários nos sistemas.
- Classificar os registros com nível de criticidade: Informativo, Aviso e Crítico.
- Classificar os registros em tipos: Documentos, Registros (Logs) e Backup de configuração.
- Os registros devem ter data e hora corretas.

4.4. ACESSO

O acesso aos equipamentos da rede deve ser feito de forma segura seguindo os seguintes procedimentos básicos:

- Todos os equipamentos serão criptografados;
- Todos os equipamentos possuem a solução de Endpoint Protection;
- Todos os equipamentos possuem uma regra de bloqueio por tempo de inatividade;
- O acesso aos recursos computacionais se dá através da solução de Gestão de Identidades e Acessos AWS (AWS IAM);
- Os acessos são liberados de acordo com as políticas de permissionamento definidas na plataforma AWS IAM;
- As permissões variam de acordo com a função do colaborador;
- Toda atividade executada dentro da plataforma é registrada e gerenciada através das soluções AWS IAM, AWS CloudWatch e AWS CloudTrail;

4.5. REGISTROS

Todos os registros (logs) obtidos da operação e configuração da rede devem seguir os seguintes procedimentos básicos:

- Os registros serão configurados com diferentes níveis de criticidade;
- Os logs serão armazenados de maneira segura dentro da solução AWS CloudTrail;

- Os logs terão sua integridade verificada pelo recurso de monitoramento de integridade de arquivo (FIM) integrado na solução AWS CloudTrail;
- Data e horário dos registros são sincronizados com o NTP.br.

4.6. GESTÃO DE HORÁRIO DOS SERVIDORES

O sistema DMS LOGISTICS adota o Amazon Time Sync Service, um serviço de sincronização de horário fornecido pelo Network Time Protocol (NTP), que usa uma frota de relógios atômicos e conectados por satélite redundantes em cada região para fornecer um relógio de referência altamente preciso. Este serviço está disponível em todas as regiões públicas da AWS para todas as instâncias em execução em uma VPC.

Entendemos que a sincronização de tempo é crítica, pois todos os aspectos do gerenciamento, proteção, planejamento e depuração de uma rede envolvem a determinação de quando os eventos ocorrem. O tempo também fornece o único quadro de referência entre todos os dispositivos na rede. Sem tempo sincronizado, é difícil, até impossível, correlacionar com precisão os arquivos de log entre esses dispositivos. Além disso:

O rastreamento de violações de segurança, uso da rede ou problemas que afetam um grande número de componentes pode ser quase impossível se os registros de data e hora nos logs forem imprecisos. O tempo geralmente é o fator crítico que permite que um evento em um nó da rede seja mapeado para um evento correspondente em outro.

Para reduzir a confusão nos sistemas de arquivos compartilhados, é importante que os tempos de modificação sejam consistentes, independentemente da máquina em que os sistemas de arquivos estejam.

As regras de segurança Sarbanes-Oxley, BACEN e CVM requerem registro de data e hora preciso, por tais aspectos a gestão de horários de servidores e serviços do sistema DMS LOGISTICS é sempre verificada e testada.

4.7. PATCHING

Sistemas Operacionais têm programas/softwares próprios que podem conter falhas de segurança. Para evitar isso, os sistemas operacionais e muitos aplicativos de software têm patches de segurança periódicos, lançados pelo fornecedor, que precisam ser aplicados.

Isso porque uma dessas falhas pode permitir que um hacker comprometa um computador e, por consequência, ameaçar a integridade da rede da DMS LOGISTICS e de todos os computadores conectados a ela.

A DMS LOGISTICS utiliza os sistemas operacionais Microsoft Windows, Linux e IOS.

Os patches relacionados a eles, sejam de segurança ou de natureza crítica, devem ser instalados o mais rápido possível.

No Anexo B deste documento encontra-se a descrição dos requisitos para manter os sistemas e softwares atualizados em todos os sistemas de TI gerenciados e mantidos pela DMS LOGISTICS.

4.8. SISTEMA

Todos os novos sistemas deverão seguir as seguintes recomendações:

- Fazer a instalação seguindo as recomendações do fornecedor;
- Desativar as interfaces não utilizadas;
- Desativar os serviços não utilizados, inseguros, DNS recursivo e Servidor NTP.
- Remover ou desativar pacotes de funções extras não utilizados;
- Desabilitar os protocolos de descoberta de vizinhança, como CDP, MNDP e LLDP;
- Fazer a manutenção do sistema sempre atualizado na versão mais recente e estável (LTS).
- Aplicar todos os patches de segurança, conforme validação de testes e verificação de CVE.
- Fazer o scan de vulnerabilidades. As vulnerabilidades encontradas deverão ser corrigidas.

4.9. SISTEMA DE CONTÊINERES

O processo de proteção da DMS LOGISTICS é contínuo. Ele é integrado ao processo de desenvolvimento e é automatizado para reduzir a intervenção humana.

A segurança de contêineres é uma medida adicional de segurança que visa proteger os processos da DMS LOGISTICS. Ela visa a implementação de ferramentas e políticas de segurança para garantir que tudo no container da DMS LOGISTICS esteja funcionando como pretendido, incluindo proteção de infraestrutura, cadeia de suprimentos de software, tempo de execução, etc.

Para maior detalhamento dessa normativa, ver o Anexo A - Segurança de contêineres.

4.10. MULTI-TENANCY

A DMS LOGISTICS utiliza uma arquitetura multi-tenancy na sua aplicação, para suportar múltiplos inquilinos ao mesmo tempo.

A DMS LOGISTICS adota o multi-tenancy para reduzir a complexidade do processo de gestão do software para os seus múltiplos clientes. Ela aumenta a segurança pois, em caso de atualização, não há o risco de algum cliente não atualizar, pois a instância do software é única.

A arquitetura do multi-tenancy fornece separação entre os clientes (inquilinos), em que uma instância compartilhada de um aplicativo de software instalado em um servidor pode atender a vários clientes. Portanto, os clientes da DMS LOGISTICS têm ambientes separados, e um não pode acessar o ambiente do outro, garantindo segurança, alta disponibilidade, confiabilidade e escalabilidade. Os clientes não podem acessar os dados uns dos outros.

Os clientes podem personalizar as configurações do seu ambiente, mas não podem acessar o código do aplicativo.

5. CONFIGURAÇÕES

Como requisitos de configurações, todos os ativos deverão:

- Manter sempre um backup atualizado das configurações atuais.
- Manter um script de hardening de máquinas da rede.
- Manter o script de hardening atualizado: cada nova política precisa ser agregada ao script.

Depois de seguir todos estes passos, o sistema poderá ser utilizado.

6. DISPOSIÇÕES GERAIS

Apenas softwares aprovados pelo departamento de SI serão autorizados a se conectarem à rede do Sistema DMS LOGISTICS.

Aplicações que não sejam necessárias para o trabalho deverão ser desinstaladas e removidas.

Os ativos serão configurados para prevenir e bloquear a execução de softwares não aprovados.

Todos os computadores seguem uma configuração padrão de segurança. Se for necessária alguma alteração, ela deverá ser avaliada e autorizada pelo departamento de SI.

As senhas padrão deverão ser alteradas após a instalação dos softwares.

A utilização de programas utilitários que podem sobrepor os controles dos sistemas e aplicações é vetada. Para mais detalhes, veja a Política de Gerenciamento de Redes.

Fornecedores terceirizados não devem receber qualquer acesso à rede da DMS LOGISTICS sem prévia permissão do departamento de SI. Qualquer alteração indevida ou acesso sem permissão deve ser informado imediatamente ao departamento de SI para que possa ser investigado e, se necessário, interrompido.

Visitantes não devem ter acesso à rede corporativa da DMS LOGISTICS.

Para acessar o sistema, deve ser feita uma solicitação para o departamento de Segurança da Informação. Apenas após a autorização e liberação pelo departamento de Segurança da Informação, será possível acessar o Sistema DMS LOGISTICS.

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

Cabe ao usuário assegurar que seu ID e senha não sejam utilizados por terceiros, impedindo que estes sejam utilizados para a obtenção de acesso não autorizado aos sistemas da DMS LOGISTICS.

Não é permitido acessar ou alterar as configurações de rede de forma alguma. Toda e qualquer situação semelhante, deve ser reportada ao departamento de SI.

As alterações na configuração das redes e sistemas devem ser feitas de acordo com o previsto na Política de Gerenciamento de Mudanças. A infraestrutura de redes segue um conjunto de protocolos aprovados pelo CISO. Qualquer mudança deve ser aprovada previamente pelo CISO.

O uso de mídias removíveis será controlado. Para mais informações, ver a Política de Dispositivos Móveis.

7. PENALIDADES

O não cumprimento dos princípios e diretrizes desta e de qualquer outra Política de Segurança da DMS LOGISTICS, suas normas e procedimentos agregados, sujeita o infrator às penalidades previstas em lei e nos regulamentos internos.

8. IMPLEMENTAÇÃO E ATUALIZAÇÃO

A Política de Hardening do sistema DMS LOGISTICS deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

9. ANEXO A - SEGURANÇA DE CONTÊINERES

A segurança de contêineres é uma medida adicional de segurança que visa proteger os processos da DMS LOGISTICS. Ela visa a implementação de ferramentas e políticas de segurança para garantir que tudo no container da DMS LOGISTICS esteja funcionando como pretendido, incluindo proteção de infraestrutura, cadeia de suprimentos de software, tempo de execução, etc.

Ao proteger seus contêineres, os principais focos da DMS LOGISTICS são:

- A segurança do host do container;
- Tráfego de rede do container;
- A segurança da aplicação dentro do container;
- Comportamento malicioso dentro da sua aplicação;
- Proteger sua stack de gestão do container;
- As camadas fundamentais de sua aplicação;
- A integridade de seu pipeline de desenvolvimento.

9.1. SEGURANÇA CONTÍNUA DE CONTÊINERES

O processo de proteção da DMS LOGISTICS é contínuo. Ele é integrado ao processo de desenvolvimento e é automatizado para reduzir a intervenção humana. Deve ser estendido à manutenção e operação da infraestrutura subjacente até o limite permitido pela AWS.

Ele protege as imagens do container do pipeline de construção e as camadas de host, plataforma e aplicação do tempo de execução. A implementação da segurança como parte do ciclo de vida de entrega contínua visa a redução dos riscos e as vulnerabilidades da DMS LOGISTICS em uma superfície de ataque cada vez maior.

Esse processo contínuo está relacionado a:

- Proteção das aplicações e do pipeline de contêineres.
- Proteção dos ambientes de implantação de contêineres.
- Proteção da infraestrutura.

9.2. SEGURANÇA NO PIPELINE DOS CONTAINERS

Coleta de Imagens

Os contêineres são criados a partir de camadas de arquivos. A imagem base é a mais importante para fins de segurança, porque ela é usada como ponto de partida para criar imagens derivadas. Com isso em foco somente são utilizadas imagens de repositórios oficiais ou desenvolvidas internamente.

A DMS LOGISTICS, ao coletar imagens de container, verifica:

- Assinatura por fonte confiável;
- Atualização das camadas do sistema operacional e do ambiente de execução;
- Periodicidade de atualização do container;
- Identificação e rastreio de problemas conhecidos;
- Gerência de acesso

Em sequência a coleta das imagens, se inicia a divulgação de todas as imagens de container usadas pela equipe e o acesso a elas. Ou seja, proteger as imagens obtidas por download e as criadas. Faz uso de um registro privado para controlar o acesso por meio de atribuições de funções, além de gerenciar o conteúdo, designando metadados ao container que fornecem informações para identificar e rastrear vulnerabilidades conhecidas, além de automatizar e atribuir políticas nas imagens de container armazenadas.

Do gerenciamento do acesso, é conferido:

- Quais controles de acesso baseado em funções para gerência de imagens de container serão utilizados
- Definição de aplicação de tags para classificar as imagens
- Registro de metadados visíveis para rastreio de vulnerabilidades conhecidas
- Utilizar o registro para atribuir e automatizar políticas

9.3. TESTE DE SEGURANÇA E IMPLANTAÇÃO

A última etapa do pipeline é a implantação. Nesse momento, depois de concluir as compilações, elas são gerenciadas e as políticas são automatizadas para sinalizar compilações que têm problemas de segurança, principalmente ao encontrar novas vulnerabilidades.

Em seguida, executam-se ferramentas de análise de componentes que rastreiam e sinalizam problemas.

- Ao integrar o teste de segurança e automatizar a implantação, é conferido:
- Evitar a aplicação de patches nos containers em execução
- Usar acionadores para recompilar e substituir containers com atualizações automatizadas

9.4. PROTEÇÃO A INFRAESTRUTURA

Outra camada da segurança de contêineres é o isolamento proporcionado pelo sistema operacional host. O sistema operacional host é ativado por meio de um ambiente de execução de container. Ele deve ser gerenciado por um sistema de

orquestração.

A DMS LOGISTICS, ao decidir como proteger a infraestrutura de contêineres, confere:

- Quais containers precisam acessar outros;
- Como eles detectam os outros contêineres;
- Como controlar o acesso aos recursos compartilhados e como fazer o gerenciamento deles;
- Como gerenciar atualizações de host;
- Necessidade de atualização simultânea dos containers;
- Como monitorar a integridade dos containers;
- Como escalar automaticamente a capacidade das aplicações para atender à demanda.

9.5. IMPLEMENTAÇÃO E ATUALIZAÇÃO

A Segurança de Contêineres da DMS LOGISTICS deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

10. ANEXO B - APLICAÇÃO DE PATCHING

As máquinas usadas no ambiente DMS LOGISTICS utilizam, de acordo com a necessidade da função, três sistemas operacionais: Microsoft Windows, Linux e IOS.

Seus princípios e diretrizes são:

- A DMS LOGISTICS é responsável por manter a confidencialidade, integridade e disponibilidade dos dados mantidos em seus sistemas de TI dentro e fora do local, incluindo sistemas e serviços fornecidos por terceiros, mas gerenciados pela companhia.
- A DMS LOGISTICS tem a obrigação de fornecer proteção adequada e adequada de todo o seu patrimônio de TI, seja físico, virtual, local ou na nuvem.

Os patches são classificados conforme mostrado nas tabelas abaixo, de acordo com o Microsoft severity rating system:

Classificação	Descrição
Crítico	Possuem vulnerabilidades cuja exploração pode permitir a disseminação de vírus sem ação do usuário.
Importante	Têm vulnerabilidades que podem comprometer a confidencialidade, integridade e disponibilidade dos dados dos usuários ou a integridade e disponibilidade de recursos de processamento de dados.

Moderado	Patches cujos riscos de exploração são mitigados de forma significativa através de configurações padrão, auditoria ou dificultando sua exploração.
Baixo	Possuem vulnerabilidades cuja exploração é extremamente difícil ou que seu impacto seja mínimo.

10.1. RESPONSABILIDADES

O Chief Information Officer é responsável por garantir que a atualização de software e a Política de Patching sejam cumpridas.

O Gerente de Serviços de TI é responsável por garantir que o software no escopo seja mantido por meio de atualizações e patches regulares de software.

Os proprietários do sistema são responsáveis por garantir que todos os softwares no escopo que eles gerenciam sejam mantidos por meio de atualizações de software e patches regulares.

O departamento de TI da DMS LOGISTICS é responsável por garantir que todos os softwares no escopo que eles gerenciam sejam mantidos por meio de atualizações de software e patches regulares.

O departamento de TI da DMS LOGISTICS é responsável por avaliar rotineiramente a conformidade com a Política de Patching e fornecer orientação a todos os grupos de interessados em relação a questões de segurança e gerenciamento de patches.

Os fornecedores terceirizados são responsáveis por garantir que todos os softwares no escopo que eles gerenciam sejam mantidos por meio de atualizações e correções regulares de software, tanto antes quanto durante sua implantação operacional. Quando isso não for possível, isso deve ser escalado para o departamento de TI da DMS LOGISTICS.

10.2. ORIENTAÇÕES PARA ATUALIZAÇÃO DE SOFTWARES E PATCHING

- Todos os sistemas de TI, sejam de propriedade da DMS LOGISTICS ou aqueles em processo de desenvolvimento e suporte de terceiros, devem ser licenciados adequadamente, com suporte do fabricante e executar sistemas operacionais atualizados e corrigidos.
- Qualquer sistema de TI que não seja mais licenciado ou suportado pelo fabricante será removido da rede da DMS LOGISTICS.

- Os fornecedores terceirizados devem estar preparados para fornecer evidências de patches atualizados antes que os sistemas de TI sejam aceitos e comecem a ser operacionalizados.

- Novos sistemas devem ser atualizados para a linha de base atual acordada antes de ficarem online, para limitar a introdução de novas ameaças.

- Os servidores devem atender aos requisitos mínimos recomendados que são especificados pelo departamento de TI da DMS LOGISTICS, que inclui: o nível de sistema operacional padrão; pacotes de serviço; hotfixes e níveis de patching. Todas as exceções devem ser documentadas pelo departamento de TI da DMS LOGISTICS.

- Uma vez alertados sobre um novo patch, os administradores de TI farão o download e revisarão o novo patch. O patch será categorizado por criticidade para avaliar o impacto e determinar o cronograma de instalação.

- Os testes serão realizados usando um sistema de teste que se aproxima dos sistemas de produção. Onde não houver um sistema de teste, os resultados do patch de outro sistema de produção não-chave serão usados e os resultados de qualquer patch serão monitorados de perto quanto a efeitos adversos.

- Um plano de contenção/backup que permita o retorno às configurações de trabalho anteriores deve estar em vigor antes de qualquer atualização.

- Os sistemas que forem removidos da rede por falta de patching só serão reconectados quando for comprovado que foram atualizados e não representam mais risco para a rede da DMS LOGISTICS.

- Caso um patch crítico ou relacionado à segurança não possa ser implantado centralmente pela TI, ele deve ser instalado em tempo hábil, usando os melhores recursos disponíveis.

- A falha em configurar corretamente novas estações de trabalho é uma violação desta política. Desabilitar, contornar ou adulterar proteções de gerenciamento de patches e/ou software é expressamente proibido e constitui uma violação da política.

10.3. CONFIGURAÇÕES DO AMBIENTE OPERACIONAL

Todas as configurações relativas ao ambiente operacional da DMS LOGISTICS são feitas através do Puppet e versionadas no Bitbucket, com isso conseguimos garantir que todas as máquinas estão rodando as mesmas versões dos softwares evitando assim diferenças entre os ambientes produtivos.

O Puppet também é utilizado para a aplicação de patchs de correção dos serviços que

são gerenciados por ele respeitando o seguinte fluxo:

- A atualização é feita no ambiente de desenvolvimento
- São realizados os testes para verificar se essa atualização não causou nenhum problema na aplicação. Deve ser agendado a aplicação do patch em produção
- O acompanhamento dos patches de segurança deve ser feito assinando a lista de anúncios de segurança do Ubuntu (https://lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce) e Debian (http://www.debian.org/MailingLists/subscribe), além de acompanhar a lista de atualizações do Debian - https://www.debian.org/security/. O Amazon Linux 2 atualiza os boletins de segurança e eventos de privacidade através do Amazon Linux Security Center (ALAS) - https://alas.aws.amazon.com/alas2.html

10.4. IMPLEMENTAÇÃO E ATUALIZAÇÃO

A normativa de patching da DMS LOGISTICS deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

11. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	09/02/2023	Criação do documento.
01	24/02/2023	Revisão e padronização de todo o documento.

12. 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