POLÍTICA DE CRIPTOGRAFIA

Código: POL-TI-003
Revisão: 01
Data: 28/02/2023

WWW.DMSLOG.COM

1. PROPÓSITO

O objetivo das regras sobre Segurança da Informação da DMS LOGISTICS. é assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

A informação é um ativo e o acesso a ela deve ser gerenciado adequadamente para garantir que a confidencialidade, integridade e disponibilidade sejam mantidas. A criptografia de informações e dispositivos ajuda a mitigar o risco de interceptação, divulgação e acesso não autorizados.

A DMS LOGISTICS utiliza criptografia para proteger dados e informações enquanto armazenados, processados e manejados, proteger as credenciais de usuários e permitir comunicações seguras.

Esta política estabelece a abordagem da DMS LOGISTICS aos controles e gerenciamentos criptográficos, e provê os requisitos e responsabilidades para garantir que os objetivos da segurança da informação e da governança de dados sejam alcançados.

A criptografia permite que dados estejam seguros fazendo com que não possam ser lidos por aqueles que não possuem as chaves para descriptografá-los, provendo confidencialidade. A criptografia permite que sejam alcançados níveis de integridade e autenticação que garantem a segurança dos dados e informações.

A Lei Geral de Proteção de Dados (LGPD) requer que as empresas implementem medidas técnicas apropriadas para proteger os dados sob sua posse, incluindo dados em repouso e em trânsito. A criptografia é um método que cumpre essa função. Ela pode servir para prover integridade a dados que poderão ser livre e publicamente lidos, mas devem ser transmitidos e armazenados de forma segura.

A DMS LOGISTICS trabalha para estabelecer e aprimorar, continuamente, uma cultura corporativa em Segurança da Informação, compatível com o uso aceitável

das informações e dos ativos que as suportam, de forma a minimizar riscos e criar um ambiente seguro para a realização das atividades da Empresa.

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. ESCOPO

Esta Política 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 do DMS LOGISTICS.

Todos os ambientes computacionais e ativos de informação pertencentes ou custodiados pela DMS LOGISTICS.

Todos os empregados, estagiários, jovens aprendizes e colaboradores de qualquer natureza jurídica do DMS LOGISTICS.

Todos os sistemas de processamento de informações utilizados pela DMS LOGISTICS que utilizam criptografia ou que tenham que proteger dados devem cumprir o estabelecido nesta política.

3. 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.

4. OBJETIVOS

4.1. ESTA POLÍTICA TEM OS SEGUINTES OBJETIVOS:

- Reduzir os riscos relacionados à informação a níveis apropriados e aceitáveis;
- Proteger a confidencialidade, integridade e disponibilidade dos ativos, serviços e dados digitais da DMS LOGISTICS;
- Garantir que as informações da companhia estejam apropriadamente protegidas de roubo ou perda acidental do dispositivo onde estão armazenadas;
- Garantir que as informações da companhia estejam apropriadamente protegidas quando forem transferidas de sistema para sistema;
- Observar os temas-chave da resiliência cibernética, quais sejam: Identificar, Proteger, Detectar, Responder e Recuperar;
- Estabelecer padrões mínimos e responsabilidades para a criptografia de ativos digitais;
- Garantir que a criptografia seja gerenciada de forma consistente e apropriada;
- Prover a segurança aos donos das informações de que suas informações estão protegidas.

5. POLÍTICA

Todas as tecnologias e técnicas de criptografia utilizadas pela DMS LOGISTICS devem ser aprovadas pela Equipe de Segurança da Informação da companhia. Esta Equipe é a responsável pela distribuição e gerenciamento de todas as chaves de criptografia.

Todo uso de tecnologia de criptografia deve ser gerenciado de maneira que permita que os funcionários designados pela DMS LOGISTICS tenham prontamente acesso a todos os dados, inclusive para fins de investigação e continuidade do negócio da companhia.

A Equipe de Segurança da Informação da DMS LOGISTICS irá criar e publicar os padrões de criptografia, que devem incluir minimamente:

● O tipo, força e qualidade do algoritmo de criptografia requerido para vários níveis de proteção;

- Gerenciamento do ciclo de vida das chaves, incluindo a geração, armazenamento, recuperação, distribuição, fim da utilização e destruição das

chaves.

Todas as informações da DMS LOGISTICS classificadas como confidenciais devem ser criptografadas quando forem transferidas eletronicamente ou através de redes públicas; armazenadas em dispositivos móveis de armazenamento; armazenadas em laptops ou outros dispositivos móveis de computação; e quando em repouso.

A política de criptografia da DMS LOGISTICS prevê a adoção de medidas para os dados em trânsito e em repouso para seus servidores e sistemas.

As medidas para a proteção de dados em repouso podem incluir:

- Criptografia do disco completo;
- Criptografia do arquivo completo;
- Criptografia do aplicativo completo;
- Criptografia da base de dados completa.

Todos os sistemas usam certificado HTTPS desde a autenticação.

A criptografia deve ser implementada usando métodos e tecnologias aprovadas. Os padrões, algoritmos, protocolos e chaves de criptografia devem cumprir os padrões aceitáveis. As cifras, protocolos e algoritmos que não são suportados devem ser desabilitados onde for possível.

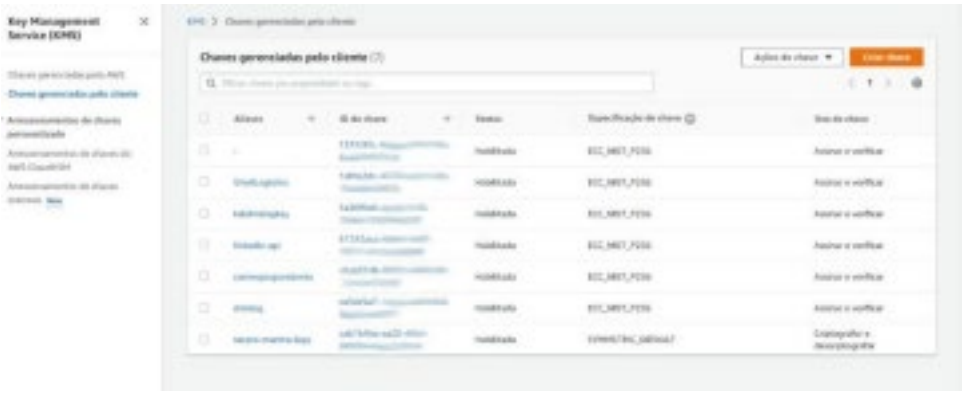
Os algoritmos de criptografia e implementações específicas de algoritmos podem conter vulnerabilidades. O uso de software de algoritmos e criptografia deve ser monitorado e gerenciado através da Política de Gestão de Vulnerabilidades.

Os sistemas, infraestruturas e aplicações e serviços devem ser configurados para aceitar somente conexões que estejam de acordo com estes requisitos.

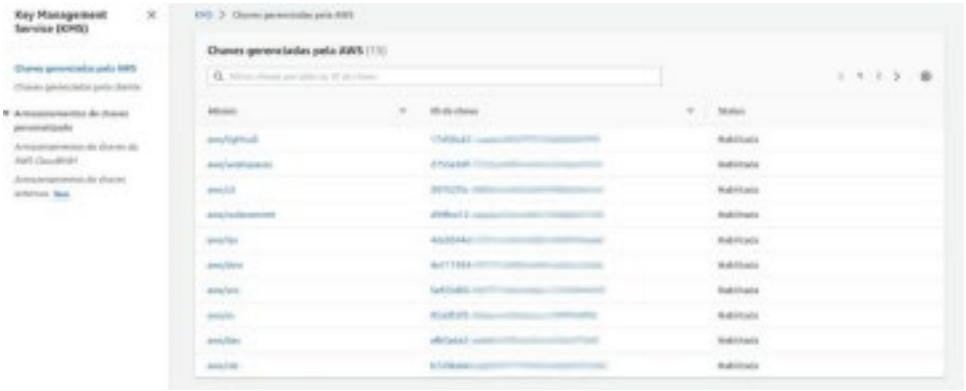
As chaves criptográficas devem ser geradas, armazenadas e gerenciadas de maneira segura e que previna sua perda, roubo ou comprometimento. O acesso às chaves criptográficas deve ser transmitido através de métodos confiáveis e seguros para manter a confidencialidade e integridade. Canais separados de comunicação devem ser usados para a transferência das chaves e dados. Sob nenhuma circunstância as chaves e os dados criptografados devem ser transferidos juntos, pelo mesmo meio.

Devem ser seguidos os procedimentos e controles para a revogação de chaves e certificados quando houver comprometimento ou expiração dos mesmos.

Por usar a nuvem da AWS não existe delay nem overhead computacional nas medidas implementadas. Evidências de criptografias.
Evidência 1:



Evidência 2:



O monitoramento da criptografia é feito com a ferramenta da AWS, o CloudWatch.

Para os desenvolvedores existe a liberdade de uso do sistema operacional que lhe convier, no entanto é obrigatório que os HD 's dos desktops e laptop estejam criptografados.

6. CHAVES

A política de criptografia da DMS LOGISTICS define que o ciclo de vida das chaves de criptografia passa em quatro fases gerais: pré-operacional, operacional, pós-operacional e destruição.

Na fase pré-operacional, o material criptográfico ainda não está disponível para uso, mas está em processo de criação ou ativação.

Na fase operacional o material criptográfico está disponível para uso normal.

Na fase pós-operacional o material criptográfico não está mais disponível para uso normal, mas o acesso ao mesmo ainda é possível em determinadas circunstâncias.

Por fim, a fase de destruição onde as chaves são destruídas, assim como todos os registros de sua existência.
A gestão das chaves de criptografia no ambiente AWS se dá pela solução AWS Key Management Service (KMS), garantindo assim a integridade e confiabilidade dos dados. Em ambiente local as chaves são armazenadas em repositório apartado (e-mail dedicado) e gerenciadas pelo Diretor de TI.

7. USUÁRIOS

A política de criptografia da DMS LOGISTICS verifica a identidade de um usuário. Somente após a autenticação, é possível utilizar as informações do usuário autenticado no sistema para definir as autorizações deste usuário.

O uso das chaves criptográficas só é permitido após a identificação do usuário.

Assim, para o gerenciamento adequado das chaves, o sistema deve fornecer mecanismos de autenticação e autorização ou permitir a utilização das chaves nos sistemas já existentes.

8. EXCEÇÕES

Qualquer exceção aos requisitos definidos neste documento deve ser justificada, com riscos sendo avaliados, documentados e aprovados pela Equipe de Segurança da Informação, em contato com o proprietário dos dados.

9. IMPLEMENTAÇÃO E ATUALIZAÇÃO

A Política de Criptografia – N2 do sistema DMS LOGISTICS ser atualizado sempre que necessário ou em um intervalo não superior a 01 (um) ano.

10. HISTÓRICO DE REVISÃO

REVISÃO	DATA	DESCRIÇÃO
00	08/02/2023	Criação do documento.
01	28/02/2023	Revisão e padronização do documento

11. APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	CyberSecurity Team	
Revisado por:	Leonardo Sabbadim	
Aprovado 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