POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

NOVEMBRO – 2022

Sumário

Responsável:	Emilson Queiroz (Gerente TI e Cloud)
Aprovado por:	Suleiman Bragança (CEO)
Data de Aprovação:	11/2022
Data de Revisão:	04/2024
Versão atual:	3.0

1 - OBJETIVO

A Política de Classificação da Informação, visa prover diretrizes para a segurança da informação, relacionadas ao manuseio, controle, proteção (contra indisponibilidade, divulgação imprópria, acesso indevido e modificação não autorizada de informações e de dados) e descarte, promovendo a melhoria contínua dos processos relacionados à segurança da informação, mantendo a confidencialidade, integridade e disponibilidade das informações;

2 - ABRANGÊNCIA

Aplica-se, independentemente de suas atribuições e responsabilidades, a todos os colaboradores da Vector e suas afiliadas, assim entendidas as empresas por ela controladas, sob controle comum e/ou coligadas, doravante denominadas em conjunto simplesmente como Vector.

3 - DOCUMENTAÇÃO COMPLEMENTAR

Lei Federal nº 13.709/2018
Código de Conduta e Ética
Política de Segurança da Informação
Política para Manuseio de Dados
Política de Armazenamento de Dados
Política de Privacidade e Proteção de Dados

4 - DIRETRIZ

Recomendar que as informações sejam classificadas de acordo com seu valor, requisitos legais, criticidade, sensibilidade e sigilo.

5 - CONCEITO

De acordo com a ISO 27001, a classificação da informação tem o objetivo de assegurar o nível adequado de proteção para a informação. A classificação tem como base o seu valor, criticidade para a organização e requisitos legais.
A classificação da informação surgiu como forma de mitigar o vazamento de informações ou o acesso indevido por falta de conhecimento do tipo de dado que se encontra disponível

5.1 – Classificação de Documentos

- Confidencial ou Restrito – Quando sua exposição e uso por pessoas não autorizadas possa acarretar perdas financeiras, de imagem, de competitividade etc.

- Interno – Quando não for desejável que o documento se torne conhecido por pessoas de fora da empresa.

- Público – Documentos que podem ser divulgados a todos, isto é, funcionários, terceirizados, clientes, fornecedores, enfim ao público geral, sem que isso provoque impactos no negócio.

6. DEFINIÇÕES

São apresentadas a seguir definições essenciais para o melhor entendimento dessa Política de Classificação das Informações:

- Assunto – aquilo sobre o que o documento trata.
- Documento – toda e qualquer informação produzida que seja registrada ou recebida.
- Formato – modo como foi confeccionado.
- Informação pessoal – toda e qualquer informação relacionada a individuo de forma identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.
- Informação sigilosa – informação submetida, por tempo determinado, à restrição de acesso do público.
- Tipo de classificação – classificação de documento por suas características comuns no que se refere ao conteúdo ou técnica de registro.
- Tratamento da informação – toda e qualquer ações referentes à informação, seja desde a produção até seu controle.

No anexo I encontra-se o Glossário com exemplos dos itens listados acima. A alteração poderá ser realizada a qualquer momento, de acordo com a necessidade.

7 – ACESSO AS INFORMAÇÕES

As informações produzidas, manuseadas e guardadas pela VECTOR são bens públicos, e sua restrição de acesso deve ser realizada apenas em casos específicos. Esse direito é previsto na Lei de Acesso à Informação, definindo que o acesso é a regra, e o sigilo, a exceção.
A LAI (Lei de Acesso à Informação) prevê alguns casos onde se aplica a restrição de acesso à informação, os quais são apresentados a seguir.

1 - Acesso Restrito / Sigilo - As informações são classificados em informações pessoais, sigilosas por legislação específica ou em grau de sigilo, conforme tópicos abaixo:

- Informações pessoais - É considerado dado pessoal qualquer informação que permita identificar, direta ou indiretamente, uma pessoa que esteja viva, tais como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies.
- Informações sigilosas protegidas por legislação específica - São informações protegidas por outras legislações, sigilo bancário, fiscal, comercial, profissional e segredo de justiça por exemplo.
- Informações classificadas em grau de sigilo - São aqueles que contenham informações pessoais e funcionais com respeito à intimidade, vida privada, honra e imagem, prevenção e diagnóstico médico, ação judicial, apuração de responsabilidade e representação contra servidor (técnico ou professor).

8 – CLASSIFICAÇÃO

Para a realização da classificação devem ser considerados quatro aspectos importantes, os quais devem servir como norteadora. São eles:

- Integridade – informação atualizada, completa e mantida por pessoal autorizado.
- Disponibilidade – disponibilidade constante e sempre que necessário para pessoal autorizado.
- Valor – a informação deve ter um valor agregado para a instituição.
- Confidencialidade – acesso exclusivo por pessoal autorizado.

No que tange a confidencialidade, procurando um entendimento melhor desse conceito, foi traçado um paralelo entre esse aspecto, o grau de sigilo e o impacto causado por sua quebra, consolidado na tabela a seguir:

Grau de sigilo	Impacto causado pela quebra da confiabilidade
Público	Sem impacto.
Restrito	Dano médio, podendo ocasionar dano colateral não desejado
Sigiloso	Dano grave/severo, podendo causar sérios danos à instituição (afetando a imagem, gerar prejuízo financeiro, impactar nas operações e inviabilizar objetivos estratégicos).

8.1 – Identificação da Classificação

Tipo de Documento	Procedimento
Papel	Para documentos gerados na Vector a identificação deverá ser feita no cabeçalho de todas as páginas, inclusive na capa. Para documentos externos recebidos, deverá ser marcado com uma etiqueta na parte superior.
E-Mail	A identificação deverá ser identificada no assunto do e-mail e inserido termo na assinatura.
Documentos Eletrônicos	A identificação será padronizada no sistema utilizado - Nomeclatura.
Outros Tipos	A classificação deverá estar visível no início do documento.

9 – ARMAZENAMENTO E TRAMITAÇÃO

O armazenamento e a tramitação de documentos eletrônicos são controlados e padronizados pela TI, seguindo os prazos.
No que se referem documentos impressos, temos:

Grau de Sigilo	Forma de Armazenamento	Forma de Tramitação
Público	Sem requisitos específicos	Sem requisitos específicos
Restrito	Armazenamento em local seguro com acesso restrito.	Envelope lacrado, com identificação de informação confidencial e confirmação de recebimento
Sigiloso	Armazenamento em local seguro com controle de acesso.	Envelope duplamente lacrado transportado sob custódia.

10 – DESCARTE DA INFORMAÇÃO

Tão importante quanto à classificação e o cuidado no armazenamento e tramitação é o descarte de tal informação. No meio eletrônico, é feito automaticamente pela área de TI, de acordo com a política de descarte.
No meio impresso todo documento com informações relevantes deve ser destruídos antes de descartadas. Todo e qualquer descarte de documentação deve obrigatoriamente respeitar a tabela de temporalidade e destinação dos documentos e acordo com a legislação vigente.

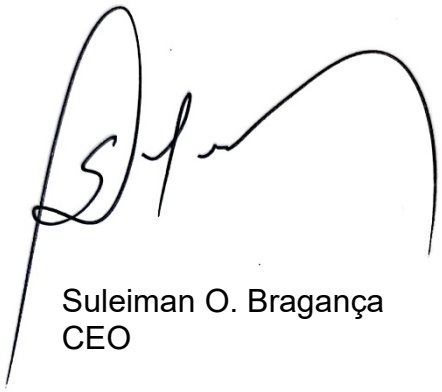
11 – RESPONSABILIDADES

É elaborada e revisada, anualmente, em conjunto a área de Segurança da Informação e o DPO, a qual considera os resultados dos testes das auditorias interna e externa e as normas vigentes, bem como as sugestões encaminhadas pelas demais áreas, e aprovada pela alta direção.

12 - VIGÊNCIA E INTRUMENTALIZAÇÃO

A presente política do tem vigência a partir de sua data de publicação e validade indeterminada, e ser decidido pela Diretoria e Alta Gestão, e posteriormente divulgado a todos os interessados.

Cuiabá – MT, 10 de novembro de 2022



Suleiman O. Bragança
CEO

ANEXO I - Alguns exemplos de dados e respectivas Classificação da Informação:

Informação	Dados
Pessoal	IP / Geolocalização, Nome, RG, CPF, Endereço Residencial / Comercial, Telefone, Conta Bancária, Dados de veículo, Contato, Endereço postal, E-mail, Detalhes de redes sociais; Fotografia, Prontuário de saúde, Renda, Cartão bancário, etc
Pessoal Sensível	Origem racial ou étnica, Convicção religiosa, Opinião política, Filiação a sindicato ou a organização de caráter religioso, filosófico ou político, Dado referente à saúde ou à vida sexual, Dado genético ou biométrico, Prevenção a Covid-19, Biometria para acesso às instalações ou ponto, etc.
Sigilosa	Informações Bancárias, Declarações Fiscais, Segredo de justiça, etc.