omnisblue

LGPD | COMPLIANCE

# POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

omnisblue

LGPD | COMPLIANCE

# Sumário

# 1. Histórico de revisão do documento

Abaixo são registrados as versões e atualizações deste documento.

| VERSÃO | DATA | AUTOR | ALTERAÇÕES |
|---|---|---|---|
| 1.0 | 03/03/2023 | Daniel Zaitz | Versão inicial do documento. |
| | | | |
| | | | |
| | | | |

# 2. Introdução

No cenário atual, onde a informação é um ativo valioso e, simultaneamente, suscetível a diversas ameaças, a necessidade de uma gestão eficaz e segura torna-se premente. A Política de Classificação de Informação surge como alicerce fundamental para a preservação da integridade, confidencialidade e disponibilidade dos dados que impulsionam a OmnisBlue.

Através desta política, estabelecemos um conjunto abrangente de diretrizes que visam categorizar e tratar a informação com a precisão necessária, considerando sua natureza e importância. Reconhecemos que a proteção de ativos críticos, o cumprimento de normativas legais e a promoção de uma cultura de segurança são imperativos inegociáveis.

Ao adotar esta política, almejamos não apenas cumprir regulamentações, mas também promover uma mentalidade organizacional voltada para a responsabilidade e o respeito pela sensibilidade dos dados que manuseamos. Esta política é, portanto, um compromisso com a excelência na gestão da informação, assegurando que nossa organização esteja segura e em conformidade.

Ao longo deste documento, exploraremos em detalhes os princípios subjacentes, as responsabilidades designadas e as práticas recomendadas que moldarão nossa abordagem à classificação de informações. Este é um passo significativo em direção a um

ambiente seguro, onde a confiança dos nossos colaboradores, clientes e parceiros é preservada e onde a informação é tratada com o rigor que merece.

## 3. Objetivo

O objetivo da Política de Classificação de Informação é estabelecer diretrizes e critérios para a classificação e proteção adequada das informações dentro da nossa organização. Essa política é parte integrante da gestão da segurança da informação e visa assegurar que as informações sejam tratadas de maneira apropriada, levando em consideração sua sensibilidade, valor e impacto para a organização.

A classificação de informações geralmente envolve atribuir diferentes níveis de confidencialidade, integridade e disponibilidade às informações com base em sua importância e na necessidade de proteção.

## 4. Determinações

A abrangência desta política estende-se por toda a organização, envolvendo diversos níveis e setores para garantir uma implementação eficaz. Alguns pontos chaves abordados incluem:

- Envolve a participação ativa da Diretoria Executiva para estabelecer uma cultura organizacional voltada à segurança da informação, definindo prioridades estratégicas e alocando recursos necessários.
- Inclui as áreas especializadas responsáveis por implementar medidas técnicas, físicas e de treinamento para garantir a segurança e conformidade com a política.
- Incorpora diretrizes específicas para garantir a conformidade com a LGPD, envolvendo áreas dedicadas à gestão de dados pessoais e à resposta a solicitações de titulares.
- Abrange todos os colaboradores, destacando a importância da conscientização e conformidade com as práticas de classificação de informação em suas atividades diárias.
- Pode estender-se à criação de comitês específicos, envolvendo representantes de diferentes áreas para promover uma abordagem colaborativa na gestão de informações sensíveis e nas tomadas de decisões estratégicas.
- Envolvimento em atividades contínuas de comunicação e treinamento para

garantir que todos os membros da organização compreendam a importância da classificação de informações e estejam alinhados com os objetivos organizacionais.

A abrangência dessa política é fundamental para criar uma cultura organizacional que valorize a segurança da informação em todos os níveis, promovendo uma gestão responsável e efetiva dos dados.

## 5. Categorias de Classificação

A classificação da informação, conforme definida pela ISO 27001, refere-se ao processo de atribuir rótulos ou categorias as informações com base em sua importância, sensibilidade e criticidade para a organização. Este processo visa garantir que os recursos de segurança sejam aplicados de forma proporcional à natureza específica de cada informação.

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. Dentre as classificações temos:

- Pública - Informações de natureza não sensível, que podem ser compartilhadas livremente com o público;
- Interna - Informações sensíveis, acessíveis apenas a funcionários autorizados da organização;
- Confidencial - Informações sensíveis que requerem um controle mais rigoroso de acesso;
- Restrito - Informações altamente críticas e restritas, exigindo controle de acesso máximo.

## 6. Processo de Classificação

A classificação da informação envolve atribuir níveis de sensibilidade ou categorias específicas a diferentes tipos de dados, com o objetivo de determinar como essas informações devem ser tratadas, protegidas e compartilhadas.

Para a realização da classificação da informação devem ser considerados quatro aspectos principais, que são:

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

- Identificação: Os gerentes e time estratégico deverão identificar os dados sob sua responsabilidade, classificando-os conforme a natureza e importância. Esse tipo de identificação pode incluir dados financeiros, informações de clientes, propriedade intelectual, entre outros.

- Critérios: Os dados serão categorizados de acordo com critérios claros que podem variar dependendo do valor estratégico da informação, seu impacto financeiro, a conformidade com regulamentações, entre outros fatores.

- Marcação: Os dados serão marcados de acordo com sua classificação e critério para fácil identificação. Métodos de marcação incluem etiquetas eletrônicas e metadados.

- Armazenamento: Dados serão armazenados em ambientes seguros, com base em suas classificações, utilizando práticas de segurança e medidas técnicas adequadas.

- Compartilhamento: O compartilhamento de dados será feito de acordo com as políticas de classificação, garantindo que apenas usuários autorizados tenham acesso

## 7. Acesso as Informações

- O acesso às informações será concedido apenas a pessoas autorizadas, com base em suas responsabilidades e necessidades de trabalho;
- Cada pessoa terá acesso apenas às informações necessárias para desempenhar suas funções;
- A política de "princípio do menor privilégio" será adotada, ou seja, os usuários terão o menor nível de acesso necessário para realizar suas tarefas;

- A equipe de TI e segurança implementará controles de acesso adequados para garantir que apenas usuários autorizados possam acessar informações sensíveis e classificadas;
- ·Serão utilizados métodos de autenticação robustos, como senhas fortes, autenticação de dois fatores e certificados digitais, conforme apropriado;
- ·Os acessos serão registrados e monitorados regularmente para identificar atividades suspeitas ou não autorizadas;
- ·Os usuários serão classificados com base em suas funções e responsabilidades, determinando o nível de acesso permitido;
- ·Uma revisão periódica das permissões de acesso será conduzida para garantir que estejam alinhadas com as mudanças nas responsabilidades dos funcionários.

## 8. Armazenamento e Tramitação

Esta seção da Política de Classificação de Dados estabelece as diretrizes para o armazenamento seguro e a tramitação adequada de informações classificadas. O objetivo é garantir a integridade, confidencialidade e disponibilidade dos dados durante todo o ciclo de vida.

- Os dados públicos podem ser armazenados em ambientes de acesso geral, como servidores públicos ou serviços de nuvem com configurações adequadas;
- Os dados internos serão armazenados em ambientes controlados e acessíveis apenas a funcionários autorizados;
- Dados confidenciais e restritos exigirão ambientes de armazenamento altamente seguros, com controles de acesso rigorosos e medidas adicionais de proteção;
- Todos os dados confidenciais e restritos armazenados ou transmitidos devem ser criptografados, utilizando algoritmos e protocolos de segurança aprovados;
- ·A equipe de TI será responsável por implementar e manter a infraestrutura de criptografia, bem como garantir a atualização constante para mitigar vulnerabilidades.

## 9. Papéis e responsabilidades

- Equipe de TI e segurança: Responsáveis por implementar as medidas de segurança, como criptografia e controle de acesso, de acordo com as categorias de dados classificados;
- ·Departamento de RH: Responsável por treinar funcionários sobre a política, monitorar conformidade e lidar com violações;
- ·Gerentes e time estratégico: Responsáveis por identificar dados críticos e designar a devida classificação.

## 10. Revisão da política

Esta política será revisada anualmente e ajustada conforme necessário para garantir sua eficácia contínua diante das mudanças nas regulamentações e nas operações da empresa.

omnisblue
LGPD | COMPLIANCE