

Norma de Classificação da Informação

Alsar Tecnologia em Redes

Classificação Pública

ÍNDICE

1.	<u>OBJETIVOS</u>	3
2.	<u>DOCUMENTOS DE REFERÊNCIA</u>	3
3.	<u>PAPÉIS E RESPONSABILIDADES</u>	3
4.	<u>DIRETRIZES GERAIS</u>	3

- **OBJETIVOS**

- Esta Norma tem por objetivo classificar a informação para que receba um nível de proteção, de acordo com a sua importância na empresa.

- **DOCUMENTOS DE REFERÊNCIA**

- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.
- Lei de Acesso a Informação (LAI) 12.527 de 18/11/2011.
- Política de Segurança da Informação – PSIC.

- **PAPÉIS E RESPONSABILIDADES**

- Responsáveis pela elaboração – **Dirigentes da Alsar**.
- Público Alvo – todos os dirigentes, colaboradores, parceiros e fornecedores.

- **DIRETRIZES GERAIS**

- Deverá ser realizada a classificação do ativo de informação em acordo com as diretrizes de segurança definidas pela organização.
- A informação deve possuir classificação quanto a sua confidencialidade, integridade e disponibilidade.
- Os níveis de controles de segurança estão diretamente associados ao grau de sigilo definido pelo Gestor da Informação.
- Todas as informações devem ser classificadas pelo Gestor da Informação no momento em que é gerada, registrada, recebida ou modificada.
- Informações que tiveram sua relevância ou potencial de impacto alterados devem ser reclassificadas pelo Gestor da Informação.
- Compete ao Gestor da Informação ou colaborador por ele designado formalmente, em revisões anuais ou quando julgar necessário, alterar ou cancelar a classificação atribuída às informações respeitando os interesses da **Alsar** e a legislação nacional vigente.
- A reclassificação e desclassificação de informação SIGILOSA deverá ser realizada por meio de formulário próprio de reclassificação ou desclassificação que contenha a devida motivação, além de ser submetido à autoridade máxima da **Alsar** para homologação ou procedimento de reclassificação.
- O processo de classificação é atribuído ao conteúdo da informação, área que se relaciona, responsabilidades e nível de exposição, portanto, não são considerados o formato, características, tipo, modelo ou nomenclatura do documento onde está inserida.

- A classificação da informação deve seguir a criticidade e sensibilidade (relevância), definida ao processo de negócio da **Alsar**, para implementação de procedimentos e controles necessários à sua proteção.
- Todas as informações de propriedade ou sob responsabilidade da **Alsar** devem ser classificadas e protegidas com controles compatíveis em todo o seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos em instrumento específico.
- É vedada a divulgação de qualquer informação de propriedade ou sob responsabilidade da **Alsar**, por seus dirigentes, colaboradores, parceiros e fornecedores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excluindo a hipótese de que a informação esteja previamente classificada como “pública”.
- A classificação da informação deve buscar, sempre que possível, o grau de segurança de acordo com sua confidencialidade, integridade e disponibilidade, visando otimizar/agilizar o processo de tratamento e reduzir os custos com sua proteção.
- Deve haver um procedimento definido, formal e divulgado para classificação, reclassificação e desclassificação da informação.
- Até que a classificação específica tenha sido definida e divulgada, as informações devem ser consideradas como restritas.
- Os ativos de informação (documentos digitais, físicos, sistemas) devem ter suas classificações rotuladas.
- As informações e quaisquer de seus procedimentos de tratamento devem ter um ciclo de vida estabelecido, durante o mesmo as informações deverão ser revisadas e/ou reclassificadas. Em caso de alterações será necessário ter sua formalização e aprovação por parte da **Alsar**.
- Devem ser realizados testes, monitoramentos e avaliações periódicas da efetividade em relação a classificação e seguimento do tratamento aos ativos.
- O acesso, a divulgação e o tratamento de informação classificada ficarão restritas apenas às pessoas de direito.
- As informações devem ser classificadas com sigilo:
- Pública: Informação que podem ser divulgadas para o público externo da **Alsar**, sem implicações de restrição e controle de acesso.
- Restrita: Informações associadas aos interesses estratégicos da **Alsar**, cujo conhecimento e uso estão limitados a determinado número de colaboradores. Sua revelação indevida é associada a impactos, graves, sob o aspecto financeiro, legal, normativo de reputação e de imagem.
- Confidencial: Informação submetida à restrição de acesso estabelecida em razão da legislação nacional vigente.
- As informações Confidenciais devem ser tratadas da seguinte forma:
- Entregas físicas e lógicas devem seguir controles que garantam sua confidencialidade e integridade ao destinatário final.

- As partes devem estar cientes do tramite do documento.
- Os documentos classificados como restrito ou confidencial devem ser mantidos e arquivados em condições especiais de segurança com controle de acesso e proteção dos dados.
- A **Alsar** respeita a privacidade dos titulares de dados e garante a confidencialidade, integridade e disponibilidade dos dados pessoais em todo o seu ciclo de vida, que vai desde a coleta, armazenamento, compartilhamento, até o descarte, em qualquer tipo de formato de armazenamento e suporte de acordo com a sensibilidade do dado pessoal, a finalidade e impacto dos riscos. Seguindo a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, para tanto, a **Alsar** deverá dispor de:
 - Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente.
 - Adoção de medidas de segurança para proteger os dados pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito.
 - Armazenamento de modo seguro, controlado e protegido.
 - Processos de anonimização e pseudonimização, sempre que necessário.
 - Protocolos de criptografia na transmissão e armazenamento, sempre que necessário;
 - Registro lógico de todas as operações de tratamento.
 - Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias.
 - Transferência a terceiros de modo seguro, contratualmente previsto e/ou autorizado pelo titular.
 - Avaliação de impacto e sistemática à privacidade dos titulares de dados.
 - Gestão e tratamento adequado de incidentes que envolvam dados pessoais.
 - Dados pessoais e os dados pessoais sensíveis devem ser armazenados separadamente.
 - Quando a informação pertencer a terceiros e a **Alsar** desempenhar o papel de custodiante, a classificação da informação e os requisitos e controles que serão aplicados para proteção da informação, devem ser informados pelo terceiro e formalizados em contrato.
 - Em casos de quebra de Segurança da Informação por meio de recursos de informática, o Canal de Atendimento (suporte@alsar.com.br) deve ser imediatamente acionado para adotar as providências necessárias.
 - Esta norma entra em vigor a partir da data de sua divulgação e sua revisão deve ocorrer em intervalos planejados, pelo menos anualmente, ou sempre que existirem alterações das regras acima expostas.
 - Dúvidas: Qualquer dúvida relativa a esta Norma deve ser encaminhada ao CSIC.

