

Norma de Classificação da Informação

NV7 Soluções Tecnológicas

Classificação Pública

ÍNDICE

1. OBJETIVOS.....	3
2. DOCUMENTOS DE REFERÊNCIA.....	3
3. PAPÉIS E RESPONSABILIDADES	3
4. DIRETRIZES GERAIS	3

1. OBJETIVOS

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

2. DOCUMENTOS DE REFERÊNCIA

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

3. PAPÉIS E RESPONSABILIDADES

- 3.1. Responsáveis pela elaboração – **Dirigentes da NV7.**
- 3.2. Público Alvo – todos os dirigentes, colaboradores, parceiros e fornecedores.

4. DIRETRIZES GERAIS

- 4.1. Deverá ser realizada a classificação do ativo de informação em acordo com as diretrizes de segurança definidas pela organização.
- 4.2. A informação deve possuir classificação quanto a sua confidencialidade, integridade e disponibilidade.
- 4.3. Os níveis de controles de segurança estão diretamente associados ao grau de sigilo definido pelo Gestor da Informação.
- 4.4. Todas as informações devem ser classificadas pelo Gestor da Informação no momento em que é gerada, registrada, recebida ou modificada.
- 4.5. Informações que tiveram sua relevância ou potencial de impacto alterados devem ser reclassificadas pelo Gestor da Informação.
 - 4.5.1. 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 **NV7** e a legislação nacional vigente.

- 4.5.2. 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 **NV7** para homologação ou procedimento de reclassificação.
- 4.6. 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.
- 4.7. A classificação da informação deve seguir a criticidade e sensibilidade (relevância), definida ao processo de negócio da **NV7**, para implementação de procedimentos e controles necessários à sua proteção.
- 4.8. Todas as informações de propriedade ou sob responsabilidade da **NV7** 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.
- 4.9. É vedada a divulgação de qualquer informação de propriedade ou sob responsabilidade da **NV7**, 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”.
- 4.10. 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.
- 4.11. Deve haver um procedimento definido, formal e divulgado para classificação, reclassificação e desclassificação da informação.
- 4.12. Até que a classificação específica tenha sido definida e divulgada, as informações devem ser consideradas como restritas.
- 4.13. Os ativos de informação (documentos digitais, físicos, sistemas) devem ter suas classificações rotuladas.
- 4.14. 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 **NV7**.
- 4.14.1. Devem ser realizados testes, monitoramentos e avaliações periódicas da efetividade em relação a classificação e seguimento do tratamento aos ativos.
- 4.15. O acesso, a divulgação e o tratamento de informação classificada ficarão restritas apenas às pessoas de direito.
- 4.16. As informações devem ser classificadas com sigilo:
- 4.16.1. Pública: Informação que podem ser divulgadas para o público externo da **NV7**, sem implicações de restrição e controle de acesso.
- 4.16.2. Restrita: Informações associadas aos interesses estratégicos da **NV7**, 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.

- 4.16.3. Confidencial: Informação submetida à restrição de acesso estabelecida em razão da legislação nacional vigente.
- 4.17.** As informações Confidenciais devem ser tratadas da seguinte forma:
- 4.17.1. Entregas físicas e lógicas devem seguir controles que garantam sua confidencialidade e integridade ao destinatário final.
- 4.17.2. As partes devem estar cientes do tramite do documento.
- 4.17.3. 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.
- 4.18.** A **NV7** 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 **NV7** deverá dispor de:
- 4.18.1. Tratamento autorizado nos termos da legislação de proteção de dados pessoais vigente.
- 4.18.2. 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.
- 4.18.3. Armazenamento de modo seguro, controlado e protegido.
- 4.18.4. Processos de anonimização e pseudonimização, sempre que necessário.
- 4.18.5. Protocolos de criptografia na transmissão e armazenamento, sempre que necessário;
- 4.18.6. Registro lógico de todas as operações de tratamento.
- 4.18.7. Descarte seguro dos dados pessoais ao término de sua finalidade e sua conservação de acordo com as hipóteses legais e regulatórias.
- 4.18.8. Transferência a terceiros de modo seguro, contratualmente previsto e/ou autorizado pelo titular.
- 4.18.9. Avaliação de impacto e sistemática à privacidade dos titulares de dados.
- 4.18.10. Gestão e tratamento adequado de incidentes que envolvam dados pessoais.
- 4.18.11. Dados pessoais e os dados pessoais sensíveis devem ser armazenados separadamente.
- 4.19.** Quando a informação pertencer a terceiros e a **NV7** 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.
- 4.20.** Em casos de quebra de Segurança da Informação por meio de recursos de informática, o Canal de Atendimento (suporte@nv7.com.br) deve ser imediatamente acionado para adotar as providências necessárias.
- 4.21.** 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.
- 4.22.** Dúvidas: Qualquer dúvida relativa a esta Norma deve ser encaminhada ao CSIC.