

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

1. Introdução

Buscando a segurança da informação as organizações buscam e investem constantemente em procedimentos dos mais diversos. Porém nem sempre esse gasto tem um retorno esperado, pois muita informação desimportante pode ser guardada de forma rígida. A classificação da informação é o procedimento em que diferenciam informações de uma instituição através de um conjunto de critérios, sendo eles: grau de confidencialidade, disponibilidade e integridade.

Esta classificação é importante, pois determina como cada informação será tratada e protegida, possibilitando um maior conhecimento das diversas informações recebidas, utilizadas, armazenadas e transmitidas.

2. Objetivo

Com a correta classificação das informações em termos de seu valor, requisitos legais, sensibilidade e criticidade se evita a modificação ou divulgação não autorizada, causando perdas e prejuízo algumas vezes irreversíveis para a instituição. Resultando em uma economia e melhor direcionamento dos seus recursos, conhecendo seu escopo, rotas e necessidades de informação com que se trabalha, permitindo o fluxo contínuo e necessário da informação e consequentemente o bom desenvolvimento dos trabalhos.

3. 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.
- Atividade finalística – conjunto de atividades que uma instituição realizada em suas atribuições específicas.
- Atividade meio – conjunto de atividades que auxiliam ou viabilizam a realização de atividades finalísticas da instituição.
- Documento – toda e qualquer informação produzida que seja registrada ou recebida.
- Formato – modo como foi confeccionado.
- Informação pessoal – toda e qualquer informação relacionada a indivíduo 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.
- Processo (documental) – conjunto de documentos reunidos em um uma ação administrativa ou judicial.
- Sistema informatizado – ferramenta utilizada para registro e gestão de documentos e processos.
- Suporte – material onde as informações são registradas.
- Termo de Classificação de Informação (TCI) – formulário que tem como finalidade formalizar a decisão de classificação ou qualquer alteração no sigilo de informação em qualquer grau de sigilo.

- Tipo de documento – 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.

4. Acesso à Informação

As informações produzidas, manuseadas e guardadas pelo Estado 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 em que se aplica a restrição de acesso à informação, os quais são apresentados a seguir.

4.1. Informações pessoais

São consideradas informações pessoais aquelas relacionadas à determinada pessoa (identificada ou identificável). Essas não são informações públicas e tem seu acesso restrito independentemente da classificação de sigilo atribuído a ela, pelo prazo máximo de 100 anos.

O acesso se restringe a agentes públicos autorizados e as pessoas as quais a informação se referir. O acesso de terceiros se dará apenas com previsão legal ou consentimento expresso das pessoas que são referenciadas.

4.2. Informações sigilosas protegidas por legislação específica

São informações protegidas por outras legislações, sigilo bancário, fiscal, comercial, profissional e segredo de justiça por exemplo. Essas informações, assim como nos pessoais, não necessitam receber o tratamento dado às informações classificadas em grau de sigilo.

4.3. Informações classificadas em grau de sigilo

Uma informação pública somente pode ser classificada como sigilosa quando considerada imprescindível à segurança da sociedade ou estado, de acordo com o que foi estabelecido como regra geral da LAI. Também é previsto a possibilidade de a informação ser sigilosa somente em parte, cabendo o acesso do interessado apenas à parte não sigilosa. No que tange a legislação vigente sobre o assunto, tanto o art. 23 da Lei nº 12.527, de 2011, tratam sobre as informações consideradas sigilosas e acesso a documentos preparatórios.

5.A Classificação

Toda classificação deve ser realizada no momento que a informação for gerada ou sempre que necessário em momento posterior. É importante destacar que toda informação classificada em grau de sigilo é sigilosa, mas nem toda informação sigilosa é classificada em grau de sigilo, o nivelamento da classificação se apresenta da seguinte maneira:

- Público - todo o conteúdo de todos os documentos de um determinado processo que são visualizados por qualquer pessoa, sendo servidor do HORTOPREV ou não.
- Restrito - o acesso ao conteúdo dos documentos em um processo é restrito às unidades, de menor hierarquia a qual a pessoa pertence, pelas quais esse processo tramitar, e, obviamente, à todas as pessoas que estiverem vinculadas àquelas unidades.

- Sigiloso - o acesso aos documentos e ao processo é exclusivo às pessoas a quem for atribuída permissão específica.

Vale ressaltar que o grau de sigilo do menor elemento se sobrepõe ao maior, ou seja, mesmo se o processo for classificado como público se houver algum documento classificado como restrito ou sigiloso, todo o processo passa a ter essa 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: 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).

São apresentados a seguir procedimentos em diferentes aspectos e práticas da implementação da classificação.

5.1. Identificação da classificação

Forma de identificação da classificação da informação em cada meio. Vale ressaltar que essa identificação será obrigatória apenas para as informações de níveis restrito e sigiloso.

Tipo de Documento	Procedimento
Papel	Para documentos gerados na instituição 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.
Documentos eletrônicos	A identificação já é padronizada pelo sistema utilizado .
Dados e aplicações	Deve conter o nível de segurança na “meta data” do documento. Para qualquer relatório gerado a identificação deverá ser descrita no cabeçalho.
Outros tipos	A classificação deverá estar visível no início do documento.

Armazenamento e Tramitação

O armazenamento e tramitação de documentos eletrônicos são controlados e padronizados, não havendo necessidade de definições ou controles. Porém 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.

Descarte da informação

Tão importante quanto à classificação e o cuidado no armazenamento e tramitação é o descarte de tal informação. Em se tratando de documentos em meio impresso todo documento com informações relevantes deve ser destruído antes de descartadas, podendo ser utilizado picotadores de papel.

Todo e qualquer descarte de documentação deve obrigatoriamente respeitar a tabela de temporalidade e destinação dos documentos definidos em legislação e aplicáveis ao HORTOPREV.

Responsabilidade

De acordo com a LAI, os maiores níveis hierárquicos das autoridades têm prerrogativa de utilizar o mais alto grau de sigilo. A pessoa mais indicada para a definição do nível de segurança da informação é o responsável pelo setor que produz tal informação. Por se mostrar como o conhecedor do que é produzido e recebido assim como as respectivas necessidades de confidencialidade, integridade e disponibilidade.

É recomendada a verificação por autoridades de instâncias superiores daquela que classificou a informação. A manutenção dos níveis de segurança é de responsabilidades de todos aqueles que manipularem tal informação.