POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

INTRODUÇÃO

Com o advento da Lei Geral de Proteção de Dados – 13.709/18, as informações são consideradas patrimônios, e em razão disso devem ser protegidas adequadamente. Por isso faz-se necessário que a informação seja classificada de acordo com sua relevância correspondentes ao seu ciclo de vida.

DA ABRANGÊNCIA

Esta política aplica-se a todos os servidores e/ou usuários que direta e indiretamente utilizam os sistemas e informações deste órgão.

DA DEFINIÇÃO

A classificação das informações consiste na definição de níveis de proteção que cada dado deve receber. Alguns documentos devem receber uma proteção relevante, tendo em vista o tipo de dado que cada um contém.

O principal objetivo dessa prática é mitigar riscos de vazamentos de dados ou o chamado acesso inadequado, criando uma série de proteções extras para informações mais sensíveis, levando em consideração sua classificação.

A classificação deve seguir a criticidade e sensibilidade aderente ao redirecionamento estratégico, para implementação de procedimentos e controles necessários à sua proteção.

Todas as informações de propriedade ou sob responsabilidade deste órgão devem ser classificadas e protegidas com controles compatíveis em todo seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos, conforme parametrizado em normativo específico.

DAS FUNÇÕES E RESPONSABILIDADES

Cada individuo será responsável pelos deveres associados a cada função. A pessoa responsável pelos dados e pela informação sendo coletada e mantida pelo seu departamento ou divisão, normalmente, uma equipe de gerenciamento.

Para isso, há uma divisão para melhor visualização e andamento:

Revisão e categorização: revisar e categorizar dados e informações coletadas pelo próprio departamento e divisão;

Atribuição de rótulos a classificação de dados: atribua e rotule os dados classificados com base no potencial nível de impacto deles;

Compilação de dados: assegurar que os dados compilados de diversas origens estejam classificados com o nível de classificação mais seguro entre os dados classificados individualmente;

Coordenação da classificação de dados: garanta que os dados que são compartilhados entre os departamentos estejam protegidos e classificados constantemente;

***Compliance* da classificação de dados:** garanta que a informação com nível de impacto alto ou moderado estejam seguros de acordo com as leis e orientações federais e estaduais;

Acesso aos dados: desenvolver orientações do acesso aos dados para cada rótulo da classificação de dados;

Guardião dos dados: departamento da tecnologia da informação são responsáveis por manter e realizar backups nos sistemas, banco de dados e servidores que armazenam dados da empresa. É responsável também pela implementação técnica das regras impostas pelos donos dos dados, garantindo que essas regras sejam aplicadas ao sistema e que funcione;

Usuários dos dados: pessoa física ou jurídica que interage, acesse, use e atualize os dados com o propósito de realizar uma tarefa permitida por quem é proprietário dos dados. Os usuários dos dados devem utilizá-los de forma consistente a que foi definida e estar ciente de todas as políticas aplicadas ao uso dos dados.

DO PROCEDIMENTO DA CLASSIFICAÇÃO

A classificação deve buscar ser compatível com o grau de segurança da informação, de acordo com sua confidencialidade, integridade e disponibilidade, visando otimizar o processo de tratamento e reduzir os custos com sua proteção.

Os ativos de informação (documentos digitais, físicos, sistemas) devem ter suas classificações definidas, conforme as seguintes categorias de sigilo:

I – ultrassecreto: quando direcionada a um grupo extremamente limitado e identificado. A divulgação deste conteúdo pode permitir acesso a informações estratégicas e colocar em risco os agentes ligados a isso, além de causar prejuízos;

II – secreto: quando pode ser acessada apenas por um grupo restrito de pessoas. Sua divulgação não autorizada pode implicar prejuízos e/ou prejudicar sua imagem;

III – reservado: o dado quando tramitado e seu conteúdo pode comprometer a integridade física ou financeira;

IV – interna: o dado quando tramitado é trafegado em diferentes órgãos e apesar de não estar claramente classificado, sua divulgação prejudicaria interesses internos e a atuação de agentes públicos poderia se beneficiar aquele que a detiver;

V – pública: quando o uso do dado é livre e seu conteúdo pode ser publicado sem comprometer os agentes envolvidos.

A classificação em grau de sigilo deve ser realizada quando a informação for gerada ou, posteriormente, quando necessária. O documento pode ser considerado como classificável quando de um pedido de informação nele contido, no todo ou em parte.

O proprietário dos dados deve atribuir um rótulo a cada parte dos dados a serem classificados com base no nível de impacto geral:

IMPACTO GERAL	RÓTULO DE CLASSIFICAÇÃO
Alto	Restrito
Moderado	Confidencial
Baixo	Público