2023

Política de Classificação da **Informação**

Avenida Tamboré 350, Barueri, São Paulo, 06460-000
+55 (11) 4688-4001 | info@abaigroup.com.br

1. POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

CONTROLE DE REVISÃO

Revisão	Data	Histórico de Alterações	Resp. pela Elaboração	Resp. pela Aprovação
00	07/11/2023	Edição para divulgação PÚBLICA no site ABAI de acordo com layout definido por Marketing Espanha	INFOSEC	CISO

1. INTRODUÇÃO

A classificação das informações consiste na definição de níveis de proteção que cada documento deve receber.

Por exemplo, alguns templates da empresa devem ter um nível de proteção como “Interno” que são templates com informações de projeto ou profissional que não devem ser enviados ao Cliente.

2. OBJETIVOS

Este documento serve para garantir que nenhum dado seja divulgado indevidamente e que apenas os interessados recebam acesso à informação. A classificação da informação faz parte das exigências da ISO 27001.

3. APLICAÇÃO

Este documento é aplicado a todo o escopo do Sistema de Gestão de Segurança da Informação, ou seja, a todos os tipos de informações (incluindo dados pessoais), independentemente do formulário/documentos em papel ou eletrônicos, aplicativos e bancos de dados, conhecimento das pessoas etc.

4. REFERÊNCIAS

- NBR ISO/IEC 27001, na versão vigente.

5. RESPONSABILIDADES

Etapas e responsabilidades para o gerenciamento de informações são as seguintes:

Passo	*Responsável*
1. Classificação de informações	Gestor de TI / Gestor SI (Com auxílio do Gestor/Coordenador e/ou Responsável do Processo)
2. Rotulagem de informações	Gestor de TI / Gestor SI (Com auxílio do Gestor/Coordenador e/ou Responsável do Processo)
3. Tratamento de informações	Gestor de TI / Gestor SI (Com auxílio do Gestor/Coordenador e/ou Responsável do Processo)

5.1 Critérios de Classificação

O nível de confidencialidade é determinado com base nos seguintes critérios:

- Valor das informações / DP – com base em impactos avaliados durante avaliação de risco;
- Sensibilidade e criticidade das informações / DP – com base no maior risco calculado para cada item de informação durante avaliação de risco;

- Obrigações legais e contratuais – com base na Lista de Obrigações Legais, Regulatórias e Contratuais e Outras.

6. PROCEDIMENTO

Essa política determina as classificações dos documentos da ABAI, conforme abaixo que será tratada como confidencial, interna ou pública.

- **Confidencial**

É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente (informações de cliente), têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa.

Documento Confidencial

- **Interna**

Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

Documento Interno

- **Restrita**

São informações de caráter restrito e confidenciais, direcionadas exclusivamente a um grupo de colaboradores ou área de trabalho específica, com acesso limitado por questões de segurança e confidencialidade.

Documento Restrito

- **Pública**

São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

Documento Público

6.1 Níveis de Confidencialidade

Todas as informações devem ser classificadas em níveis de confidencialidade, sendo classificadas como “Uso Interno” por padrão. Caso a informação não for de “Uso Interno”, deve-se analisar criticamente os critérios de classificação e determinar a rotulagem da mesma, com exceção a documentos recebidos e/ou enviados às partes interessadas que possuem layout específico (ex: bancos), conforme abaixo:

Nível de	*Rotulagem*	*Critérios de classificação*	*Restrição de acesso*

Confidencialidade			
Público	(Sem rótulo)	Tornar a informação pública não pode prejudicar a organização de forma alguma. *Exemplos: serviços ofertados, notícias, marketing disponíveis nos websites, newsletter, redes sociais, Política de Privacidade e outros meios.*	As informações estão disponíveis ao público
Uso interno	(Sem rótulo) ou INTERNO	O acesso não autorizado às informações pode causar danos leves e/ou inconvenientes à organização. Exemplos: informações/dados pessoais, documentos (procedimentos, manuais) e registros (formulários) necessários à execução das atividades contratuais (escopo do SGSI), tanto internas quanto externas (clientes / fornecedores).	As informações estão disponíveis para todos os funcionários, terceiros e clientes (ambos, quando necessário/solicitado).
Confidencial	CONFIDENCIAL	O acesso não autorizado à informação pode causar danos consideráveis / catastróficos (irreparáveis) aos negócios e/ou à reputação da organização. Exemplos: informações sobre compra e venda de empresas do grupo, informações estratégicas e privilegiadas que possam comprometer a ABAI no mercado (clientes, funcionários e fornecedores).	As informações estão disponíveis apenas para pessoas específicas da organização (gestores, diretores, alta gestão, ou pessoas autorizadas).
Restrito	RESTRITO	O acesso não autorizado às informações pode causar danos leves e/ou inconvenientes à organização. Exemplos: informações/dados pessoais, documentos (procedimentos, manuais) e registros (formulários) necessários à execução das atividades contratuais (escopo do SGSI), tanto internas quanto externas (clientes / fornecedores).	As informações estão disponíveis apenas para pessoas específicas da organização (gestores, diretores, alta gestão, ou pessoas autorizadas).

A regra básica é usar o nível de confidencialidade mais baixo garantindo um nível adequado de proteção, a fim de evitar custos desnecessários de proteção.

6.2 Pessoas Autorizadas

Todas as informações classificadas como "Restritas" são tramitadas pelos funcionários ABAI, clientes com contratos ativos, subcontratadas ativas de clientes ativos, fornecedores da ABAI com contrato ativo e com os titulares de dados.

As informações classificadas como “Confidenciais" devem ser utilizadas junto à Direção, Financeiro, Comercial e Recursos Humanos (em casos de Dados Pessoais).

Os proprietários de ativos devem rever o nível de confidencialidade de seus ativos de informação a cada dois anos e avaliar se o nível de confidencialidade pode ser alterado. Se possível, o nível de confidencialidade deve ser reduzido.

6.3 Rotulagem

Toda informação com classificação diferente de “Pública”, deverá ser rotulada quanto ao seu grau de sigilo (interna, confidencial), por qualquer pessoa que tenha acessos às informações da ABAI.

A rotulagem deverá ser identificada no documento, como uma tarja, de forma acessível e legível, conforme item anterior:

Os níveis de confidencialidade são rotulados da seguinte forma:

Meio	*Uso interno*	*Confidencial e/ou Restrito**
Documentos em papel / impressos (incluindo DP)	Não é necessário rotular.	O nível de confidencialidade é indicado no envelope / pasta que carrega / transporta tal documento. Caso seja gerado dentro da organização deve apresentar a classificação em todas as páginas, na capa é opcional, exceto apresentação que é somente na capa. Caso venha de fora, o mesmo não é classificado.
Documentos eletrônicos (incluindo DP)	Não é necessário rotular.	O nível de confidencialidade é garantido pela restrição de acesso conforme as políticas de acesso às pastas e sistemas, sendo seu acesso autorizado apenas às pessoas autorizadas (vide item 4.4).
Sistemas de informação / Bancos de Dados e Aplicações (incluindo DP)	Não é necessário rotular.	O nível de confidencialidade em aplicativos e bancos de dados é garantido pela restrição de acesso conforme as políticas de acesso aos sistemas. Não aplicável, visto que somente determinada equipe e/ou área tem autorização de acesso a essas informações.
Correio eletrônico (incluindo DP)	Não é necessário rotular.	O nível de confidencialidade é indicado na assinatura do e-mail. Deve apresentar “disclaimer” ao final da mensagem.
Mídia eletrônica de armazenamento (incluindo DP)	Não é necessário rotular.	O nível de confidencialidade deve ser indicado na superfície de tal meio.
Informações transmitidas oralmente (incluindo DP)	Não é necessário rotular.	O nível de confidencialidade das informações confidenciais a serem transmitidas na comunicação presencial, por telefone ou algum outro meio de comunicação, deve ser comunicado antes das informações em si.

Para as informações constantes em sistemas, como não é possível a implementação de rótulo diretamente nelas, os acessos a esses sistemas são restritos a profissionais autorizados conforme controle de acessos.

6.4 Tratamento de Informações

Todas as pessoas que acessam informações confidenciais devem seguir as regras listadas na tabela a seguir.
Todos os colaboradores devem observar a rotulagem do documento, de forma a tratar a informação conforme tabela abaixo, preservando a confidencialidade, integridade e disponibilidade da informação.

As informações classificadas e rotuladas deverão seguir as seguintes recomendações em relação ao uso e tratamento:

----------	Pública	Interna (somente ABAI)	Restrita (áreas especificas da ABAI)	Confidencial (ABAI e Cliente)
Acesso à Informação	Poderá ser acessada por qualquer pessoa.	Poderá ser acessada por qualquer colaborador.	Poderá ser acessada por qualquer colaborador.	Poderá ser acessada por qualquer colaborador ou cliente.
Cópias	Poderá ser copiada sem restrições	Poderá ser copiada para fins de conhecimento interno.	Poderá ser copiada para fins de conhecimento interno de uma determinada equipe ou área.	Poderá ser copiada para fins de conhecimento interno, desde que seja assunto referente ao cliente.
Correio Eletrônico (E-mail)	Sem Restrições	Se a origem e destinatário for um endereço interno: Sem restrições. Se o destinatário for um endereço externo: Com o disclaimer no final do e-mail e preferencialmente enviar com o arquivo zipado.	Se a origem e destinatário for um endereço interno: Sem restrições. Se o destinatário for um endereço externo: Com o disclaimer no final do e-mail e preferencialmente enviar com o arquivo zipado.	Se a origem e destinatário for um endereço interno: Sem restrições. Se o destinatário for um endereço externo: Com o disclaimer no final do e-mail e preferencialmente enviar com o arquivo zipado.
Guarda Física	Sem procedimento específico	Deve ser mantida em local seguro* quando não estiver sendo utilizada.	Deve ser mantida em local seguro* quando não estiver sendo utilizada.	Deve ser mantida em local seguro* quando não estiver sendo utilizada.
Destruição	Sem procedimento específico	Destruir de acordo com o procedimento interno, de modo a assegurar a eliminação completa da informação.	Destruir de acordo com o procedimento interno, de modo a assegurar a eliminação completa da informação.	Destruir de acordo com o procedimento interno, de modo a assegurar a eliminação completa da informação.

* ***Local Seguro*****:** áreas restritas (com armários com controle por chave ou salas com controle de acesso) como por exemplo: financeiro, RH, diretoria, datacenter.

6.5 Comunicação de Irregularidades

Em caso de identificação de qualquer irregularidade em relação a esta política, comunicar a área de SI pelo e-mail info@abaigroup.com.br, que deverá avaliar se tal irregularidade caracteriza um incidente de segurança da informação ou violação da proteção de dados pessoais e tomará as medidas necessárias de acordo com o procedimento Gestão de Incidentes de Segurança da Informação.

6.6 Transferência da Informação

Além da classificação da informação e seus rótulos, o prazo de armazenamento e transferências deverá seguir o novo Código Civil, em seu artigo 206 e parágrafos no que se refere à guarda de documentos.

Os documentos devem ser guardados microfilmados, digitalizados ou pela tradicional e adequada guarda física dos originais.

- Comprovante de aluguel - 3 anos
- Água, luz e telefone - 5 anos
- Carnês do ISS - Até o pedido do benefício
- Condomínio - 5 anos
- Declaração de IR, IPTU e IPVA - 5 anos
- Prestações da casa - 5 anos
- Notas fiscais / Garantia ou vida útil do produto e Contratos de seguro - 1 ano
- Consórcios- Até a quitação
- Plano se saúde - 5 anos
- Folha de pagamento - 5 anos
- Notas de serviços de profissionais liberais - 5 anos
- Cobrança do FGTS e demais encargos vinculados à previdência social, que deverão ser guardados pelo prazo de contribuição do segurado (35 anos se homem e 30 anos se mulher)
- A documentação das sociedades empresárias (Cofins, CSLL e Pis) - 10 anos.

CLASSIFICAÇÃO DA INFORMAÇÃO				
Descrição	Pública	Interna	Confidencial e/ou Restrito	
Envio e Armazenamento				
Correio Eletrônico	Sem restrições.	Interno: enviar em texto claro, via sistema de correio eletrônico interno. Externo: Criptografado.	Interno: Criptografado. Externo: Criptografado.	Interno: Criptografado. Externo: Criptografado.

				Adicional: Bloqueio de encaminhamento.
Correspondência Interna (cópia em papel)	Sem restrições.	Pasta fechada entregue pessoalmente em mãos ao destinatário.		Não utilizar o sistema de correspondência interna.
Correspondência Externa / Courier	Sem restrições.	Controle de envio (remetente e destinatário), envelope de segurança com lacre (tipo adesivo).		
Transmissão Eletrônica dentro da empresa	Sem restrições.	Sem restrições.	A informação deve ser transmitida através de canal criptografado ou criptografar a mesma antes da transmissão.	
Transmissão Eletrônica fora da empresa	Sem restrições.	Proteção de arquivo com senha, monitoramento de tráfego de dados.	A informação deve ser transmitida através de canal criptografado ou criptografar a mesma antes da transmissão.	
Transportar / Conduzir dentro do País	Sem restrições.	Transportar em recipiente fechado.	Papel: Transportar em recipiente fechado e nunca deixar desacompanhado. Mídia: Criptografar.	
Transportar ou Transmitir informação para fora do País	Sem restrições.	Assegurar conformidade com as legislações brasileiras e legislações e regulamentos locais de exportação e privacidade de dados.	Assegurar conformidade com a legislação brasileira e legislações e regulamentos locais de exportação e privacidade de dados. Legislação brasileira: Papel: Transportar em recipiente fechado e nunca deixar desacompanhado. Mídia: Criptografar	
Copiar, Imprimir ou Transmitir por Fax	Sem restrições.	Permitido, de acordo com as necessidades de negócio da empresa.	Cópias e Impressão: Com a permissão do Gestor ou Custodiante da Informação. Fax: transmissão com verificação de recebimento.	Cópias e Impressão: necessária aprovação do Gestor ou Custodiante da Informação e inclusão da marca d'água "Cópia controlada". Fax: Não é permitido o envio.
Armazenamento	Sem restrições.		Papel: Local protegido com chave/cartão de acesso, registro de acesso aos documentos. Eletrônica: A criptografia não é necessária para a informação eletrônica em servidores protegidos em locais protegidos, com controle de acesso apropriado, mas quando mídias forem enviadas para locais externos, devem ser criptografadas.	
Destruição e Descarte – Atentar para o período de retenção de registros e conformidade legal. Descartar somente após expirar os períodos de retenção, exceto se houver justificativa legal para manter a informação.				

Cópia em papel	Sem restrições.	Métodos internos de descarte.	Deve ser fragmentado ou armazenado em recipiente trancado para fragmentação posterior.
Eletrônico	Sem restrições.		Destruição física ou processo magnético de limpeza.

7 VIOLAÇÕES DA POLÍTICA E PENALIDADES

O não cumprimento desta Política de Classificação implica em falta grave e poderá resultar em medidas disciplinares cabíveis, tais como, advertência, suspensão ou desligamento, a qualquer colaborador que violar esta política, o Código de Ética e Conduta, demais políticas da empresa e leis e regulamentos aplicáveis, de âmbito nacional ou internacional.

8 ANEXOS

Este documento não contém anexos.