POLÍTICA INTERNA DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO ASSOCIAÇÃO BRASILEIRA DE CAFÉS ESPECIAIS – BSCA

Por ocasião da Lei nº 13.709/2018 – Lei Geral do Proteção de Dados (LGPD) – e pelo valor empresarial do Sigilo, a BSCA, por meio de seu Comitê Especial de Planejamento e Implantação da LGPD, insNtui a presente PolíNca Interna de Proteção de Dados e Segurança da Informação, a qual deverá ser rigidamente seguida por todos aqueles que possuem relações internas com a empresa, quais sejam sócios, estagiários, prestadores de serviços conUnuos, funcionários, parceiros e quaisquer outros que tenham acesso a informações por ocasião do trabalho desempenhado.

NOTA INTRODUTÓRIA

Qualquer documento, dado ou informação deverá receber tratamento conforme diretrizes desta PolíNca, sendo o órgão mencionado acima, habilitado para quaisquer esclarecimentos necessários. Eventuais situações não contempladas serão analisadas e deliberadas em conjunto com os diretores.

A adoção de políNcas, normas e procedimentos que visem garanNr a segurança da informação deve ser uma das prioridades do *compliance* e governança corporaNva, permeando todas as aNvidades e reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que podem gerar atos contrários à disposição legal e consequências graves e indesejadas.

CAPÍTULO I Classificação de Dados, Informações e Documentos

Todas as informações que circulam internamente na empresa devem ser tratadas em caráter sigiloso, não podendo ser disponibilizadas ao público externo, a exceção daquelas que tenham objeNvo de alcançar este público. Para tanto, as classificações abaixo servirão de parâmetro para nortear a equipe quanto ao nível de segurança a ser aplicado ao sigilo da informação.

1) Pública

São informações previamente classificadas pela empresa como de interesse do público externo e por essa razão estão expostas nos meios de comunicação e facilmente acessíveis.

Exemplos: missão; visão; valores; processos seleNvos em andamento; campanhas voltadas ao público externo (sociais, educaNvas etc.); localização; horário de funcionamento.

2) Interna

São informações básicas disponíveis a toda equipe, não sendo, portanto, desNnadas ao uso e conhecimento do público externo. Exemplos: diretrizes, políNcas e procedimentos internos, circulares, e-mails e lista de contatos; avisos, informações de processos (desde que não estejam em segredo de jusNça).

3) Confidencial

São informações de acesso restrito a um membro ou membros da equipe. Sua revelação pode violar a privacidade de indivíduos, acordos de confidencialidade, dentre outros. Exemplos de informações confidenciais: qualquer informação relacionada ao cliente; fluxos operacionais desNnados a aNvidades específicas; informações pessoais de qualquer integrante da equipe; plano de carreira, informações de processos em segredo de jusNça.

4) Confidencial Restrita

São informações de acesso restrito a um membro ou membros da equipe que estejam associadas ao interesse estratégico da empresa ou ao interesse do cliente, podendo seu vazamento, ainda que internamente, provocar danos à empresa ou ao cliente.
Exemplos: atas de reuniões gerenciais; informações financeiras da empresa; acordos e/ou negociações em andamento ou firmados pelo cliente a depender a complexidade; informações referentes a planejamentos; projeção futura de negócios da empresa.

- Na estação de trabalho não deverão ser deixadas informações em meio hsico que contenha informação confidencial e/ou confidencial restrita.
- Deverá ser aproveitado como rascunho apenas impressos que contenham informação pública e/ou interna. Impressos que contenha informação confidencial e/ou confidencial restrita deverão ser devidamente descartados seguindo esta polínca.

CAPÍTULO II Uso de Equipamentos, Senhas e Chaves

- Todos os notebooks e/ou equipamentos eletrônicos uNlizados no desempenho das aNvidades da empresa deverão ter senha cadastrada para acesso. A senha de acesso ao equipamento eletrônico jamais deverá ser fornecida a outros, a exceção de casos extremamente necessários. Ao deixar a estação de trabalho, o membro da equipe deverá obrigatoriamente bloquear seu equipamento, jamais deixando o mesmo em livre acesso.
- Senhas de alarme são de uso individual, não devendo ser fornecidas a terceiros, nem entre membros da empresa.

- As chaves de acesso jamais deverão ser fornecidas a terceiros. As que são de uso comum deverão sempre ser armazenadas em local adequado para acesso dos membros, mas em segurança à acesso de terceiros.
- De igual forma não deverão ser fornecidas a terceiros senhas de e-mail corporaNvo, servidor, sistema de assinatura digital, sistema de gestão de processos e serviços, cerNficado digital, autarquias e qualquer outra vinculado direta ou indiretamente ao exercício das aNvidades internas.

CAPÍTULO III Uso do Servidor Digital

No servidor digital ficarão armazenados todos os arquivos digitais concernentes a empresa e aos clientes, com idenNficação de pastas gerais.

- Novas pastas gerais não poderão ser criadas pelos usuários, sendo ato exclusivo da administração, mas admiNdas sugestões. A organização dos documentos nos diretórios é de responsabilidade dos usuários;

CAPÍTULO IV Arquivo Físico

- O arquivo hsico será manNdo para armazenamento de documentos novos e anNgos.
- Sempre que possível deverá ser dada preferência para documentos digitais, visando reduzir o consumo de papel, bem como oNmizar o espaço desNnado para arquivamento de documentos hsicos.
- Arquivos que não necessitarem de devolução ao cliente deverão ser descartados conforme indicado nesta políNca.
- Deverá ser observada a caixa de arquivo específica em que já tenha arquivos relacionados ao cliente e/ou tema do documento a ser armazenado, evitando duplicidade. Em caso de não haver caixa, deverá ser solicitado ao apoio administraNvo o fornecimento e a devida idenNficação.
- Com relação ao tempo de arquivamento deverá ser observado o que dispõe esta políNca.
- O descarte de documentos hsicos deverá ser feito por meio da destruição, garanNndo assim que não possa haver vazamento de dados constantes no documento após o descarte.

CAPÍTULO V
Uso de AplicaSvos de Mensagens Instantâneas e Servidores Independentes

O uso de aplicaNvos de mensagens instantâneas (Whatsapp, Telegram, outros) e e-mail para comunicação entre membros e clientes para trataNvas de assuntos profissionais será admiNdo devendo seguir as seguintes premissas.

Os membros deverão sempre pautar pela uNlização do aplicaNvo recomendado pela empresa para que haja unicidade e centralização.

- Aqueles que possuem linha corporaNva deverão priorizar seu uso para questões profissionais.
- Todos devem sempre evitar trataNvas inbox com clientes direcionando o conteúdo para o grupo específico do cliente. Conteúdo manNdo inbox poderão ocasionar responsabilização do usuário.
- As trataNvas por e-mail, buscar sempre manter o histórico, sem criar um e-mail novo para resposta de assunto que já está em andamento, mas sim dando seguimento neste.
- Manter nas trataNvas apenas às partes interessadas.

O armazenamento de informações em nuvem (One Pass, Google Drive, iCloud, entre outros) poderá ser uNlizado.

- Quando do uso deste Npo de armazenamento deverá ser feito preferencialmente em conta vinculada à empresa e não ao usuário.
- Esse meio deverá ser uNlizado em situações idenNficadas como necessárias, não devendo ser a regra e uNlização com frequência.

CAPÍTULO VI Proibições

Não será permiNdo aos usuários armazenar:

I) qualquer informação, dado ou material que viole qualquer lei federal, estadual ou municipal;
II) quaisquer materiais com direitos reservados, de propriedade intelectual ou com copyright, incluindo MP3, MPEG, ROM ou emuladores ROM, vídeos, distribuição ou divulgação de senhas para acesso de programas alheios, difamação de pessoas ou negócios, alegações consideradas perigosas ou obscenas, protegido por segredo de estado ou outro estatuto legal;
III) qualquer informação instruNva sobre aNvidades ilegais, que promovam ou induzam dano hsico ou moral contra qualquer grupo ou indivíduo;
IV) qualquer material que explore de alguma forma, crianças ou adolescentes e menores;
V) qualquer material de cunho racista, neonazista, anNssemita ou qualquer outro que venha a atentar contra a integridade moral de terceiros ou grupos da sociedade;
VI) qualquer material relacionado a hacking/cracking, incluindo links para sites com conteúdo desse Npo;
VII) qualquer material de cunho eróNco ou pornográfico, mesmo que seja na sua pasta pessoal;
VIII) arquivos parNculares no servidor;
IX) arquivos da empresa e/ou clientes em equipamento parNcular;

X) soqwares, ainda que estejam entre aqueles usados na insNtuição. Todos os soqwares insNtucionais e seus respecNvos instaladores armazenados no servidor de arquivos serão manNdos pelos responsáveis;

XI) dados considerados sensíveis, a menos que estritamente necessário para conNnuidade dos serviços.

CAPÍTULO VII Visitantes

Visitantes serão sempre bem-vindos, no entanto, com o objeNvo de proporcionar um ambiente de trabalho seguro e agradável a todos os indivíduos que estejam na empresa, além de monitorar e registrar os acessos às suas instalações, todos devem cumprir as seguintes orientações:

- Deverão sempre ser idenNficados.
- Nunca deverão ser deixados sozinhos, apenas por curto período no ambiente da recepção.
- Preferencialmente, as visitas deverão ser programadas para que o(s) visitante(s) esteja(m) sendo aguardado(s).
- Poderão ser agendadas visitas com parceiros e/ou visitas guiadas de acadêmicos por moNvos insNtucionais, no entanto, nesse caso, deverá haver comunicação prévia.
- Os visitantes eventualmente poderão conhecer os departamentos, desde que estejam acompanhados.
- Deve-se tomar muito cuidado para que o visitante não tenha acesso a qualquer informação da empresa e/ou clientes.
- A visita deverá ser programada para que tenha duração razoável ao fim que se desNna.
- Deve-se evitar conversas e/ou apresentações longas nos ambientes de trabalho, afim de que o visitante acabe por ouvir questões ligadas ao desempenho das aNvidades da equipe.
- Poderão ocorrer visitas ocasionais de familiares e amigos com moNvação justa, sendo de responsabilidade daquele que estará recebendo os visitantes o acesso e permanência.
- Membros da equipe que façam pedidos parNculares de entrega na empresa tais como almoço, remédios, documentos etc. deverão ficar atentos ao acesso e permanência do entregador nas dependências da empresa, sendo de sua responsabilidade verificar que este tenha deixado as dependências da empresa após realizada a entrega.

CAPÍTULO VIII Retenção e Descarte de Dados

Para cada um dos propósitos, a tabela a seguir mostra o período máximo de retenção de Dados Pessoais pela empresa, por categoria de registro, descrição, bem como o formato de descarte.

Tipo de Registro	Descrição	Período de Retenção	Formato de Descarte
Negócios	Contato Comercial / Prestação de Serviços (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail)	1 (um) ano após contato inicial sem resposta, ou prontamente, no caso de revogação do consenNmento ou da manifestação de desinteresse em ser contatado.	Eliminação pela empresa, *opt-out*, ou a qualquer tempo pelo Ntular.
Negócios	Contratos Gerais (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail; conta bancária; dados de cobrança)	3 (três) anos após o término do contrato.	Eliminação pela empresa.
Negócios	Documentos Tributários	5 (cinco) anos a contar da data de emissão do documento.	Eliminação pela empresa.
Negócios	Proteção do Crédito (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail)	Durante relação comercial ou prontamente, em caso de exaurimento da finalidade.	Eliminação pela empresa.
Negócios	Prontuários e informações médicas (paciente)	20 (vinte) anos a contar da data de emissão do documento.	Eliminação pela empresa.

MarkeNng e Comunicação	Campanhas Publicitárias, Ações Promocionais e Pesquisas (nome, RG, CPF, endereço, país de origem, e-mail, telefone, respostas a pesquisas	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou revogação do consenNmento.	Eliminação pela empresa, ou *opt-out* a qualquer tempo pelo Ntular.

MarkeNng e Comunicação	Site e Redes Sociais (dados de geolocalização, endereço de IP, dados online capturados, cookies)	12 (doze) meses após a úlNma aNvidade ou prontamente após revogação do consenNmento.	Eliminação pela empresa, ou *opt-out* a qualquer tempo pelo Ntular.
Recursos Humanos	Gestão de RH (incluindo-se todos que tenham relação profissional com a empresa)	Durante Contrato de Trabalho e mais 5 (cinco) anos após o término, exceto FGTS (30 anos) e Folha de Pagamento (10 anos).	Eliminação pela empresa.
Recursos Humanos	Gestão de Carreiras e Administração pelo RH	Durante Contrato de Trabalho e mais 5 anos após o término.	Eliminação pela empresa.

Recursos Humanos	Recrutamento e Seleção	Reprovação préentrevista: 15 (quinze) dias. Reprovação pós entrevista: 90 (noventa) dias. Obs.: Se autorizado pelo candidato no momento da inscrição, os dados poderão ser manNdos em banco de armazenamento específico para seleção pelo período de 1 (um) ano. Aprovação do candidato: Durante Contrato de Trabalho e mais 5 (cinco) anos após o término.	Eliminação pela empresa.
Segurança	Acesso às instalações hsicas da empresa	5 (cinco) anos após o úlNmo acesso.	Eliminação pela empresa.
	(dados biométricos, nome, foto, RG, CPF, chaves)		
Segurança	Sistema de captura de imagens (câmeras)	120 (cento e vinte) dias após a gravação.	Eliminação pela empresa.
Segurança	Acesso ao sistema de informação da empresa (login e senha)	5 (cinco) anos após o úlNmo acesso.	Eliminação pela empresa.

CAPÍTULO IX

Eliminação pelo Empresa Assim que o período expirar, e desde que não haja uma razão válida para que os mantenhamos, os Dados Pessoais em cópia hsica serão destruídos como resíduo confidencial e aqueles manNdos eletronicamente serão excluídos dos sistemas da empresa e de terceiros contratados.

Hipóteses de invesNgação em curso, processos administraNvos e judiciais são razões válidas para manutenção dos registros e, independentemente de consenNmento, os períodos de armazenamento indicados acima poderão ser prorrogados nesses casos.

Exceto nas hipóteses acima indicadas, caso a empresa tenha o interesse em estender o prazo de armazenamento, os Ntulares dos Dados Pessoais deverão ser noNficados, por escrito, com antecedência razoável da data de término do período de retenção. Se o Ntular dos Registros optar por exercer seu direito de eliminação dessas informações, os Dados Pessoais serão descartados imediatamente pela empresa, exceto em hipóteses de cumprimento de obrigação legal ou regulatória.

CAPÍTULO X Violações e Sanções

Nos casos em que houver violação desta PolíNca e Procedimentos de Segurança da Informação, sanções administraNvas e/ou legais poderão ser adotadas, podendo culminar o desligamento do profissional e ou eventuais processos criminais, se aplicáveis.

Qualquer caso de não cumprimento da políNca de segurança da informação da empresa, por uma área, cliente ou fornecedor, deve ser documentado seguindo o processo correspondente definido.

Os dados manipulados pelo usuário são de sua inteira responsabilidade, de forma que em caso de condenação em ação judicial por vazamento de dados e/ou penalidade aplicada pela Agência Nacional de Proteção de Dados (ANPD), além da multa prevista em contrato por infrações, a empresa se resguarda em envolver o usuário nestes procedimentos, bem como uNlizar do direito de regresso em face daquele que for o causador do vazamento.

CAPÍTULO XI Vigência e Atualização

A vigência deste documento se dará na data de 06/09/2021

A empresa reserva-se o direito de alterar ou atualizar esta PolíNca a qualquer tempo.

Varginha/MG, 06 de setembro de 2021.

ASSOCIAÇÃO BRASILEIRA DE CAFÉS ESPECIAIS – BSCA

Comitê Especial de Planejamento e Implantação da LGPD