POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

Responsável:	Diretor Geral
Última atualização:	Aprovada pelo Conselho de Administração em 25 de outubro de 2022
Normas relacionadas:	Estatuto Social Código de Ética Política de Gerenciamento de Crises

1. Objetivo

Definir a governança e as diretrizes para gestão de informações a que o IBGC tenha acesso no desempenho de suas atividades, diretamente ou por intermédio dos Destinatários, em meio físico ou digital, e que, por sua natureza, exijam medidas especiais de segurança e proteção ("Informações Protegidas").

2. Destinatários:

São Destinatários desta Política os colaboradores, diretores e membros dos órgãos de governança e gestão do IBGC, incluindo coordenadores de capítulos e comissões temáticas, associados, instrutores e demais parceiros da educação, bem como terceiros que acessem Informações Protegidas por força de relação contratual que mantenham com o Instituto ("Destinatários").

3. Espécies de Informações Protegidas

As Informações Protegidas podem consistir em:

Dados Pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável, sujeitas ao regime jurídico da LGPD ("Dados Pessoais");

Informações Organizacionais: dados de empresas e demais organizações com as quais o IBGC se relaciona, bem como as próprias informações do IBGC ("Informações Organizacionais").

4. Classificação das Informações quanto ao Grau de Proteção

O processo de classificação de todas as Informações Protegidas, sejam elas Dados Pessoais ou Informações Organizacionais, deve ser iniciado com a definição do grau de proteção necessário, com base na classificação abaixo:

INFORMAÇÕES CONFIDENCIAIS: Dados sensíveis que devem ser mantidos em confidencialidade e manuseados apenas por pessoas autorizadas pelo detentor ou gestor

da informação. O vazamento de informações com esta classificação pode gerar impactos graves e irreversíveis tanto para o Instituto, quanto para os titulares de dados.

INFORMAÇÕES RESTRITAS: Dados cujo acesso e manuseio são restritos a determinada área, atividade ou nível hierárquico no âmbito do IBGC. Caso sejam divulgadas indevidamente, informações com essa classificação podem prejudicar o Instituto ou os titulares dos dados.

INFORMAÇÕES DE USO INTERNO: Dados de menor criticidade, mas que só devem circular internamente, entre colaboradores, integrantes dos órgãos de governança e de gestão do Instituto e prestadores de serviço, não sendo de acesso público. Vazamentos desse tipo de dado podem prejudicar o bom funcionamento do Instituto.

A gestão estudará as possibilidades de estampar a classificação nas Informações Protegidas como forma de atender ao princípio estabelecido no item 5(i), a seguir.

5. Princípios Gerais

No tratamento das Informações Protegidas, o IBGC observará os seguintes princípios:

(i) Segurança e prevenção: o IBGC adotará as medidas técnicas e organizacionais recomendadas por especialistas no intuito de proporcionar a segurança adequada das Informações Protegidas e prevenir a ocorrência de incidentes de vazamento;

(ii) Boa-fé: todas as operações de tratamento das Informações Protegidas deverão ser pautadas em boas intenções, ética e nos princípios e melhores práticas de governança corporativa.

6. Proteção de Dados Pessoais

Os Dados Pessoais recebidos ou de qualquer forma tratados pelo IBGC serão classificados como Informações Restritas ou como Informações Confidenciais, quando se tratar de dados considerados sensíveis pela Lei Geral de Proteção de Dados - origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

6.1. Princípios Específicos

(i) Finalidade e adequação: o tratamento de Dados Pessoais deve se limitar aos propósitos legítimos, específicos, explícitos e autorizados pelo titular, e somente deve ocorrer de formas compatíveis com estas finalidades;

(ii) Necessidade: a coleta e utilização de Dados Pessoais deverá ser limitada ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular, de modo que tais informações sejam armazenadas pelo menor tempo possível/necessário;

(iii) Livre acesso e qualidade dos dados: a consulta a Dados Pessoais deverá ser disponibilizada aos respectivos titulares de forma simples e gratuita;

(iv) Transparência: os titulares de Dados Pessoais têm direito a receber informações claras, precisas e facilmente acessíveis sobre o tratamento conferido a seus dados;

(v) Não discriminação: as atividades de tratamento de Dados Pessoais jamais poderão objetivar fins discriminatórios, ilícitos ou abusivos;

(vi) Responsabilização: o IBGC deverá armazenar registros de todas as atividades de tratamento de Dados Pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados pessoais, comprovando a eficácia e eficiência de tais medidas.

6.2. Governança do Sistema de Proteção de Dados Pessoais

Para a proteção de Dados Pessoais, o IBGC contará com um Encarregado de Proteção de Dados (“DPO”) e um Comitê de Privacidade, nomeados pelo Diretor Geral.

6.2.1. Comitê de Privacidade

Os objetivos do Comitê de Privacidade são: (i) monitorar e fomentar a comunicação e os treinamentos relacionados à proteção de Dados Pessoais, (ii) discutir e tomar decisões sobre novas atividades de tratamento e (iii) participar das decisões que envolvam tratamento com riscos avaliados como altos pelo DPO.

O Comitê de Privacidade será liderado pelo Diretor Geral e composto pelos gestores de áreas que tenham relação com os temas de privacidade e proteção de dados, incluindo o DPO e representantes dos departamentos Financeiro e de Tecnologia da Informação.

O Comitê de Privacidade reunir-se-á trimestralmente para acompanhamento do programa de privacidade do Instituto.

6.2.2. Encarregado de Proteção de Dados (“DPO”)

O DPO será indicado pelo Diretor Geral e aprovado pelo Conselho de Administração.

Caberá ao DPO adotar todas as medidas adequadas no sentido de manter a conformidade do Instituto com as leis e demais normas de privacidade e proteção de dados aplicáveis às

atividades do IBGC, através do programa de privacidade. Suas principais atribuições consistirão em:

(i) Gestão do programa de privacidade;

(ii) Desenvolvimento, manutenção e revisão anual dos procedimentos de privacidade da organização;

(iii) Fiscalização do cumprimento desta Política e dos Manuais e Procedimentos de Segurança da Informação e Proteção de Dados Pessoais referidos no item 8;

(iv) Monitoramento do nível de conformidade do Instituto;

(v) Atuação como ponto de contato para autoridade nacional de proteção de dados e os titulares dos dados;

(vi) Recepção das eventuais requisições realizadas por titulares de dados pessoais, dando imediato atendimento a tais requerimentos, quando aplicável;

(vii) Preparo dos Relatórios de Impacto à Proteção de Dados Pessoais exigidos por lei, com apuração e revisão dos riscos das atividades nele relatadas;

(viii) Validação da nomeação da rede de colaboradores que apoiará o programa de privacidade;

(ix) Decisão, em casos de risco baixo a moderado, sobre as atividades de tratamento de Dados Pessoais conduzidas pelo Instituto. Caso o DPO classifique um risco como alto, deverá submeter a decisão ao Comitê de Privacidade;

(x) Esclarecimento de dúvidas e orientação aos Destinatários sobre tratamento de Dados Pessoais; e

(xi) Reportes de incidentes aos órgãos internos e externos, em conformidade com esta Política e com a legislação aplicável.

6.3. Providências em Caso de Violação ou Falha de Segurança

Incidentes envolvendo exposição ou vazamento de Dados Pessoais deverão ser imediatamente comunicados ao DPO para que adote as providências de gerenciamento e comunicação devidas.

Além dos demais procedimentos e do plano de comunicação previstos nos Manuais e Procedimentos que complementam esta Política, em caso de incidente de severidade alta ou muito alta, o DPO deverá comunicar imediatamente o Comitê de Privacidade. Caso o

Comitê entenda que o incidente ameaça a imagem, reputação ou operação do IBGC, o Comitê de Crise deverá ser imediatamente acionado.

7. Segurança das Informações Organizacionais

Informações Organizacionais Confidenciais, Restritas ou de Uso Interno deverão ter sua segurança continuamente aprimorada.

O Gerente de Tecnologia da Informação será responsável pela elaboração do Plano de Ação Anual para Melhoria Contínua da Proteção das Informações Organizacionais ("Plano de Proteção das Informações"), o qual contemplará a revisão e atualização de regras e processos, bem como treinamentos e comunicação adequados.

O Plano de Proteção das Informações deverá ser aprovado pelo Diretor Financeiro e de Operações e pelo Diretor Geral, o qual supervisionará a sua execução e, semestralmente, se reportará ao Comitê de Auditoria.

7.1. Providências em Caso de Violação ou Falha de Segurança

Incidentes envolvendo Informações Organizacionais deverão ser imediatamente comunicados ao Gerente de Tecnologia da Informação para que adote as providências necessárias para contenção de danos.

Caso a violação ou falha de segurança seja considerada grave, o caso deve ser comunicado ao Diretor Geral que, se entender necessário, acionará o Comitê de Crises.

8. Manuais e Procedimentos

Os princípios previstos nesta Política serão detalhados nos Manuais e Procedimentos de Segurança da Informação e Proteção de Dados Pessoais, de responsabilidade da gestão do IBGC, que deverá mantê-los atualizados e revisá-los a cada 2 anos.

Os Manuais deverão prever, minimamente, os mecanismos e procedimentos necessários a ou ao:

(i) obtenção da segurança física das Informações Protegidas;

(ii) fixação das regras de utilização de recursos de Tecnologia da Informação disponibilizados pelo IBGC aos Destinatários;

(iii) tratamento de Informações Protegidas;

(iv) retenção e descarte de Informações Protegidas;

(v) estabelecimento de procedimentos e plano de comunicação em caso de incidentes que resultem em vazamento/exposição das Informações Protegidas;

(vi) contratação de consultoria independente para realização de testes rotineiros de intrusão no sistema do IBGC e apresentação de relatório de resultados e plano de ação de melhorias.

9. Treinamentos

Os Destinatários deverão receber treinamentos periódicos sobre segurança de informação e proteção de Dados Pessoais, que deverão cobrir o teor desta Política, bem como dos Manuais e Procedimentos de Segurança da Informação e Proteção de Dados Pessoais que a complementam, conforme necessidade de cada grupo de Destinatários.

Novos colaboradores e membros dos órgãos de gestão e governança do Instituto deverão receber orientações e acesso a esta Política e aos Manuais e Procedimentos de Segurança da Informação e Proteção de Dados Pessoais como parte de seu processo de integração.