

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

### SUMÁRIO DA NORMA

1. OBJETIVO.....	3
2. DEFINIÇÕES.....	3
3. PRINCÍPIOS.....	4
4. ABRANGÊNCIA.....	4
5. DIRETRIZES.....	4
6. COMPETÊNCIAS E RESPONSABILIDADES.....	5
7. DISPOSIÇÕES FINAIS.....	6

## **PREFÁCIO**

### **TÍTULO**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

### **UNIDADE GESTORA**

GERÊNCIA EXECUTIVA ADMINISTRATIVA E FINANCEIRA

### **UNIDADE(S) CO-RESPONSÁVEL(IS)**

GERÊNCIA EXECUTIVA DE GOVERNANÇA

### **ÓRGÃO APROVADOR**

CONSELHO DE ADMINISTRAÇÃO - CONAD

### **ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR**

Revisão Geral

### **RELAÇÃO COM OUTROS NORMATIVOS**

Não se aplica.

### **REGULAMENTAÇÃO UTILIZADA**

Despacho CONAD – Nota Técnica nº 121/2020, de 09/11/2020

### **DOCUMENTAÇÃO UTILIZADA**

ABNT NBR ISO/IEC 27002

Lei nº 12.527, de 18/11/2011

Lei nº 13.709, de 14/08/2018

Decreto nº 7.724, de 16/05/2012

### **NORMATIVOS REVOGADOS**

Não se aplica.

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

### 1. OBJETIVO

1.1. Estabelecer os princípios e diretrizes para garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações lógicas e físicas processadas pela ABGF (“Empresa”), em todos os níveis da Empresa, respeitando a legislação e regulamentação vigentes sobre o tema.

### 2. DEFINIÇÕES

- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- Autenticidade: garantia de identificação e registro do usuário que está produzindo, enviando ou modificando a informação, de forma claramente documentada.
- Confidencialidade: garantia que a informação é acessível somente por pessoas autorizadas a terem acesso.
- Dado Anonimizado: dado pessoal relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável, desde que coletada em território nacional.
- Dado Pessoal Sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural.
- Diretriz: conjunto de instruções ou indicações para se tratar e levar a termo um plano, uma ação, um negócio.
- Disponibilidade: garantia de que usuários autorizados obtenham acesso à informação e aos ativos correspondentes.
- Incidente / Violação de Segurança: tentativa ou concretização de um evento que comprometa a integridade, autenticidade, conformidade ou disponibilidade de qualquer ativo da Empresa.
- Informação: recurso fundamental para o desenvolvimento das atividades da ABGF, e, como tal, necessita ser protegida. A segurança da informação visa preservar a confidencialidade, integridade e disponibilidade da informação.
- Integridade: manutenção da informação na forma em que foram originalmente produzidas e armazenadas, não podendo sofrer modificações não autorizadas previamente. Tais modificações, quando não planejadas, podem gerar informações incorretas e comprometer a integridade de todo o sistema de informações.
- Plano de Contingência: também denominado de planejamento de riscos, plano de continuidade de negócios ou plano de recuperação de desastres, tem o objetivo de descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar

plenamente, ou em um estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à Empresa.

- **Proteção de Dados:** ações integradas com o objetivo de promover a proteção dos dados pessoais, buscando sempre a sua anonimização, bem como a observância da legislação vigente.
- **Segurança da Informação:** proteção de um conjunto de informações no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas corporativos, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.
- **Sigilo Bancário:** direito individual de clientes e de terceiros à manutenção da confidencialidade de seus dados econômicos e financeiros, não podendo ser revelados, fora das hipóteses legais, no exercício das atividades da Empresa.
- **Sigilo Empresarial:** proteção dos dados e documentos produzidos por uma empresa no exercício de sua atividade econômica, buscando proteger as informações que propiciam à ABGF vantagens competitivas fundamentais para o êxito da atividade. Estão enquadradas nesta categoria marcas, patentes, *know-how*, análises e segredos industriais, cuja divulgação pode acarretar danos materiais ou morais à Empresa.

### **3. PRINCÍPIOS**

3.1. Os princípios a serem observados na gestão da segurança da informação da ABGF são: confidencialidade, integridade, disponibilidade e autenticidade.

### **4. ABRANGÊNCIA**

4.1. Esta Política aplica-se à ABGF em toda a sua estrutura organizacional, ou seja, alta administração, gestores, funcionários, colaboradores e demais partes relacionadas.

### **5. DIRETRIZES**

5.1. A Política de Segurança da Informação da ABGF tem como diretrizes:

- I. Assegurar a fidedignidade das informações, ou seja, a conformidade dos dados armazenados com relação às inserções, alterações e processamentos autorizados e efetuados, sendo possível confirmar a identidade da pessoa que produziu ou entidade que prestou as informações, desde que não sejam identificados como dados pessoais sensíveis;
- II. Garantir que as informações somente sejam acessadas por pessoas autorizadas, evitando que terceiros tomem conhecimento das informações, de forma acidental ou proposital, posto que não dispõem de autorização para o acesso;
- III. Assegurar o sigilo de informações que são protegidas por lei, em especial aquelas relativas ao sigilo bancário e empresarial, quando for o caso;

- IV. Assegurar que as informações sejam prestadas pelos órgãos ou instâncias competentes da ABGF;
- V. Certificar que as informações necessárias estejam disponíveis às pessoas e aos processos autorizados, para a prestação contínua dos serviços;
- VI. Assegurar que os controles de segurança da informação sejam percebidos por todos os níveis da Empresa;
- VII. Garantir a proteção de dados de funcionários, clientes e fornecedores em observância aos dispositivos estabelecidos nas regulamentações relacionadas ao assunto;
- VIII. Garantir a existência de mecanismos e/ou instrumentos que assegurem o acesso à informação, preservadas as situações de sigilo das informações protegidas pela legislação;
- IX. Assegurar a existência de mitigadores de riscos para evitar incidentes / violações de segurança nas atividades da Empresa; e
- X. Garantir a existência de procedimentos de segurança, tais como cópias de segurança (*backup*) e de recuperação (*restore*) e a manutenção de registros de periodicidade, atualização e testes.

## **6. COMPETÊNCIAS E RESPONSABILIDADES**

- 6.1. As competências e responsabilidades dos entes que compõem a estrutura de segurança da informação da ABGF estão previstas no Estatuto Social, Regimento Interno e normativos da Empresa.
- 6.2. Compete ao Conselho de Administração:
  - 6.2.1. aprovar as Políticas da ABGF.
- 6.3. Compete à Diretoria Executiva:
  - 6.3.1. submeter os assuntos relacionados à Política de Segurança da Informação, que dependam de deliberação do Conselho de Administração.
- 6.4. Compete à Comissão de Segurança da Informação:
  - 6.4.1. manifestar-se, preliminarmente, ao encaminhamento à Diretoria Executiva, de propostas relacionadas a:
    - 6.4.1.1. Política de Segurança da Informação;
    - 6.4.1.2. normativos relacionados à segurança de informação; e
    - 6.4.1.3. Plano de Continuidade de Negócios.
  - 6.4.2. manifestar-se, preliminarmente, ao Comitê de TI, sobre investimentos, projetos, demandas ou ações de TI, que envolvam segurança da informação;
  - 6.4.3. aprovar estratégias, planos e ações relacionadas à segurança da informação;
  - 6.4.4. promover a disseminação da cultura em segurança da informação; e

6.4.5. acompanhar a efetividade das ações relacionadas à segurança da informação.

## **7. DISPOSIÇÕES FINAIS**

7.1. Esta política será revisada anualmente.

7.2. O original desta Política, bem como a Nota Técnica e o Voto que a aprovou, em meio físico, estão sob a guarda da GEGOV.

7.3. O Normativo e a Nota Técnica, ambos digitalizados, em formato de documento *PDF*, estão arquivados na rede da ABGF.