CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
POL-03-01 Versão 01	**00**	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	**A partir de: 31/08/2023**

DESTINATÁRIO

- Todas as Unidades Organizacionais.

PRINCIPAIS ALTERAÇÕES

- Implantação

UNIDADE GESTORA DO PROCESSO (Assinatura e Carimbo)	DOCUMENTO DE APROVAÇÃO
Gerência de Tecnologia da Informação	**DIRE** **CONSELHO ADMINISTRATIVO – ATA 447ª**

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
POL-03-01 Versão 02	**00**	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	**A partir de: 31/08/2023**

SUMÁRIO

AGEHAB
Agência Goiana de Habitação

1. OBJETIVO

1.1. A presente Política tem por objetivo conduzir estrategicamente os assuntos relacionados à segurança da informação, por meio do estabelecimento de diretrizes quanto ao tratamento dos dados, garantindo a proteção, a preservação e o descarte de informação no ambiente convencional ou de tecnologia da AGEHAB. Os dados, quando coletados e/ou produzidos, são tratados, compartilhados, transferidos e armazenados na Agência.

2. NORMAS APLICÁVEIS

2.1. Esta Política foi elaborada à luz das seguintes Legislações:

2.1.1. Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais "LGPD");

2.1.2. Decreto nº 10.222, de 5 de fevereiro de 2020 – Aprova a Estratégia Nacional de Segurança Cibernética;

2.1.3. Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

2.1.4. Lei Federal nº 12.527/2011 (Lei de Acesso à Informação);

2.1.5. Lei Estadual nº 18.025/2013 - Dispõe sobre o acesso a informações e a aplicação da Lei federal no 12.527, de 18 de novembro de 2011, no âmbito do Estado de Goiás, institui o serviço de informação ao cidadão e dá outras providências.

2.1.6. Decreto Estadual nº 7.904/2013 - Regulamenta a Lei nº 18.025, de 22 maio de 2013, que dispõe sobre o acesso à informação e a aplicação da Lei nº 12.527, de 18 de novembro de 2011, no âmbito do Estado de Goiás, institui o serviço de informação ao cidadão e dá outras providências.

2.1.7. Lei Federal nº 12.965/2014 (Marco Civil da Internet);

2.1.8. Lei Federal nº 8.078/1990 (Código de Defesa do Consumidor), sem prejuízo de observância às demais legislações aplicáveis para as atividades desempenhadas pela AGEHAB;

2.1.9. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação;

2.1.10. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação;

2.1.11. ABNT ISO GUIA 73:2009 – Gestão de riscos;

2.1.12. Código de Ética e Conduta da AGEHAB;

2.1.13. Política de Privacidade de Dados da AGEHAB;

2.1.14. Política de Gestão de Riscos da AGEHAB.

3. CONCEITOS

TERMO	DEFINIÇÃO
Artefato Malicioso	Programa ou parte de um programa construído no intuito de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou rede de computadores.
Ataque	Tentativa não autorizada visando o acesso ou manipulação de informações, ou, ainda, tornar um sistema não íntegro, inacessível, ou indisponível.
Ativo	Todo e qualquer recurso que tenha valor para a AGEHAB.
Ativo de Informação	Informações, dados e seus meios de armazenamento, transmissão e processamento, bem como os equipamentos necessários para tanto, os sistemas utilizados, os locais onde se encontram esses meios, além dos recursos humanos que se têm acesso.
Informação	Dados, processados ou não, que podem destinar-se à produção e transmissão de conhecimento, contidos em qualquer formato, suporte ou meio.
Colaborador	Todos os diretores, gerentes, assessores, coordenadores, conselheiros, empregados, cedidos, requisitados, contratados, prestadores de serviço, estagiários e jovens aprendizes que atuem na AGEHAB.
Gestor de Informação	Aqueles que exercem atividades gerenciais ou são titulares dos órgãos executivos de direção superior, conforme norma específica.
Espaço Cibernético	Espaço virtual constituído por redes e canais de comunicação que asseguram a interconexão dos dispositivos, integrando todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, bem

	como as demais ações, humanas ou automatizadas, operadas neste espaço.
Incerteza	Estado de escassez ou carência de informações relacionadas a um tema, assunto ou evento, dificultando sua compreensão, com a possibilidade de se transformar em uma ameaça ou em uma oportunidade para a Agência.
Incidente de Segurança da Informação	Todo e qualquer evento adverso, confirmado ou sob suspeita, que venha a atingir a proteção dos sistemas de informação e, consequentemente, a segurança da informação.
Privacidade	Direito à reserva de informações pessoais, bem como prerrogativa de controlar e filtrar a exposição e disponibilidade de informações acerca de si mesmo.
Proprietário da Informação	Gestor de unidade organizacional incumbido de produzir ou tratar das informações em seus processos de negócio.
Proprietário do Risco	Aquele que possui autoridade e responsabilidade pelo gerenciamento dos riscos de segurança da informação.
Risco de Segurança da Informação	Evento possível relacionado à exploração de uma ou mais vulnerabilidades de um ativo de informação, por parte de uma ou mais ameaças.
Segurança Cibernética	Atividade voltada à segurança das operações, visando assegurar sistemas de informação capazes de resistir a investidas no espaço cibernético capazes de comprometer a integridade, a confidencialidade, a autenticidade e até mesmo a disponibilidade dos dados armazenados e dos serviços que esses sistemas dispõem.
Segurança da Informação	Ações pertinentes à disponibilidade, integridade, confidencialidade e autenticidade da informação.
Segurança Física	Regras e parâmetros físicos adotados no intuito de impedir, detectar e responder ao acesso não autorizado a pessoas, bens, valores, equipamentos e instalações referentes aos ativos de informação.
Titular	Pessoa natural detentora dos dados pessoais objetos de tratamento.
Usuário	Pessoa habilitada para acessar os ativos de informação da AGEHAB.
Violação	Toda e qualquer atividade que desrespeite as diretrizes aqui estabelecidas ou nos demais instrumentos e normas regulamentares que complementem a presente política.

4. ABRANGÊNCIA

4.1. A presente Política se aplica a todos os colaboradores, prestadores de serviços, estagiários e menores aprendizes, usuários das informações da AGEHAB.

4.2. Esta Política compreende todos os requisitos de segurança lógica, física e pessoal nos ambientes físicos e computacionais.

5. PRINCÍPIOS

5.1. A AGEHAB atua com base nos seguintes princípios:

5.1.1. **Disponibilidade**: garantir a acessibilidade da informação e a sua utilização sob demanda da Agência;

5.1.2. **Integridade**: garantir que a informação não seja modificada ou destruída de maneira não autorizada ou acidental;

5.1.3. **Confidencialidade**: garantir que a informação não esteja disponível a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

5.1.4. **Autenticidade**: garantir a origem e a autoria da informação, para que sejam sempre identificáveis.

5.1.5. **Simplicidade**: garantir que os controles de segurança sejam simples e objetivos, visando mitigar as chances de erros advindos da complexidade;

5.1.6. **Auditabilidade**: garantir a rastreabilidade de todos os eventos significativos de usuários e processos, por meio do registro detalhado;

5.1.7. **Criptografia**: garantir que os controles de segurança utilizem tecnologias modernas e sistemas criptográficos na transmissão de dados e informações confidenciais, inclusive nos meios de comunicação móvel;

5.1.8. **Conformidade e Legalidade**: garantir a adesão de padrões normativos, contratos e legislações vigentes.

6. DIRETRIZES

6.1. A Informação

6.1.1. Toda informação utilizada pela AGEHAB é um ativo e possui valor, necessitando do gerenciamento adequado ao longo de todo seu ciclo de vida, com a disponibilização do acesso ao público apropriado, resguardada contra manipulação indevida, com tratamento adequado ao seu grau de sigilo ou restrição de acesso e passível de rastreamento.

6.2. Proprietário da Informação

6.2.1. A AGEHAB é proprietária e detentora do direito de uso exclusivo das informações geradas, armazenadas, processadas ou transmitidas no ambiente convencional ou de tecnologia.

6.3. Classificação da Informação

6.3.1. Todas as informações utilizadas pela AGEHAB deverão ser classificadas a partir de critérios definidos em documentos normativos internos, quanto ao seu grau de sigilo ou nível de restrição de acesso, em vista dos processos e atividades nas quais estão inseridas, no intuito de garantir que as informações recebam um nível adequado de proteção, com base no seu valor, sensibilidade, requisitos legais e criticidade para a Agência.

6.3.2. As Informações podem ser classificadas como:

6.3.2.1. públicas: informações corporativas que devem ser divulgadas publicamente por força de lei; que possa ou precise ser divulgada à sociedade, sem a iminência de riscos; por interesse ou necessidade da AGEHAB na realização e efetivação das atividades desenvolvidas;

6.3.2.2. internas: informações que, por sua natureza, conteúdo ou força de lei, caso publicizada, possam representar risco ou incidente operacional;

6.3.2.3. restritas: informações que, se divulgadas, trarão impacto significativo nas operações da Agência e, devido ao nível de confidencialidade maior, somente pode ser acessada por usuários da AGEHAB;

6.3.2.4. confidenciais: informações que, se divulgadas, trarão maiores impactos sobre os objetivos estratégicos e a imagem da Agência e, portanto, somente pode ser acessada por usuário da AGEHAB explicitamente indicado pelo gestor da informação.

6.4. Utilização da Informação e dos Recursos

6.4.1. Cabe ao gestor da informação determinar a autorização de acesso, incluindo os relacionados ao sistema de gestão da Agência, tendo em vista o sigilo adequado e a necessidade de acesso para cada de tipo de agente;

6.4.2. O acesso à informação deve ser autorizado apenas aos colaboradores que dela necessitem para o desempenho de suas atividades profissionais;

6.4.3. É vedado o acesso do colaborador às informações ou sistemas não autorizados previamente. Qualquer tentativa não autorizada de acesso à informação ou sistema deve ser considerada uma falta disciplinar;

6.4.4. É vedada a utilização da credencial (*login* e senha) por colaborador diferente do autorizado, sendo seu uso individual, intransferível e de conhecimento exclusivo;

6.4.5. Os recursos corporativos fornecidos pela AGEHAB, especialmente o e-mail, devem ser utilizados prioritariamente para fins profissionais. Deste modo, o uso destes recursos deve seguir o padrão de linguagem profissional, que não comprometa a imagem da Agência, e que não viole leis e normativas vigentes, bem como o Código de Ética e Conduta da AGEHAB;

6.4.6. A utilização do correio eletrônico é pessoal e o usuário se responsabilizará por toda mensagem enviada pelo seu endereço de e-mail;

6.4.7. A utilização dos recursos corporativos deve ser registrada e monitorada pela AGEHAB, não devendo o colaborador ter expectativa de sigilo em sua utilização.

6.5. Proteção da Informação

6.5.1. A segurança da informação será alcançada por meio da implementação dos controles adequados, com a inclusão de processos, procedimentos, políticas, estruturas organizacionais e sistemas;

6.5.2. Cabe ao colaborador preservar a integridade dos documentos, cadastros, registros e sistemas de informação da AGEHAB, em todos os meios utilizados pela Agência, tanto físico quanto eletrônico;

6.5.3. Cabe aos gestores dos departamentos tomar providências visando a proteção e controle de acesso físico aos seus recursos de informação, devendo observar o nível de criticidade e/ou classificação;

6.5.4. Todo e qualquer incidente que venha a afetar a segurança da informação deve ser reportado à diretoria responsável por segurança da informação;

6.5.5. Todos os riscos de segurança da informação deverão ser identificados, quantificados e priorizados visando a sua mitigação por meio de medidas de proteção pertinentes;

6.5.6. Cabe às áreas de segurança cibernética a manutenção dos registros atualizados dos indicadores de segurança da informação, da arquitetura cibernética, dos ativos tecnológicos, das configurações e das soluções de segurança utilizados pela Agência;

6.5.7. Cabe às áreas de segurança cibernética informar às áreas de segurança da informação quaisquer dados que se façam necessários para compor relatórios à administração da AGEHAB.

6.6. Segurança Física dos Ambientes

6.6.1. Toda informação considerada crítica deve ser armazenada em área segura, protegidas por um perímetro de segurança pré-definido e de acesso controlado;

6.6.2. Apenas aos responsáveis pelas informações incumbe o acesso administrativo a estas, havendo a necessidade de credenciais para tanto.

6.7. Sigilo da Informação

6.7.1. A AGEHAB adotará como regra o princípio da transparência e publicidade máxima, devendo seguir as determinações da Lei de Acesso à Informação (Lei N. 12.527/2.011), bem como da Lei Estadual nº 18.025/2.013 e o Decreto Estadual N. 7.904/2.013, com relação ao sigilo de suas informações;

6.7.2. É vedada a divulgação ou utilização das informações corporativas da AGEHAB em benefício próprio ou de terceiros, não importando o tipo de mídia ou suporte utilizado.

6.8. Continuidade do Uso da Informação

6.8.1. Os recursos presentes em ambientes físicos ou virtuais utilizados nas atividades de gestão, nas operacionais e nas atividades de suporte da AGEHAB, devem se manter resguardados de hipóteses de indisponibilidade, contando ainda com planos de continuidade definidos;

6.8.2. Cabe aos gestores das áreas a definição e implementação de medidas de proteção e recuperação em face a desastres e situações de contingência, as quais devem contemplar os colaboradores e os recursos de tecnologia e de infraestrutura necessários.

6.9. Do tratamento formal com terceiros

6.9.1. Todos os contratos, convênios, acordos de gestão, formação de consórcios, etc. que envolvam terceiros com compartilhamento de

informações da AGEHAB e/ou a concessão de acesso aos seus ambientes e recursos corporativos devem ser precedidos por termos de confidencialidade que, por sua vez, devem conter cláusulas específicas acerca da privacidade e segurança da informação.

6.10. Capacitação e Treinamento

6.10.1. A AGEHAB deve incluir o tema “Segurança da Informação” em seus programas de capacitação, de modo a promover maior consciência da responsabilidade individual dos usuários.

6.11. Temporalidade da Informação

6.11.1. A AGEHAB deve garantir que todas as informações que possuam valor comprobatório para fins de auditorias ou processos judiciais sejam preservadas na forma e pelos prazos demandados.

6.12. Tratamento de Dados Pessoais

6.12.1. A AGEHAB deve garantir o adequado tratamento de dados pessoais, conforme o que dispõe a Lei Geral de Proteção de Dados (LGPD), assegurando o exercício pleno de um encarregado de tratamento de dados pessoais e, ainda, estabelecer um canal de atendimento à sociedade e de interação com a Autoridade Nacional de Proteção de Dados (ANPD) e processos formais de tratamento de incidentes com privacidade dos dados pessoais.

6.13. Penalidades

6.13.1. A comprovação de qualquer descumprimento das determinações da Política de Segurança da Informação deve ser relatada à chefia imediata do infrator, que por sua vez deve relatar ao Comitê Gestor de Segurança da Informação **ou** à Gerência de Procedimentos Correicionais (GECOR), vez que esta unidade atua nos processos administrativos disciplinares e de sindicância da AGEHAB, que fundamentarão as penalidades administrativas/contratuais a serem aplicadas, sem qualquer prejuízo de outras.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. **Conselho Administrativo:** Aprovar esta política e deliberar sobre as diretrizes estratégicas de segurança da informação, no intuito de nortear o processo de implementação na AGEHAB;

7.2. **Alta Administração**: Apoiar e exigir o cumprimento desta política, bem como instituir o Comitê Gestor da Segurança da Informação na AGEHAB;

7.3. **Comitê Gestor de Segurança da Informação**:

7.3.1. elaborar e atualizar as Instruções Normativas de Segurança da Informação, em conformidade com a presente política, as legislações e regulamentos pertinentes;

7.3.2. desenvolver um Plano de Continuidade de Negócios, periodicamente testado, com a exibição de resultados;

7.3.3. estabelecer mecanismos de registro e controle de não conformidade à presente política, às normas e procedimentos pertinentes à segurança da informação;

7.3.4. auxiliar as diretorias da AGEHAB na classificação das informações de sua custódia;

7.3.5. revisar esta Política;

7.3.6. O Comitê Gestor de Segurança da Informação será nomeado pelo Diretor-Presidente, sendo preferencialmente composto por:

7.3.6.1. um gestor de Segurança da Informação, que conduzirá as atividades do Comitê;

7.3.6.2. um membro da Gerência de Tecnologia da Informação;

7.3.6.3. um membro da Assessoria Jurídica;

7.3.6.4. um membro da Gerência de Gestão de Pessoas - GGP;

7.3.6.5. um membro da Assessoria de Controle Interno.

7.4. Gestor da Informação

7.4.1. elaborar relatórios críticos acerca da aplicabilidade e adesão dos requisitos da segurança da informação estabelecidos na presente política;

7.4.2. analisar, periodicamente, a classificação dos ativos que requerem algum grau de sigilo sob sua propriedade, em consonância com o que dispõe a legislação vigente;

7.4.3. participar do processo de avaliação de risco;

7.4.4. participar de deliberações relacionadas a qualquer violação de segurança dos ativos sob sua responsabilidade;

7.4.5. participar da criação dos critérios para o estabelecimento dos perfis de acesso a informações sob sua responsabilidade;

7.4.6. autorizar a liberação de acesso à informação sob sua responsabilidade;

7.4.7. auxiliar na investigação de incidentes de segurança em ativos sob sua responsabilidade;

7.5. Gestor da Segurança da Informação

7.5.1. presidir o Comitê Gestor de Segurança da Informação;

7.5.2. assegurar a aderência da Política de Segurança da Informação, por meio de avaliações e auditorias;

7.5.3. monitorar as investigações de danos referentes às quebras de segurança;

7.5.4. requerer dos proprietários a classificação das informações no departamento sob sua gerência;

7.5.5. realizar e conduzir estudos de novas tecnologias, atualizando-se e, quando possível, remediando e/ou reduzindo impactos na segurança da informação;

7.5.6. definir parâmetros que permitam aferir a eficácia dos controles de segurança aplicados.

7.6. Usuários:

7.6.1. Figuram-se como usuários todos os colaboradores da AGEHAB, prestadores de serviço, estagiários e menores aprendizes, sem a observância do nível hierárquico da Agência;

7.6.2. Cabe ao usuário:

7.6.2.1. observar e seguir rigorosamente as orientações da presente Política, utilizando-se de mecanismos e controles de segurança disponíveis, sob a sua guarda e responsabilidade;

7.6.2.2. comunicar ao departamento competente quaisquer riscos ou incidentes de segurança que tenha conhecimento;

7.6.2.3. participar de treinamentos acerca da segurança da informação, quando forem ofertados;

7.6.2.4. manter, obrigatoriamente, os dados critérios da sua área de atuação em compartilhamentos de rede disponibilizados pela AGEHAB;

7.6.2.5. não utilizar serviços de e-mail diferente do institucional para realização de atividades referente à AGEHAB, vez que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;

7.6.2.6. utilizar sua conta de e-mail corporativo para fins estritamente institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou da própria AGEHAB;

7.6.2.7. acessar à Internet apenas para navegação em sítios cujo conteúdo esteja em conformidade às atribuições institucionais, às determinações da AGEHAB e aos dispositivos legais.

8. DISPOSIÇÕES GERAIS

8.1. O presente documento deve integralmente lido, debatido e aplicado em conjunto com as demais políticas e normas vigentes na AGEHAB. Outrossim, esta política deve ser acompanhada por outros documentos normativos que tratem especificamente da segurança da informação, sempre alinhados às diretrizes e princípios aqui estabelecidos.

8.2. As diretrizes e princípios aqui expostos devem nortear a atuação de todos os colaboradores (usuários) da AGEHAB, em especial, aos departamentos responsáveis pela tecnologia da informação e da segurança da informação.

8.3. A segurança da informação é uma responsabilidade contínua de cada usuário da AGEHAB, sempre consciente de todas as informações que acessa e gerencia.

8.4. A presente política, juntamente aos seus documentos normativos complementares, deve ser amplamente divulgada a todos os colaboradores.

9. ATUALIZAÇÃO

9.1. A Política de Segurança da Informação da AGEHAB será atualizada sempre que houver necessidade, no intuito de garantir que os parâmetros técnicos e legais de segurança estejam alcançando o seu cumprimento integral.

10. APROVAÇÃO

10.1. A presente Política foi aprovada pelo Conselho Administrativo da AGEHAB, na data de 31 Agosto de 2023, registrada na Ata 447ª.