POL .CORP. TI .001 *POLÍTICA GERAL DA SEGURANÇA DA INFORMAÇÃO*

Elaborado por: *Meline Rodrigues – Analista de TI*
Revisado por: *Rodrigo Maia – Superintendente de TI*
Aprovado por: *Marcelo Augusto Raposo da Mota – CFO*
Revisão*: 01*

1. OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores e parceiros do Grupo Águas do Brasil seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de políticas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do GAB quanto à: Integridade, Confidencialidade, Disponibilidade e Legalidade.

2. APLICAÇÃO

Colaboradores, estagiários, prestadores de serviço, parceiros e fornecedores que possuem acesso às informações do Grupo Águas do Brasil.

3. CONTEÚDO GERAL

3.1. Siglas

- PSI: Política de Segurança da Informação.
- SGSI: Sistema de Gestão de Segurança da Informação.
- GAB: Grupo Águas do Brasil.

3.2. Definições

- **Segurança da Informação**: preservação de confidencialidade, integridade e disponibilidade da informação.
- **Alta Direção:** grupo de pessoas que representam o mais alto nível da hierarquia do GAB.
- **Controle de Acesso:** meios para assegurar que o acesso aos bens é autorizado e limitado baseado nos requisitos de segurança e do negócio.
- **Autenticação:** provisão de garantia que uma característica alegada por uma entidade está correta.
- **Incidente de Segurança da Informação:** um ou mais eventos de segurança da informação indesejados ou inesperados que tem probabilidade significativa de comprometer operações do negócio, ameaçando a segurança da informação.
- **Evento de Segurança da Informação:** ocorrência identificada de um sistema ou rede, que indica uma possível violação da PSI ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em prejuízo ao sistema ou organização.

- **Validação:** confirmação, através de evidência objetiva, que os requerimentos para uma utilização ou aplicação desejada específica foram cumpridos (ISO 9000).
- **Verificação:** confirmação, através da disponibilização de evidência objetiva, que requerimentos especificados foram cumpridos (ISO 9000).
- **Vulnerabilidade:** fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças
- **Informação Sigilosa:** informação sigilosa na qual o acesso é restrito por lei ou regulamentos internos do GAB a classes específicas de pessoas.
- **Informação sensível**: toda informação que verse diretamente sobre o desempenho das atividades vinculadas ao objeto social do GAB. Ex: custos; nível de capacidade e objetivo de expansão; principais clientes; principais fornecedores e termos de contratos com eles celebrados; estratégias competitivas, etc.

4. DETALHAMENTO

4.1. Infraestrutura de Segurança

4.1.1. A informação é um ativo dos mais importantes para GAB e, por tal valor crítico para o negócio, deve ser adequadamente protegida. Sua Segurança deve ser baseada tanto na implementação de controles físicos, lógicos e comportamentais quanto na preservação e garantia de princípios fundamentais:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protege-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Legalidade**: conformidade com obrigações legais e contratuais.

4.1.2. Os objetivos supramencionados, visam proteger os sistemas e sua informação, independente da forma ou meio como ela é tratada, de diversos tipos de ameaças, minimizando danos de qualquer ordem ou tipo, preservando a continuidade dos serviços críticos e negócios e maximizando o retorno de investimentos e as oportunidades de negócio.

4.1.3. A Alta Direção, alinhada ao planejamento para a Segurança da Informação, deve estar envolvida e comprometida com o processo de implementação, manutenção e aperfeiçoamento desta Política que, baseada na ISO/IEC 27001 e ISO/IEC 27002, pretende criar um Sistema de Gestão de Segurança da Informação (SGSI), destinado a preservar a Segurança e a Continuidade do Negócio. Assim, a Alta Gestão Executiva deve ter como responsabilidades:

- Aprovar a Política de Segurança da Informação;
- Garantir que os objetivos para Segurança da Informação são estabelecidos e acompanhados;
- Estabelecer regras e responsabilidades para Segurança da Informação;
- Comunicar a todos sobre a importância do atendimento aos objetivos da Segurança da Informação;
- Ministrar ações de conscientização e acompanhar incidentes;
- Provisão de recursos suficientes para desenvolver, implementar, operar e manter o SGSI;
- Decidir sobre critérios de aceitação e níveis de risco;
- Definir o estabelecimento de processo de auditorias internas anuais.

4.1.4. Periodicamente, devem ser estabelecidas e revistas as diretrizes da Segurança da Informação, atribuídas, claramente, as responsabilidades e destinados os recursos necessários para a sua implementação, assim como deverão ser feitas análises críticas sobre resultados obtidos e ações corretivas efetivadas.

4.1.5. Os gestores (ou proprietários) de sistemas e informações, como responsáveis por estas, devem examinar a necessidade de protegê-los, definindo, a intervalos regulares, sua classificação, medidas de proteção e direitos de acesso, em conformidade com esta Política.

4.1.6. Os usuários dos serviços e recursos corporativos providos pelo GAB devem:

- Estar cientes e cumprir, rigorosamente, esta Política de Segurança da Informação;
- Implementar medidas de proteção aos ativos sob sua responsabilidade, custódia ou uso, assegurando a conformidade com as regras estabelecidas;
- Respeitar, zelar e preservar os ativos sob sua responsabilidade, custódia ou uso, sobretudo o grau de confidencialidade das informações por eles custodiadas, divulgando-as apenas conforme autorização formal;
- Observar e respeitar a legislação, estatutos e acordos contratuais a que o GAB esteja submetida;
- Relatar incidentes de segurança acontecidos, por acontecer ou mesmo supostos;
- O login e senha são sigilosos, devendo ser apenas de conhecimento do profissional que o criou, ou seja, o seu usuário;
- Os referidos login e senha só poderão ser fornecidos ao superior imediato do usuário mediante determinação deste por escrito.

POL .CORP. TI .001 ***POLÍTICA GERAL DA SEGURANÇA DA INFORMAÇÃO***

Elaborado por: *Meline Rodrigues – Analista de TI*
Revisado por: *Rodrigo Maia – Superintendente de TI*
Aprovado por: *Marcelo Augusto Raposo da Mota – CFO*
Revisão*: 01*

4.2. Gestão e Uso de Ativos

4.2.1. O GAB é o único proprietário de toda a informação adquirida, gerada, armazenada, processada ou transportada por meio dos seus ativos tecnológicos e ambientes físicos, assim como de todos os ativos responsáveis por este processo.

4.2.2. Todos os ativos tecnológicos sejam eles relacionados ao processamento, armazenamento ou transmissão de informações, devem ser submetidos a processo de identificação e inventário sistemático, atualizado periodicamente, e a eles deve estar relacionado um gestor responsável.

4.2.3. Os sistemas de informações do GAB devem ser disponibilizados e configurados de acordo com a PSI estabelecida para o GAB, bem como os demais procedimentos do Grupo.

4.2.4. A classificação dos ativos tecnológicos, sobretudo informações, e a consequente aplicação de medidas de proteção físicas e lógicas, deve se basear, principalmente, no valor e criticidade destes ativos para os processos de negócio do GAB, bem como nos requisitos legais a que eles estiverem submetidos. As medidas de proteção devem ser feitas conforme os procedimentos departamentais estabelecidos pelo gestor responsável pelo ativo.

4.2.5. Os recursos ou serviços corporativos, providos pelo GAB, devem ser usados apenas para desenvolvimento das atividades profissionais, sendo cada um dos colaboradores desta empresa co-reponsável pela implementação e manutenção das regras de segurança estabelecidas.

4.2.6. Quanto a troca de informações:

- Quaisquer informações não endereçadas ao respectivo colaborador não devem ser usadas ou reveladas a terceiros, salvo quando autorizado;
- Antes de disseminar informações confidenciais, deve ser assegurada a sua proteção adequada;
- Deve estar de acordo com a legislação vigente e as políticas estabelecidas, inclusive os demais procedimentos do GAB.

4.2.7. O acesso aos sistemas de informações GAB em regime de Home Office ou em viagens de negócio, deve ser feito através de métodos e softwares formalmente estabelecidos e aprovados pelo GAB.

4.2.8. Informações confidenciais (ex.: arquivos digitais e impressos, manuscritos, relatórios de sistemas), baseadas no processo de Classificação da Informação estabelecido, devem ser manipuladas de forma segura, seja durante seu armazenamento, processamento, transporte ou descarte. Desta forma:

- Informação confidencial não deve ser exposta publicamente ou revelada, salvo se autorizado (ex.: senhas);
- Informação confidencial em formato eletrônico deve ser enviada para o mundo externo ao GAB em e-mails ou arquivos apenas se criptografados;
- Informação confidencial em formato eletrônico deve ser armazenada em pastas criptografadas com acesso lógico restrito;
- Antes de encaminhar informação confidencial em formato eletrônico, devem ser checados os endereços de destino e observados os requerimentos de segurança necessários;
- Informação confidencial ou sensível em formato eletrônico deve, em caso de manutenção de equipamentos, ser adequadamente protegida contra a perda de integridade e confidencialidade pelo uso de criptografia, backup ou, se for o caso, exclusão irreversível dos dados ou destruição de mídias;
- Informação confidencial em formato eletrônico, impresso ou manuscrito quando requerido seu descarte , deve ser realizado de forma a não poder ser reutilizada ou recuperada (ex.: trituração de papel ou exclusão eletrônica definitiva);
- Informação confidencial em formato eletrônico, impresso ou manuscrito não deve ser disponibilizada a terceiros sem prévia autorização de seu gestor imediato;
- Lembrando que o encaminhamento de informação confidencial deve considerar que pessoas não autorizadas podem ganhar acesso em certas circunstâncias. Informação confidencial em formato impresso ou manuscrito deve ser recolhida, imediatamente, de locais de circulação livre (ex.: salas de reunião e impressão/fax/cópia).

4.2.9. Todos os ativos do GAB devem ser submetidos, anualmente, a um processo de análise e tratamento de riscos pertinente com os critérios estabelecidos.

4.2.10. Mídias, documentação sobre os negócios e equipamentos móveis do GAB devem receber medidas de proteção contra acesso não autorizado, roubo ou dano.

4.2.11. Ao deixar seu ambiente de trabalho, o acesso à sua estação de trabalho deve ser protegido com medidas adequadas:

- Ativação do Screen Saver com proteção por senha;
- Bloqueio de tela (Control+Alt+Del+Enter); ou
- Processo de Log off.

4.2.12. Dispositivos que possam causar riscos à sua estação de trabalho ou notebook não devem ser a estes conectados (ex.: dispositivos USB de armazenamento em massa), salvo se formalmente autorizados.

4.2.13. Todas as estações e servidores devem ter uma ferramenta antivírus instalada e atualizada, não devendo o usuário desinstalar, reconfigurar ou desabilitar a mesma. Da mesma forma:

- Devem estar estabelecidos medidas para assegurar a recuperação de sistemas em caso da ocorrência de vírus (ex.: backup, reinstalação);
- Devem ser usados serviços de fabricantes ou terceiros para manter os sistemas atualizados contra ameaças de vírus;
- Devem tão logo testadas, ser instaladas pelos técnicos administradores as atualizações de segurança para corrigir ocorrências de vírus.

4.2.14. Quanto ao uso de e-mail:

- Antes de usar o software de conversação online com terceiros, o nível de confidencialidade das informações a serem trocadas deve ser considerado;
- No envio de informações através de uma conexão de internet pública, a responsabilidade pelos perigos possíveis é do emissor;
- Para troca de e-mails de trabalho, somente o serviço de e-mail corporativo deve ser usado;
- O serviço de e-mails corporativo deve ser usado em conformidade com a legislação vigente, a Política de Segurança estabelecida e os demais procedimentos do GAB;
- Ao usar o serviço de e-mails corporativo para a comunicação com terceiros, deve ser considerado que esta troca de informações representa o GAB;
- Correntes não devem ser enviadas tampouco instruções contidas em e-mails de origem desconhecida devem ser seguidas;
- A troca de informações confidenciais deve encontrar requerimentos legais estabelecidos;
- A caixa postal corporativa deve ser usada cuidadosamente, inclusive no cadastro para o recebimento de Listas de Discussão.

4.2.15. Quanto ao acesso à internet:

- O acesso à internet deve ser feito conforme regras aplicáveis no GAB e a legislação vigente;
- Devem ser considerados os riscos na transmissão de informação confidencial pela internet;
- O acesso à internet deve ser feito apenas por procedimentos, rotas de acesso e software aprovados pelo GAB.

- Como o acesso a conteúdo na internet não ocorre anonimamente, caso existam boas pistas para suspeitar de abuso, o GAB se reserva o direito de analisar e identificar o acesso conforme os contratos e legislação vigente;
- Captura (download) autorizada de softwares e drivers deve utilizar apenas sites reconhecidamente confiáveis e padrões de mercado. A princípio, apenas, os dos fabricantes e fornecedores pertinentes.
- Captura ou acesso intencional de conteúdo que infrinja a proteção de dados, proteção de privacidade, direitos de cópia ou o código penal vigente é proibido. Assim como a qualquer conteúdo que possa causar quebra dos princípios de segurança. Desta forma, é vetado o uso da internet para captura (download) de softwares, drivers de configuração, arquivos executáveis ou relacionados a jogos, música, vídeo e imagem ou quaisquer que não sejam do interesse do GAB, salvo se devidamente e formalmente autorizados. Está proibido, portanto, o acesso a:
    - Conteúdo pornográfico;
    - Conteúdo relacionado a ferramentas de verificação ou exploração de vulnerabilidades de recursos tecnológicos, salvo se formalmente autorizado;
    - Sites com conteúdo relacionado entretenimento em rede (ex.: jogos), que possam prejudicar o desempenho e disponibilidade dos recursos disponibilizados;
    - Sites externos de redirecionamento de serviços de internet (proxies);
    - Quaisquer sites de serviços públicos de relacionamento ou conversação em tempo real (on-line), salvo se os mesmos forem formalmente autorizados, já que estes provêm falhas de segurança e possibilidades de troca de arquivos e códigos maliciosos. Ex.: Facebook Messenger, Whatsapp, Youtub, twitter, Instagram, etc;

4.2.16. Deve haver um processo sistematizado para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração de sistemas operacionais e outros arquivos críticos pré-definidos.

4.2.17. Todos os registros relacionados ao acesso e uso de sistemas, serviços ou quaisquer outros recursos tecnológicos devem ser armazenados de forma protegida, conforme o nível de classificação estabelecido para as informações relacionadas, além de sujeitos a auditoria.

4.2.18. O GAB se reserva o direito de monitorar e gravar o acesso a quaisquer serviços corporativos (ex.: internet e e-mail), podendo, a qualquer momento e conforme seu exclusivo critério, bloquear tráfego impróprio, ilegal ou não relacionado ao desenvolvimento das atividades profissionais, independentemente de qualquer motivação ou justificativa.

4.3. Gestão de Recursos Humanos

4.3.1. Devem estar documentadas as descrições de cargos e funções, contendo referência as responsabilidades em Segurança da Informação de todos os profissionais a serviço do GAB.

4.3.2. Profissionais, sob qualquer vínculo contratual, a serviço do GAB, em novas funções, seja por admissão ou remanejamento, devem ser comunicados das responsabilidades em Segurança da Informação, como pré-requisito para liberação de uso de recursos e/ou informações.

4.3.3. Para os casos de emergência e/ou ocorrência de incidentes, devem estar definidas e documentadas as responsabilidades em Segurança da Informação.

4.3.4. A Alta Gestão Executiva do GAB deve exigir o cumprimento da sua Política de Segurança da Informação dos profissionais a seu serviço, estando estes sob qualquer vínculo contratual, que, como condição indispensável para a contratação e manutenção de serviços, deve assinar um termo de ciência e compromisso com a Segurança da Informação.

4.3.5. O GAB deve prover meios para disseminar sua Política de Segurança da Informação, capacitando e conscientizando em Segurança da Informação todos os profissionais a seu serviço, estando estes, em caso de descumprimento das regras estabelecidas, passíveis de processo disciplinar.

4.3.6. Quanto ao encerramento definitivo de atividades profissionais, os ativos sob custódia dos profissionais desligados devem ser devolvidos ao GAB, assim como tais profissionais devem ter o acesso a sistemas, serviços e equipamentos descontinuado.

4.4. Segurança do Ambiente

4.4.1. Devem estar, de acordo com sua criticidade, claramente identificados e segregados por barreiras físicas os perímetros de segurança, que devem ser definidos e estabelecidos para conter e proteger informações e os ativos tecnológicos responsáveis pelo processamento, armazenamento e tráfego.

4.4.2. Áreas físicas devem ser submetidas a controle de acesso condizente com o valor e criticidade das informações e ativos mantidos.

4.4.3. O acesso a áreas internas ou privadas do GAB deve ser baseado em, pelo menos, um fator de segurança, o uso e visualização explícita da identificação funcional oficial (crachá) do Grupo.

4.4.4. O processo de entrada e/ou saída de quaisquer pessoas, sob qualquer vínculo com o GAB, incluindo-se empregados, terceirizados ou visitantes, em/de áreas internas ou privativas deve ser controlado e registrado. Empregados ou terceirizados fixos que, por qualquer motivo, estejam sem o crachá oficial do GAB devem ter, mesmo assim, seu acesso à empresa controlado e registrado.

4.4.5. Todas as instalações do GAB devem ter infra-estrutura elétrica adequada, de acordo com as especificações dos fabricantes dos equipamentos e as necessidades dos processos de negócio suportados.

4.4.6. A infra-estrutura elétrica e de dados devem seguir padrões e/ou melhores práticas estabelecidos por normas técnicas reconhecidas, de forma a manter-se a estabilidade e continuidade dos processos de negócio do GAB.

4.4.7. Conexões relacionadas ao cabeamento elétrico, de dados e voz devem estar devidamente identificadas e documentadas, para prover, em caso de incidentes, a reconexão adequada.

4.4.8. Todas as instalações do GAB devem estar protegidas, adequadamente, contra incêndios, alagamentos ou inundações e, desta forma, devem ter dispositivos de contenção e detecção pertinentes para proteger e resguardar os ativos armazenados.

4.4.9. Equipamentos fotográficos, de filmagem ou quaisquer outros desnecessários para operar equipamentos de Tecnologia da Informação não devem ser usados em áreas de armazenamento de ativos críticos (ex.: Data Center), salvo se formalmente autorizados.

4.4.10. Como meio de não causar incidentes aos equipamentos e informações, não deve-se fumar, beber ou comer em áreas de armazenamento de ativos críticos (ex.: Data Center) e, desta forma, os usuários destes ambientes devem ser comunicados explicitamente e conscientizados.

4.4.11. Entrada e, principalmente, saída de material do GAB deve ser rigidamente controlada e formalmente autorizada por profissionais pré-definidos pelo Grupo.

4.5. Gerenciamento das Operações e Comunicações

4.5.1. Os procedimentos operacionais para o funcionamento dos ativos e serviços tecnológicos críticos devem estar documentados e disponíveis aos mantenedores dos mesmos.

4.5.2. Os ambientes computacionais de desenvolvimento, homologação e produção do GAB devem estar em segmentos de rede e equipamentos logicamente e fisicamente isolados.

4.5.3. Deve haver um processo rigoroso para o controle de mudanças nos ambientes computacionais em Produção, em que se avaliem impactos que possam comprometer a segurança da informação e a continuidade dos serviços e negócios do GAB.

4.5.4. A infra-estrutura de rede e sistemas, assim como seus equipamentos e sistemas componentes, devem ser submetidos a monitoração e avaliação periódica de sua capacidade de armazenamento e desempenho de forma a manter-se adequada a novas soluções e/ou a mudanças, garantindo-lhes a continuidade dos negócios, bem como a previsão ou correção de falhas.

4.5.5. Apenas ativos, sejam software ou hardware, homologados pelo Departamento formalmente responsabilizado, devem ser instalados ou conectados a infraestrutura tecnológica do GAB.

4.5.6. Devem ser cumpridos, de acordo com definição formal em documento ou contrato, os acordos de nível de serviço (SLA´s) dos serviços tecnológicos prestados, sejam estes terceirizados ou internos, sobretudo os relacionados a disponibilidade das informações, conforme as necessidades dos usuários pertinentes do GAB.

4.6. Segurança Lógica

4.6.1. Os controles para a segurança da informação devem considerar o valor, sensibilidade e criticidade das informações relacionadas para os objetivos de negócio do GAB.

4.6.2. Dados, informações e sistemas de informação do GAB ou sob sua custódia, devem ser protegidos contra acessos e ações não autorizados, sejam estas intencionais ou acidentais, reduzindo riscos e garantindo a preservação da confidencialidade, integridade e disponibilidade dos mesmos.

4.6.3. Violações de segurança devem ser registradas e seus registros analisados, periodicamente, seja com o objetivo corretivo, legal ou de auditoria.

4.6.4. Deve existir um processo rigoroso de controle de acesso aos sistemas, serviços e equipamentos, de forma que apenas usuários ou processos formalmente autorizados sejam permitidos, sendo os responsáveis pela autorização claramente definidos e documentados

4.6.5. No processo de solicitação e concessão formal de privilégios de acesso lógico, devem constar informações sobre o solicitante, incluindo-se autorizador, atividades, projetos ou funções relacionados, período de concessão e justificativa, a serem devidamente registradas para fins de documentação e auditoria.

4.6.6. Identificações para acesso aos equipamentos, sistemas e serviços do GAB (ex.: id´s, usuários, etc) devem ser pessoais, únicas e intransferíveis, além de autenticadas por, pelo menos, um fator de segurança (ex: senhas).

4.6.7. O acesso lógico de todos os usuários, inclusive de nível privilegiado, deve ser registrado e analisado, periodicamente, sendo o tempo de retenção destes registros (logs) e as medidas de proteção relacionadas definidas e documentadas.

4.7. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

4.7.1. O GAB é a única proprietária dos sistemas por ela adquiridos ou desenvolvidos por profissionais a seu serviço, seja em ambiente interno ou externo, sejam estes funcionários ou prestadores de serviços, sendo, por conseguinte, os códigos-fonte relacionados pertencentes a mesma, assim como os direitos de uso e propriedade.

4.7.2. Antes de adquiridos, desenvolvidos ou implementados no ambiente de Produção, os sistemas devem ser avaliados com relação a suas vulnerabilidades de segurança.

4.7.3. Devem ser criados arquivos de controle que permitam detectar e verificar a integridade dos sistemas, baseado em qualquer irregularidade na entrada, processamento e saída de dados dos mesmos.

4.7.4. Os sistemas devem estar preparados para:

- Evitar conexões simultâneas para uma única conta de usuário;
- Desconectar usuários por tempo de inatividade;
- Vincular perfis somente a grupos de usuários.

4.7.5. Sistemas devem ser desenvolvidos em módulos e seus desenvolvedores devem ter acesso somente aos fontes necessários à execução do seu módulo e trabalho pertinente.

4.7.6. Sistemas devem possuir níveis de privilégio de acesso adequados a segregação de funções pré-definida, restringindo-se o acesso privilegiado máximo ao imprescindível e segmentando-o em funções específicas. (ex.: administrador, operador de usuários, operador de backup).

4.7.7. Sistemas devem prover cadastros de usuários que possam registrar, ao menos:

- Nome completo e conta de usuário;
- Data de criação e bloqueio (se for o caso) da conta de usuário;
- Data da última atualização de dados cadastrais do usuário;

- Usuário que atualizou os dados cadastrais.

4.7.8. Os sistemas devem estar preparados para gerar trilhas de auditoria indicando quem o acessou e com que perfil, a data, a hora, a identificação dos registros modificados e, consequentemente, da informação modificada.

4.7.9. Os dados de entrada devem ser rigidamente validados pelo sistema para evitar que controles mal intencionados sejam implementados para burlar o acesso aos dados do sistema.

4.7.10. Se o processo de classificação exigir, informações de nível privilegiado devem ser armazenadas na forma criptografada, conforme as melhores práticas de mercado (ex.; RSA ou 3DES).

4.8. Continuidade de Negócios

4.8.1. Em caso de incidentes que comprometa a disponibilidade de processos e informações críticas, deve ser previsto e planejado a implementação de contramedidas, como o backup periódico das informações de negócio, para garantir a continuidade da operação dos negócios do GAB.

4.9. Gestão de Incidentes

4.9.1. Usuários devem relatar, exclusivamente pelos canais formalmente estabelecidos, quaisquer incidentes de segurança presenciados ou mesmo suspeitos, inclusive evasão, perda ou roubo de ativos ou informações a Área de Gestão de Segurança da Informação.

4.9.2. A estrutura de suporte local deve estar em conformidade com os requisitos de negócio do GAB (ex.: Disponibilidade baseada nos dias e horas de trabalho pré-definidos).

4.10. Conformidade e Legalidade

4.10.1. Quaisquer requisitos contratuais, regulamentares e legais dos sistemas GAB devem ser definidos, documentados e cumpridos.

4.10.2. Quanto ao uso de dados pessoais:

- Deve ser assegurado proteção e sigilo aos dados pessoais ou privados relacionados aos clientes ou profissionais a serviço do GAB, conforme definido em cláusulas contratuais.
- A coleta de dados só é permitida se houver razão legal, contratual ou outra explícita e formalizada para tal.
- Dados pessoais devem ser processados somente dentro de limites específicos e estabelecidos formalmente.
- O processamento de dados deve ser mantido anônimo e em proporção mínima, tanto quanto possível.

4.10.3. O GAB se reserva o direito de monitorar e auditar a conformidade com a Política de Segurança da Informação, procedimentos e a legislação estabelecidas.

4.11. Infrações e Punições

4.11.1. Infrações contra esta Política de Segurança da Informação devem ser enquadradas e classificadas de acordo com sua gravidade, estando sujeitas a imputação de sanções administrativas inclusive que possam culminar em demissão por justa causa, penais e civis, conforme o caso.

4.11.2. É considerada falta grave tanto não cumprir esta Política de Segurança da Informação quanto tentar interferir, obstruir ou dissuadir profissionais a serviço do GAB a agir de acordo com ela ou a reportar incidentes de Segurança da Informação.

5. Anexos

Não aplicável.

6. Controle de Versões

Versão	Descrição	Data
001	Criação da Política de Segurança da Informação	31/08/2018
002	Alteração dos itens: 1; 3.2., 4.1.2., 4.1.3., 4.2.4., 4.2.6., 4.2.8., 4.2.14, 4.2.15, 4.3.4., 4.4.5, 4.9.1. e 4.11.1	21/09/2018