REGULAMENTO DO PROGRAMA TORNEIRA LAB *STARTUPS*

1. SOBRE O PROGRAMA

1.1. O Programa denominado "Torneira Lab *Startups*" é promovido pela Saneamento Ambiental Águas do Brasil S.A., sociedade com sede na Rua Marquês do Paraná, n° 110, parte, Centro, Niterói, Rio de Janeiro, inscrita no CNPJ nº 09.266.129/0001-10, denominada "Organizadora" ou simplesmente "Cliente", em parceria com a empresa Innoscience Consultoria em Gestão da Inovação Ltda., sociedade com sede na AL Vicente Pinzon 54, 7º andar - Vila Olímpia - CEP: 04547-130, inscrita no CNPJ sob o nº 11.255.538/0001-63, denominada "Innoscience", sendo Organizadora ou Cliente, em conjunto com a Innoscience, denominadas "Partes".

1.2. O "Torneira Lab *Startups*" é um programa voluntário de conexão e criação de novos negócios com *startups* brasileiras em nível avançado de qualquer segmento, com produto e modelo de negócios com grande possibilidade de crescimento ("Programa").

1.3. Constituem objetivos do Programa: ***(i***) gerar eficiência operacional: capturar ganhos de economia, produtividade e novas oportunidades; ***(ii)*** cocriar projetos em parcerias com *startups*; ***(iii)*** fortalecer e fomentar a reputação de liderança da Cliente no ecossistema de inovação brasileiro; e ***(iv)*** promover a cultura de inovação na Cliente.

1.4. Não será prevista qualquer modalidade de prêmio ou pagamento aos participantes, não se comprometendo, a Cliente, com qualquer tipo de investimento ou incentivo, nem tampouco obrigação em contratar quaisquer das *startups* participantes.

1.5. Como critério de seleção, o Programa irá priorizar inscrições de projetos enquadrados em cada um dos seguintes itens:

a) Maturidade da *Startup*
a.1) Scale-ups e *startups* que apresentem crescimento rápido e consistente; e
a.2) Tração e vendas recorrentes.

b) Solução e Modelo de Negócios

b.1) Solução pronta ou apta a um co-desenvolvimento;
b.2) Resolvam os desafios estabelecidos pelo Torneira Lab *Startups*;
b.3) Possuam um modelo de negócio escalável; e
b.4) Podem ter destaques com relação a impacto social (adicional).

c) Perfil dos Sócios

c.1) Ao menos dois(duas) sócios(as) com dedicação exclusiva;
c.2) Batch com diversidade geográfica.

Que se enquadrem e busquem solucionar os Desafios:

Desafio 1: Gestão inteligente de redes de abastecimento de água;
Desafio 2: Monitoramento para detecção ágil de vazamentos não visíveis;
Desafio 3: Predição de falhas em bombas com uso de dados operacionais;
Desafio 4: Gestão eficiente de sensores online para monitoramento da qualidade da água;
Desafio 5: Medição Inteligente com análise de dados para gestão eficiente de água;
Desafio 6: Otimização do consumo energético em operações de tratamento.

2. DOS PARTICIPANTES

(i) Podem se inscrever no Programa *startups* cujo nível de desenvolvimento esteja em estágio de tração ou escala com produto e modelo de negócios com grande possibilidade de crescimento.
(ii) As *startups* devem ser pessoas jurídicas: possuir cadastro ativo na Receita Federal com inscrição no Cadastro Nacional de Pessoa Jurídica e os seus sócios e colaboradores devem ser maiores de 18 (dezoito) anos na data de inscrição.
(iii) Não serão aceitas inscrições de empresas/*startups* que tenham membros empregados ou estagiários da Cliente ou Innoscience.
(iv) A *startup*, ao efetuar sua inscrição, receberá o convite para cadastramento na Plataforma Nimbi, devendo anexar os documentos e declarações que forem necessários para a conclusão do cadastro.

3. DA PARTICIPAÇÃO

3.1. A participação no Programa é voluntária.

3.2. Os participantes deverão se inscrever no Programa por meio do preenchimento do formulário de inscrição, presente no link https://torneiralab.com.br durante o período de inscrição impreterivelmente, e seguir os passos mencionados na página.

3.3. A participação neste Programa implica na aceitação irrestrita deste Regulamento. Ao confirmar a participação neste Programa, o participante autoriza a utilização de seu e-mail para fins de recebimento de comunicação de atualização do programa durante o período do mesmo e para contatos necessários posteriormente.

3.4. O Torneira Lab *Startups* não se responsabiliza por inscrições que não sejam computadas por problemas técnicos que ocorram na transmissão dos dados.

3.5. O Torneira Lab *Startups* se reserva o direito de recusar a inscrição de qualquer *startup* que não reúna os requisitos descritos neste Regulamento, no formulário de inscrição, no perfil desejado elencado nos temas do item 1.5 deste Regulamento e que não cumpra com os termos de participação.

4. DIRETRIZES GERAIS:

4.1. O não cumprimento dos prazos estipulados pela organização do Torneira Lab *Startups* para a entrega dos documentos requeridos em cada etapa possibilitará a eliminação do Programa, a critério exclusivo da organização do Torneira Lab *Startups*.

4.2. Serão motivos para eliminação do Torneira Lab *Startups*, a exclusivo critério da Cliente, as seguintes situações, entre outras: ***(i)*** descomprometimento com as iniciativas do Programa; ***(ii)*** não comparecimento aos eventos; ***(iii)*** apresentação de qualquer informação incorreta, alterada ou em descumprimento com o Regulamento ou ***(iv)*** cujo projeto não esteja de acordo com o Regulamento; ***(v)*** incompatibilidade com o perfil do Programa, ***(vi)*** conduta inadequada, de acordo com os valores da Torneira Lab *Startups* ou da Cliente presentes neste Regulamento, ***(vii)*** avaliação de riscos após *due diligence* de integridade, que será realizada em paralelo com o cadastramento na Plataforma Nimbi.

4.3. No entanto, o Torneira Lab *Startups* reserva-se o direito de convidar e selecionar *startups* para apresentar-se no *Pitch Day*, mesmo não havendo realizado a inscrição prévia no site https://torneiralab.com.br.

5. DA COLABORAÇÃO PARA MÍDIA E DIREITO DE IMAGEM

5.1. Os participantes, desde já, autorizam, de forma gratuita, a captação e fixação da sua imagem, nome, voz e outros dados pessoais, incluindo, mas não se limitando, entrevistas e vídeos, mediante uso, fruição, reprodução e disposição da sua participação no Programa, à Cliente e à Innoscience, para publicação, reprodução, transmissão com ou sem fio, emissão, retransmissão, distribuição, comunicação ao público, edição, adaptação e outras transformações, uso por representação, execução, sonorização, captação, radiodifusão e outros meios de comunicação, mediante o emprego de qualquer tecnologia (analógica, digital, com ou sem fio e outras), inclusão em base de dados, armazenamento em quaisquer meios de fixação, digitalização, divulgação e quaisquer outras modalidades de utilização existentes ou que venham a ser inventadas, em quaisquer meios e suportes existentes ou que venham a ser inventados, próprios e/ou de terceiros,

dentro e fora do território nacional, por número ilimitado de vezes e por tempo indeterminado com a finalidade de divulgação do Programa e resultados obtidos.

6. DAS FASES DO PROGRAMA

6.1. O Programa Torneira Lab *Startups* está divido em 5 (cinco) fases, abaixo descritas em formato 100% online:

1ª Fase – *Scouting*: Fase de inscrição de *startups* com avaliação de acordo com os critérios de seleção descritos neste Regulamento. Serão selecionadas *startups* para a fase 2.

2ª Fase – Filtro: Etapa que contará com duas fases, com eventos remotos e obrigatórios:

1. Pitch Reverso: Momento de apresentação detalhada do desafio pelos sponsors e pela área de inovação do Grupo Águas do Brasil para as startups selecionadas para o Pitch Day.
2. Pitch Day: Momento em que as startups irão apresentar suas soluções aos executivos da empresa e outros parceiros. Após as apresentações, os executivos irão decidir quais participarão da fase 3.

3ª Fase – Imersão: Evento remoto e obrigatório de 2 (dois) dias em conjunto com a área da Cliente mais adequada para a solução da startup participante, para a cocriação de pilotos com a Cliente. As propostas aprovadas pela Cliente ao final da Imersão, participarão da fase 4.

4ª Fase – Piloto: Fase de execução dos projetos piloto aplicados à cadeia de parceiros da Cliente, com a gestão e apoio direto de representantes da *startup* e da Cliente.

5ª Fase – Resultado final/*Rollout*: Ao final da "4ª Fase – Piloto", a critério exclusivo da Cliente, as Partes poderão dar continuidade a sua relação comercial por meio de parceria estratégica estabelecida em comum acordo.

7. CRONOGRAMA

7.1. O Programa seguirá o cronograma abaixo descrito:

- Inscrições – abertura no dia 22/04/2026 até o dia 08/05/2026.
- Pitch Reverso: maio/2026.
- Divulgação das startups selecionadas para o Pitch Day – em maio/2026.
- Pitch Day – em maio/2026, em formato remoto.
- Divulgação das startups selecionadas para Imersão – em junho/2026.
- Imersão – Em junho/2026, em formato remoto.
- Apresentação das Propostas de Piloto – Em junho/2026, em formato remoto.

- Divulgação das startups selecionadas para Piloto – em junho/2026.
- Período de contratação e setup dos pilotos – julho/2026.
- Período de desenvolvimento e execução do piloto – agosto/2026 até novembro/2026.
- Apresentação dos resultados do Piloto – Em dezembro/2026, em formato remoto.

7.2 As datas descritas acima estão passíveis a alterações de acordo com o cronograma e andamento do programa. Em casos de alterações, todos os participantes serão previamente comunicados.

8. DO PERÍODO DE VIGÊNCIA

8.1. O presente Programa vigorará de janeiro/2026 até dezembro/2026. O Programa poderá, eventualmente, ser prorrogado ou passar por alterações por decisão exclusiva da Cliente.

9. DA PROPRIEDADE INTELECTUAL

9.1. Os participantes declaram que a solução apresentada no Programa é única e exclusivamente sua, e que a mesma não viola direitos de terceiros, sendo que na hipótese de violação, os participantes se responsabilizam em tomar as devidas providências para excluir a Cliente e a Innoscience de quaisquer reclamações ou ações, ressarcindo todo e qualquer valor a ser gasto pela Cliente e, eventualmente, Innoscience, incluindo custas, despesas e honorários advocatícios e contratuais. Qualquer solução que viole a propriedade de terceiros ou que manifeste conteúdo impróprio será automaticamente desclassificada, assim como qualquer solução que sugira ou encoraje atividade ilegal ou divulgação de informações que não possam ser transmitidas por motivos legais ou contratuais.

10. DA PROTEÇÃO DE DADOS PESSOAIS

10.1. Os participantes obrigam-se, perante a Cliente, a tratar os dados pessoais obtidos em decorrência deste Regulamento, que por ventura tenham acesso, de acordo com as exigências aqui previstas e em observação à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. Os participantes deverão tratar os dados pessoais a que tiverem acesso para a exclusiva finalidade de participação no Programa, devendo garantir que tais dados pessoais não serão tratados para quaisquer outras atividades e que nenhum dado pessoal desnecessário será tratado.

10.2. Os participantes garantem que para a realização do tratamento dos dados pessoais que venham a ter acesso, utilizarão os sistemas e tecnologia necessários para assegurar a coleta/tratamento seguro das informações.

10.3. Encerrada a participação das startups neste Programa, decorrente deste Regulamento e/ou cumprida a finalidade para a qual os dados pessoais foram coletados, os participantes obrigam-se a exclui-los, bem como todas as suas eventuais cópias.

10.4. Em caso de incidentes de segurança envolvendo dados pessoais relacionados a este Regulamento, os participantes obrigam-se, perante a Cliente e à Innoscience, a informar em menos de 24 (vinte e quatro) horas da ciência sobre o ocorrido todas as informações que possuírem sobre o incidente, incluindo as medidas já tomadas para mitigação de riscos, bem como indenizar e reembolsar e a todo o tempo manter a Cliente e a Innoscience - inclusive na capacidade de sucessoras ou corresponsáveis - indenes contra todos de quaisquer perdas, danos ou demandas judiciais ou administrativas, incorridas ou sofridas em decorrência ou em razão de qualquer violação às obrigações de proteção de dados pessoais previstas neste Regulamento e na legislação aplicável, em especial na Lei nº 13.709/2018.

10.5. Os participantes estão cientes que a Cliente e a Innoscience poderão tratar dados pessoais de seus colaboradores, sócios, representantes e/ou diretores, entre outros terceiros relacionados à *startup*, visando:

(i) Executar o Programa e cumprir o Regulamento;
(ii) Executar outros contratos e instrumentos que possam vir a ser celebrados com os participantes do Programa;
(iii) Cumprir com obrigações legais ou regulatórias da Cliente e/ou da Innoscience;
(iv) Defender os interesses da Cliente e/ou da Innoscience perante os participantes ou terceiros, em procedimentos administrativos, judiciais ou extrajudiciais;
(v) Enviar aos participantes notícias, informações e outras comunicações comerciais relevantes sobre os produtos e serviços da Cliente e da Innoscience, podendo tais comunicações serem interrompidas pelo *opt-out* disponibilizado na própria mensagem, ainda que após encerramento do Programa.

10.6. A Cliente e a Innoscience poderão armazenar os dados pessoais relacionados à *startup* advindos deste Regulamento e do Programa pelo período necessário para desempenhar as finalidades aqui previstas.

10.7. Os participantes declaram ciência e concordância com as Boas Práticas de Proteção de Dados Pessoais descritas no link https://www.grupoaguasdobrasil.com.br/politica-de-privacidade/.

11. DA CONFIDENCIALIDADE

11.1. Aos participantes, fica expressamente proibido divulgar, fornecer ou tornar disponíveis quaisquer informações, dados ou trabalhos, exclusivos ou confidenciais relativos ou criados em conjunto durante Programa, não podendo sob qualquer pretexto, utilizar ou dar conhecimento a terceiros estranhos.

11.2. A Cliente e a Innoscience tratarão as soluções comerciais de forma confidencial e também não divulgarão ou tornarão disponíveis as informações, dados e trabalhos do Programa.

11.2.1. Serão consideradas Informações Confidenciais:

(i) informações por escrito, contidas em arquivos eletrônicos ou verbalmente transmitidas, obtidas em reuniões com a Cliente, Innoscience, parceiros e outras partes envolvidas no projeto e no Programa, incluindo documentos, relatórios, arquivos; informações derivadas, decorrentes ou relacionadas às Informações Confidenciais, recebidas na forma desta Cláusula; e informações de terceiros, sujeitas a dever de sigilo por sua parte; ou

(ii) informações econômico-financeiras a respeito das atividades da Cliente e/ou suas Afiliadas ou das empresas participantes, como Balanço Patrimonial, Balancetes Mensais, Mapa de Endividamento, Faturamento Previsto, informações eventualmente fornecidas sobre seus produtos, empregados, planos de negócio ou de operações, e outras informações financeiras; ou

(iii) toda e qualquer informação referente à Cliente, seus clientes, empresas controladas, controladoras ou sociedades sob controle comum ("Afiliadas"), bem como a todas as empresas que compõem o grupo econômico, bem como aos seus respectivos negócios, incluindo-se, mas sem limitação a estes itens, os segredos comerciais e/ou informações financeiras, operacionais, econômicas, técnicas, jurídicas, planos e planejamentos de negócios, projetos, marketing, *know-how*, informações comerciais e/ou relacionadas a clientes, planos comerciais, atividades promocionais, tecnologia (tais como: sistemas, acessos, simuladores tipo GTM – *Go To Market*, etc.), além de outros negócios que, de modo geral, sejam restritos, internos e de desconhecimento público.

11.2.2. As obrigações assumidas nesta Cláusula 11 subsistirão pelo prazo de 5 (cinco) anos contados do término das negociações objeto deste Regulamento ou celebração de contrato de prestação de serviços a ser celebrado entre as Partes, o que ocorrer primeiro.

12. DA SELEÇÃO DE PROJETOS

12.1. O processo de seleção do Programa Torneira Lab *Startups* seguirá os seguintes critérios, a serem filtrados e avaliados pelo corpo técnico da Cliente:

Filtro 1 – Seleção de *startups* para o Pitch Reverso e *Pitch Day*:

I- Maturidade da *startup*.
- Fase de tração/escala;
- Vendas recorrentes.

II- Match com o desafio
- Conexão da solução com o desafio;
- Capacidade de resolver um problema real.

III- Solução e Modelo de Negócio.
- Solução pronta;
- Capacidade de resolver um problema real;
- Modelo de negócio escalável.

Filtro 2 – Seleção de *startups* para a imersão:

I- Características da oportunidade / novo negócio com a Cliente.
- Potencial de geração de resultados;
- Facilidade de implementação;
- Nível de inovação.

II- Adequações Legais.

III- Potencial Tecnológico.

IV- Fit com a Cliente.
- Interesse da Cliente na oportunidade identificada / proposta;
- Disponibilidade de potenciais *sponsors* e times;
- Perfil dos empreendedores.

Filtro 3 – Seleção de *startups* para o piloto:
- Aderência entre as partes
- Nível de risco
- Valor do investimento para o piloto

- Potencial de ganho dos resultados

Filtro 4 – Seleção de *startups* para *rollout*:

- Avaliação do piloto
- Relacionamento com a *startup*
- Potencial de escalabilidade
- Projeção dos resultados

A *Startup* deverá participar dos processos via portal de compras e realizar uma manutenção periódica do cadastro uma vez que se encontre nessa fase.

13. DO ATENDIMENTO ÀS STARTUPS

13.1. Todos as *startups* que precisarem de atendimento poderão entrar em contato com a equipe organizadora do Torneira Lab *Startups* pelo e-mail carolina.zanini@innoscience.com.br ou luciana.madeira@innoscience.com.br.

14. DA ALTERAÇÃO NO REGULAMENTO

14.1. A Organizadora do Torneira Lab *Startups* poderá, a qualquer momento, realizar alterações no presente Regulamento, caso entenda necessário. As alterações no Regulamento serão comunicadas aos participantes por e-mail.

15. DAS OBRIGAÇÕES LEGAIS E ÉTICAS

15.1. Os participantes comprometem-se a não adotar, sob qualquer hipótese, quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 (conforme alterada), do Decreto nº 8.420/2015 (revogado pelo Decreto n.º 11.129 de 11 de Julho de 2022 (conforme alterado), do U.S. *Foreign Corrupt Practices Act* de 1977 (conforme alterado) ou de quaisquer outras leis ou Regulamentos aplicáveis ("Leis Anticorrupção"), ainda que não relacionadas com o presente Regulamento, sob pena de eliminação, em qualquer fase do Programa, bem como adoção das medidas cabíveis.

15.2. Os participantes também se comprometem a fornecer todas as informações requeridas pela Cliente para fins de *due diligence* e avaliação de Compliance.

15.3. Sem prejuízo do disposto na cláusula anterior, os Participantes declaram que tem conhecimento que a Cliente possui políticas e procedimentos internos que têm como objetivo garantir o cumprimento dos compromissos legais e éticos por ela assumidos,

dentre os quais está incluído o Código de Conduta Ética do Grupo Águas do Brasil, que pode ser consultado a qualquer momento pelo Participante, caso assim o deseje. Os Participantes cumprirão e se responsabilizarão por si e pelo cumprimento por seus sócios e todos os seus membros do conselho, diretores, empregados, trabalhadores, prepostos e/ou representantes (“Integrantes"), durante todo o período de vigência deste Regulamento.

15.3.1. A atuação dos Participantes com os Integrantes, clientes, fornecedores, órgãos públicos e privados, e com todos aqueles com quem mantiver relacionamento profissional será pautada em valores éticos, respeito à lei, boa-fé, transparência e cordialidade.

15.3.2. As atividades desempenhadas pelos Agentes Públicos não devem ser dificultadas, impedidas, perturbadas ou importunadas pelos Integrantes dos Participantes.

15.3.3. Os Participantes não praticarão e adotarão medidas para combater o assédio moral e sexual, trabalho infantil, trabalho forçado, compulsório ou em condições degradantes nos seus estabelecimentos, garantindo e respeitando os direitos individuais, coletivos e trabalhistas dos Integrantes.

15.3.4. Os Participantes valorizarão a saúde e segurança de seus Integrantes no ambiente de trabalho e respeitará o meio ambiente, observando a legislação ambiental aplicável às suas atividades.

15.3.5. Os Participantes não praticarão e adotarão medidas para combater a prática de ato de corrupção, principalmente a oferta, entrega ou promessa, direta ou indireta, de vantagem indevida (tais como dinheiro, favores, presentes e viagens) a Agente Público ou a terceira pessoa a ele relacionada.

15.3.6. Os Participantes não adotarão práticas consideradas como infração à ordem econômica, tais como ajustes para divisão de mercados ou clientes ou ajustes de preços.

15.3.7. Os Participantes manterão de forma precisa e detalhada seus registros comerciais e contábeis, bem como o sigilo das informações confidenciais da Cliente das quais venha a ter conhecimento.

15.4. Para fins deste Regulamento, na forma do artigo 2° da Lei n° 8.429/92, é “Agente Público” todo sujeito que exerça, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função na administração direta, indireta ou fundacional de qualquer dos Poderes da União, dos Estados, do Distrito Federal, dos Municípios, de Território, de empresa incorporada ao patrimônio público ou de entidade

para cuja criação ou custeio o erário haja concorrido ou concorra com mais de cinquenta por cento do patrimônio ou da receita anual. A presente definição também abrange qualquer dirigente de partido político, seus empregados ou outras pessoas que atuem para ou em nome de um partido político ou candidato a cargo público, bem como a definição de agente público estrangeiro contida no art. 5º, § 3º, da Lei n.º 12.846/2013. 15.5 Para fins deste Regulamento, o termo "Autoridade Governamental" significa qualquer órgão, entidade, autoridade, agência, autarquia, fundação, comissão ou repartição governamental brasileira, de qualquer nível ou esfera de governo (federal, estadual, municipal, regional, distrital ou local), ou, ainda, qualquer pessoa jurídica controlada, direta ou indiretamente, pelo poder público brasileiro, ou órgão, entidade estatal ou representação diplomática de país estrangeiro, de qualquer nível ou esfera de governo, bem como qualquer pessoa jurídica controlada, direta ou indiretamente.

15.5. Os participantes declaram ciência e concordância com a Política de Segurança da Informação da Cliente, conforme Anexo [1], comprometendo-se a cumprir integralmente suas diretrizes durante toda a vigência do Programa.

16. DISPOSIÇÕES GERAIS

16.1. Surgindo divergências quanto à interpretação do presente Regulamento ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, o corpo técnico do Torneira Lab *Startups*, responsável pelo programa, solucionará tais divergências, de acordo com os princípios de boa-fé, da equidade e da razoabilidade.

16.2. Os participantes concordam que não deverão, sem o consentimento prévio e escrito da Cliente, usar os nomes e marcas Torneira Lab *Startups* e Cliente ou qualquer outra marca de propriedade da Cliente para fins de publicidade própria ou para qualquer outra finalidade, notadamente em placas, folders, panfletos publicitários, portfólios ou quaisquer outros materiais de divulgação, sob pena de eliminação da sua participação no projeto, além da adoção das medidas judiciais cabíveis.

ANEXO 1 - Política de Segurança da Informação da Cliente

POL.CORP.TI.0001 - Política Geral
Próxima Revisão: 16/07/2026 **Revisão: 2**

1. OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores e parceiros do Grupo Águas do Brasil (GAB) 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 GAB.

3. CONTEÚDO GERAL

3.1. Siglas

DLP – *Data Loss Prevention*

GAB – Grupo Águas do Brasil

ISO – Organização Internacional de Padronização

LGPD – Lei Geral de Proteção de Dados Pessoais

PSI – Política de Segurança da Informação

SGSI – Sistema de Gestão de Segurança da Informação

SLA – *Service Level Agreement*

TI – Tecnologia da Informação

VPN – *Virtual Private Network*

3.2. Definições

– **Alta Direção**: grupo de pessoas que representam o mais alto nível da hierarquia do GAB.

- **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em prejuízo ao sistema ou organização.
- **Autenticação**: provisão de garantia que uma característica alegada por uma entidade está correta.
- **Controle de Acesso**: meios para assegurar que o acesso aos bens é autorizado e limitado baseado nos requisitos de segurança e do negócio.
- **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.
- **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.
- **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.
- **Informação Sigilosa**: informação sigilosa na qual o acesso é restrito por lei ou regulamentos internos do GAB a classes específicas de pessoas.
- **Segurança da Informação**: preservação de confidencialidade, integridade e disponibilidade da informação.
- **Validação**: confirmação, através de evidência objetiva, que os requerimentos para uma utilização ou aplicação desejada específica foram cumpridos (ABNT NBR ISO 9000).
- **Verificação**: confirmação, através da disponibilização de evidência objetiva, que requerimentos especificados foram cumpridos (ABNT NBR ISO 9000).
- **Vulnerabilidade**: fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças.

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 protegê-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 ABNT NBR ISO/IEC 27001 e ABNT NBR 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;
- Manter sigilo sobre seu *login* e senha.

4.2. Gestão e Uso de Ativos

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.

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.

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 corporativos.

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.

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

4.2.1. 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.

4.2.2. 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.

4.2.3. 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).

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

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

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

4.2.7. 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.

4.2.8. 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.

4.2.9. 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.

4.2.10. 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 (*online*), 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, YouTube, Twitter, Instagram, etc;

4.2.11. 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.

4.2.12. 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.

4.2.13. 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.

4.2.14. Gestão de Recursos Humanos 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.

4.2.15. 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.

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

4.2.17. 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.

4.2.18. 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.

4.2.19. 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.

4.3. Segurança do Ambiente

4.3.1. 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.

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

4.3.3. 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 GAB.

4.3.4. 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.

4.3.5. Todas as instalações do GAB devem ter infraestrutura elétrica adequada, de acordo com as especificações dos fabricantes dos equipamentos e as necessidades dos processos de negócio suportados.

4.3.6. A infraestrutura 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.

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

4.3.8. 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.

4.3.9. 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.

4.3.10. Como meio de não causar incidentes aos equipamentos e informações, não se deve 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.

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

4.4. Gerenciamento das Operações e Comunicações

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

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

4.4.3. 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.

4.4.4. A infraestrutura 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.

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

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

4.5. Segurança Lógica

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

4.5.2. 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 deles.

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

4.5.4. 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

4.5.5. 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 relacionadas, período de concessão e justificativa, a serem devidamente registradas para fins de documentação e auditoria.

4.5.6. 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).

4.5.7. 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.

4.6. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

4.6.1. 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.

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

4.6.3. 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 deles.

4.6.4. 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.

4.6.5. Sistemas devem ser desenvolvidos em módulos e seus desenvolvedores devem ter acesso somente às fontes necessárias à execução do seu módulo e trabalho pertinente.

4.6.6. 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*).

4.6.7. 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.

4.6.8. 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.

4.6.9. 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.

4.6.10. Se o processo de classificação exigir, informações de nível privilegiado devem ser armazenadas na forma criptografada, conforme as melhores práticas de mercado.

4.7. Continuidade de Negócios

4.7.1. 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.

4.8. Gestão de Incidentes

4.8.1. 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.

4.8.2. 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).

4.9. Conformidade e Legalidade

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

4.9.2. 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.

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

4.10. Gestão de Mudanças de TI

Todas as modificações que envolvem os ativos de tecnologia da informação das áreas de infraestrutura e sistemas do GAB devem obrigatoriamente seguir o padrão de abertura de Gestão de Mudanças para fins de comunicação e fluxo de aprovação.

4.11. Classificação da Informação

Toda informação do GAB deve ser classificada pelo proprietário da informação. As informações classificadas devem ser manuseadas de acordo com as regras definidas pela equipe de Segurança da Informação.

4.12. Controle de Acesso Remoto e VPN

O GAB deve garantir o controle de acesso remoto e VPN a serviços disponibilizados nos servidores, a fim de manter a segurança e a disponibilidade ofertado aos usuários.

4.13. Controle e Especificações sobre *Datacenter*

Todo *Datacenter* do GAB deve seguir boas práticas de mercado em relação à segurança física, buscando ter diretrizes para controles de acesso e monitoramento.

4.14. Gerenciamento de Ativos

Os recursos ou serviços corporativos, providos pelo GAB, devem ser usados apenas para desenvolvimento das atividades profissionais, sendo cada um dos funcionários desta empresa corresponsável pela implementação das regras de segurança estabelecidas.

Todos os funcionários e prestadores de serviços que utilizam ativos do GAB devem ser conscientizados sobre o uso aceitável destes ativos considerando os aspectos de Segurança da Informação.

4.15. Gestão de Incidentes de Segurança de Informação

Os envolvidos pela gestão de incidentes de segurança da informação devem ser capacitados para responder aos incidentes por meio de programa de treinamento.

4.16. Gestão e Recuperação de Desastre

O GAB precisa estar apto a se recuperar de um desastre, com regras claras contendo conjunto de políticas e procedimentos para suportar a recuperação do processamento dos sistemas críticos na eventualidade de um incidente que comprometa sua operação no datacenter do GAB. O Plano de Recuperação de Desastres deve ser testado e atualizado, no mínimo, uma vez por ano ou quando mudanças significativas ocorrerem no ambiente.

4.17. Gestão de Segurança e Privacidade em Prestadores de Serviços

O GAB define diretrizes de gestão de segurança da informação e privacidade de prestadores de serviços assegurando a qualidade e segurança no manuseio e armazenamento de informações/dados pessoais do GAB.

4.18. Uso das Ferramentas de Colaboração

As ferramentas de colaboração devem ser utilizadas em conformidade com as normas e procedimentos definidos pelo GAB.

4.19. Uso seguro de Dispositivos Móveis

Todos os funcionários, estagiários e terceiros que utilizam dispositivos móveis com informações do GAB e de suas concessionárias, devem seguir os critérios de segurança estabelecidos pela área de Segurança da Informação sobre uso seguro de dispositivos móveis.

4.20. Gestão de *Backup*

A área de Tecnologia da Informação deve estabelecer regras de *backup* e *restore*, visando garantir confidencialidade, integridade, disponibilidade e privacidade das informações em caso de necessidade de uso das cópias de segurança.

4.21. Ciclo de Vida da Informação e Dados Pessoais

A área de Tecnologia da Informação segue diretrizes de ciclo de vida da informação / dados pessoais, levando em consideração a coleta, tratamento/processamento, compartilhamento, armazenamento e descarte das informações / dados pessoais do GAB.

Toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração deve seguir as diretrizes estabelecidas pela equipe de Segurança da Informação.

4.22. Ciclo de Vida de Projetos

A área de tecnologia da informação estabelece diretrizes associadas ao gerenciamento de projeto de desenvolvimento de sistemas e tem por objetivo servir de instrumento de apoio na criação, condução e acompanhamento de projetos no GAB.

4.23. Rastreabilidade, *Log* e Registros

A área de tecnologia da informação deve estabelecer regras de monitoramento, análise de *log* e eventos dos recursos de processamento da informação do GAB.

Os sistemas devem ser monitorados e seus *logs* mantidos para verificação das atividades executadas.

4.24. Descarte de Equipamentos

A área de Tecnologia da Informação junto com a área responsável por Patrimônio, estabelece diretrizes para descarte e destruição seguro de equipamentos e informações do GAB.

4.25. DLP (*Data Loss Prevention*)

A área de tecnologia estabelece diretrizes para a prevenção e perda de dados do GAB, definindo topologia de rede no qual a ferramenta de DLP deverá ser inserida no ambiente do GAB.

4.26. Gestão de *Cookies*

A política de *cookies* visa detalhar todos os *cookies* utilizados no *website* do GAB, o intuito deste detalhamento é atender os requisitos da Lei Geral de Proteção de Dados Pessoais – LGPD, para manter a transparência aos titulares dos dados sobre a realização do tratamento dos dados e a coleta de consentimento, quando for aplicável.

4.27. Monitoramento de Dados Pessoais Vazados na *Web*

A área de Tecnologia da Informação (TI) deve considerar as atividades ao monitorar, detectar, analisar e corrigir um incidente de vazamento de dados de forma contínua.

As atividades de tratamento de um incidente de vazamento de dados, devem estar alinhadas com as diretrizes de incidentes de segurança de informação.

4.28. Criptografia de Dados Pessoais

O GAB deve adotar o uso de criptografia para a proteção das informações restritas ou confidenciais armazenadas em seus domínios ou transportadas em dispositivos móveis, *e-mails* ou serviços de compartilhamento de arquivos.

4.29. Gerenciamento de *Patchs*

O GAB deve ter uma rotina clara para gerenciamento e aplicação de *patchs* de segurança, visando a prevenção e proteção contra ameaças.

4.30. Infrações e Punições

4.30.1. 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.

4.30.2. 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.