TAG	**POLÍTICA** **- PO -**	CÓDIGO **PO-GTI-CYB-001** CLASSIFICAÇÃO **PÚBLICA** REVISÃO

TÍTULO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VERSÃO	DATA	ALTERAÇÃO	ELABORAÇÃO/ REVISÃO	APROVAÇÃO DIRETORIA	APROVAÇÃO CONSELHO DE ADMINISTRAÇÃO
0	24/08/2020	Emissão Inicial	Úrsula Mangia - GTI	Ata DIR-TAG-1104, de 24/08/2020	

TÍTULO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1. OBJETIVO

1.1 Esta Política tem por objetivo:

a) Definir os princípios de segurança das informações da **TAG**, a fim de proteger os seus ativos tangíveis e intangíveis;

b) Servir de fundamento para as diretrizes e processos relacionados à garantia da segurança das informações;

c) Estabelecer as responsabilidades e limites de atuação dos colaboradores da **TAG** e de terceiros em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias em conformidade com os objetivos do negócio e requisitos aplicáveis.

2. APLICAÇÃO / ABRANGÊNCIA

2.1 Esta Política é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos colaboradores e terceiros da **TAG**, nos âmbitos administrativo (recursos de TIC), industrial (recursos de TA) e de internet das coisas (recursos de IoT).

3. DEFINIÇÕES

3.1 **Ameaça:** Causa potencial de um incidente indesejado que pode resultar em dano à **TAG**.

3.2 **Ativo:** Qualquer coisa que tenha valor para a **TAG** e precisa ser adequadamente protegido.

3.3 **Ativo Intangível:** Todo elemento que possui valor para a **TAG** e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à reputação, imagem, marca e conhecimento.

3.4 **Autenticidade:** Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

3.5 **Colaborador:** Empregado, estagiário, menor aprendiz ou qualquer outro indivíduo que venha a ter relacionamento profissional, direta ou indiretamente, com a **TAG**.

3.6 **Confidencialidade:** Garantia de que as informações sejam acessadas e divulgadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

3.7 **Conformidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com os requisitos legais, regulatórios, organizacionais e contratuais.

3.8 **Dado pessoal:** informação relacionada a pessoa natural (física) identificada ou identificável independente do meio em que estiver armazenada.

3.9 **Dado pessoal sensível:** dado pessoal sobre origem racial, etnia, saúde, genética, biometria, e de orientação política, sexual e religiosa.

3.10 **Disponibilidade:** Garantia de que as informações e os recursos de informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

3.11 **Informação:** Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

3.12 **Integridade:** Garantia de que as informações estejam completas e fidedignas em relação à última alteração desejada durante o seu ciclo de vida, além de protegida contra alteração ou destruição não autorizada.

3.13 **Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

3.14 **Nível de Confidencialidade:** identifica o nível de proteção necessário para as informações, de acordo com a sua natureza e o impacto estimado para a **TAG** no caso de divulgação indevida:

a) **Informações públicas:** são as informações que, por não apresentarem riscos, podem ser distribuídas livremente dentro e fora dos limites físicos e dos Recursos de TIC da **TAG**;

b) **Informações internas:** são informações cuja divulgação a terceiros não autorizados poderia promover desvantagem comercial, questionamento de condições contratuais, ou a boa execução das atividades;

c) **Informações restritas:** são informações cuja divulgação a pessoas não autorizadas poderia promover o comprometimento do sigilo de decisões gerenciais, cobertura em mídia local, o nível de segurança físico e lógico do ambiente corporativo, ou a divulgação indevida de dados pessoais;

d) **Informações confidenciais:** são as informações cuja divulgação a pessoas não autorizadas poderia promover o comprometimento dos objetivos estratégicos da **TAG** ou de suas empresas controladas, a perda de negócios, cobertura negativa em mídia nacional, afetar de forma negativa no faturamento da **TAG**, ou a divulgação indevida de dados pessoais sensíveis.

3.15 **Risco:** Efeito da incerteza sobre os objetivos, verificado pela combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos (consequências).

3.16 **Recursos de Tecnologia da Informação e Comunicação (recursos de TIC):** Hardwares, softwares, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

3.17 **Recursos de Tecnologias de Automação (recursos de TA**): conjunto de recursos de TIC aplicados especificamente nas atividades de operação, supervisão, automação controle, incluindo os sistemas de controle industrial.

3.18 **Recursos de Internet das Coisas (recursos de IoT):** conjunto de recursos de TIC que formam uma rede de objetos que possuem tecnologia embarcada para identificar, comunicar e interagir com seu estado interno ou com o ambiente externo.

3.19 **Recurso de Informação:** é o conjunto de todos os recursos de TIC, TA e IoT.

3.20 **Segurança da Informação:** É a preservação da confidencialidade, integridade, disponibilidade, conformidade e autenticidade da informação. Visa proteger a informação e os recursos de informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

3.21 **Tentativa de Burla:** Fazer esforços para não respeitar ou tentar violar as diretrizes e os controles estabelecidos nos normativos da **TAG**.

3.22 **Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos normativos da **TAG**.

4. RESPONSABILIDADES

4.1 A **Diretoria** e o **Conselho de Administração** da **TAG** têm a responsabilidade de analisar, aprovar e declarar formalmente o seu comprometimento com esta **Política**.

4.2 Para o cumprimento desta Política a **Diretoria** da **TAG** define o **Comitê de Segurança da Informação e Privacidade**, formado pelo Gestor de Proteção de Dados Pessoais - DPO, e por representantes das áreas de Tecnologia da Informação & Digitalização, Pessoas & Cultura, Jurídico e Ética, Riscos e Controles Internos, e Projeto SCADA da **TAG**, que é responsável por:

a) Manter esta Política atualizada e submetê-la para aprovação da Diretoria e do Conselho de Administração da **TAG**;

b) Garantir que o **Comitê de Segurança da Informação e Privacidade** seja composto por uma equipe multidisciplinar, tenha atuação permanente, e reúna-se periodicamente;

c) Definir e manter o Programa de Segurança da Informação da **TAG**;

d) Promover e realizar a gestão da Segurança da Informação na **TAG**;

e) Analisar e aprovar, ou não, os pedidos de exceções a esta **Política**;

f) Garantir a publicidade e disponibilidade desta Política na **TAG**, e o seu cumprimento através da definição e implementação de documentos normativos, modelos, padrões, processos, controles e recursos necessários para a Segurança da Informação.

4.3 O ***Chief Information Security Officer*** **- CISO** é responsável por coordenar as atividades do Programa de Segurança da Informação da **TAG**. A **TAG** seguirá o Programa de Segurança da Informação da ENGIE Brasil e contará com o apoio do CISO da ENGIE Brasil para a implementação e coordenação do Programa.

4.4 O ***Chief Information Officer*** **- CIO** é responsável por coordenar as atividades do Comitê de Segurança da Informação e Privacidade e as atividades técnicas relacionadas à avaliação e garantia da segurança das tecnologias digitais da **TAG**.

4.5 O **Gestor de Proteção de Dados Pessoais - DPO** é responsável pela gestão e coordenação das atividades de Privacidade e Proteção de Dados Pessoais da **TAG**.

4.6 Os **Diretores** da **TAG** são responsáveis pela adoção desta Política em suas respectivas Diretorias.

4.7 Os **Gerentes** da **TAG** são responsáveis por:

a) Garantir e gerenciar o cumprimento desta **Política** e demais documentos normativos relacionados pelos colaboradores e terceiros sob sua responsabilidade;

b) Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de negócio sob sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir o risco ao negócio; e

c) Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por colaboradores e terceiros sob sua responsabilidade, e comunicar eventuais ocorrências imediatamente à Gerência de Tecnologia da Informação & Digitalização.

4.8 Os colaboradores da **TAG** são responsáveis por estarem cientes, cumprir e manterem-se atualizados com esta **Política** e demais documentos normativos que a complementem.

5. ORIENTAÇÕES GERAIS

5.1 INTRODUÇÃO

5.1.1 As informações e os recursos de informação são ativos críticos da **TAG**, necessários para a realização de tarefas, tomada de decisão e desenvolvimento contínuo dos negócios e, por isso, devem ser adequadamente produzidos, adquiridos, utilizados, atualizados, administrados e descartados, de forma segura, independentemente do meio ou forma em que estejam armazenados.

5.1.2 O primeiro passo para a implementação da segurança da informação é a adoção de uma Política de Segurança da Informação (**Política**), cujo cumprimento depende, principalmente, das ações dos colaboradores e de terceiros, independentemente do nível hierárquico, da Companhia e da atividade desenvolvida.

5.1.3 Para proteger seus ativos tangíveis e intangíveis, a **TAG** elaborou esta Política, pautada na legislação nacional vigente, nas melhores práticas do mercado e nos princípios da ética e da transparência, e que deve ser cumprida diariamente por todos.

5.1.4 A **Diretoria** e o **Conselho de Administração** da **TAG** estão comprometidos com a proteção dos ativos tangíveis e intangíveis e aprova os princípios de Segurança da Informação contidos nesta Política para garantir a confidencialidade, integridade, disponibilidade e autenticidade desses ativos, e o seu uso em conformidade com a legislação pertinente, as necessidades de negócio e contratos estabelecidos.

5.1.5 A segurança das informações e dos recursos de informação da **TAG** é uma responsabilidade de todos os colaboradores, terceiros, e de todas as pessoas que se relacionam, direta ou indiretamente, com a **TAG**.

5.2 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

5.2.1 Gerais

5.2.1.1 A **TAG** tem os seguintes princípios gerais de segurança da informação:

a) **Preservar e proteger** as informações e os recursos de informação da **TAG** ou de terceiros, ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça e em todo o seu ciclo de vida, contidas em qualquer suporte ou formato;

b) **Prevenir, monitorar, identificar e responder aos incidentes de segurança da informação**, reduzindo os seus impactos e assegurando a confidencialidade, integridade, disponibilidade, autenticidade das informações e a conformidade no uso dos recursos de informação no desenvolvimento das atividades profissionais;

d) **Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares** relacionados ao negócio no que diz respeito à segurança da informação e aos objetivos corporativos, morais e éticos da **TAG** e do **Grupo ENGIE**.

5.2.1.2 As medidas de prevenção e controle adotadas pela **TAG** visam, em essência, gerenciar e manter os riscos em um nível adequado ao negócio.

5.2.2 Propriedade

5.2.2.1 As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os recursos de informação e demais ativos tangíveis e intangíveis disponibilizados, são de propriedade da **TAG** ou, quando de terceiros, estão sob sua guarda e sujeitos às determinações desta Política e documentos normativos que a complementam.

5.2.3 Estratégia de ação

5.2.3.1 A estratégia utilizada para o cumprimento dos princípios de segurança definidos nesta Política é a adoção do Programa de Segurança da Informação da ENGIE Brasil que define os papéis, responsabilidades e as atividades de gestão e de melhoria contínua do nível de Segurança das Informações da **TAG**, e também a adoção de ações táticas de segurança que incluem a definição de Diretrizes, padrões, e a implementação de processos e controles para a adequada:

a) Gestão dos riscos relacionados à falta de segurança das informações e do uso dos Recursos de informação;

b) Proteção dos ativos tangíveis e intangíveis relacionados às informações e recursos de informação da **TAG** e de terceiros, de acordo com a sua importância para o negócio e nível de confidencialidade;

c) Garantia da legalidade e conformidade do uso das informações e recursos de informação;

d) Proteção da privacidade dos dados pessoais das pessoas que se relacionam com a **TAG**, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo seu tratamento autorizado nos termos da legislação de proteção de Dados Pessoais vigente;

c) Conscientização e treinamento dos colaboradores e terceiros para o adequado uso das informações e recursos de informação;

d) Identificação de ameaças, correção de vulnerabilidades e de problemas, e prevenção e resposta a incidentes de segurança da informação;

e) Gestão de projetos e de mudanças nos recursos de informação e nos processos que os utilizam;

f) Gestão das operações dos recursos de informação;

e) Gestão da continuidade das atividades de negócio;

f) Verificação e monitoramento do uso das informações e dos recursos informação;

g) Atuação em caso de violação dos princípios, dos controles estabelecidos e dos normativos da **TAG**;

h) Monitoramento e a melhoria contínua do nível de segurança das informações.

5.2.3.2 As ações para a gestão e o uso seguro das informações e dos recursos de informação devem ser aplicadas em todos os empreendimentos e processos corporativos, de forma a garantir alinhamento com o Planejamento Estratégico Empresarial, com os requisitos de negócio, e com a gestão dos riscos às atividades de negócio e à segurança das informações e recursos de informação.

5.2.3.3 As contratações em que ocorra o compartilhamento de informações de propriedade ou sob a responsabilidade da **TAG**, ou a concessão de acesso aos seus ambientes ou ativos, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à segurança da informação, além de controles que assegurem o conhecimento e o cumprimento desta Política e demais Diretrizes e processos aplicáveis.

5.3 EXCEÇÕES

5.3.1 As exceções que ocorram de forma exclusiva e excepcional a esta Política e aos demais documentos normativos complementares devem ser formalizadas e fundamentadas pelo Gestor responsável pela atividade de negócio, analisadas pelos responsáveis pela área gestora dos recursos de informação, e aprovadas pelo **Comitê de Segurança da Informação e Privacidade**, que poderá a qualquer tempo revoga-las.

5.4 MONITORAMENTO DO USO DAS INFORMAÇÕES E DOS RECURSOS DE INFORMAÇÃO

5.4.1 Os ambientes físicos e lógicos da **TAG** são monitorados visando a eficácia dos controles implantados e a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referentes a segurança da informação.

5.4.2 A **TAG** se esforça e toma ações para proteger a privacidade dos dados pessoais de colaboradores e todas as pessoas que se relacionem com a **TAG**, dentro dos seus processos de negócio, mas não pode garantir a privacidade de informações pessoais de usuários gravadas sem proteção nos recursos de informação corporativos, tais como arquivos em áreas acessadas por outros usuários e mensagens eletrônicas sem proteção.

5.5 VIOLAÇÕES

5.5.1 As violações a esta Política serão avaliadas pelo **Comitê de Segurança da Informação e Privacidade**, que poderão encaminhar ao Comitê de Ética e apurar as responsabilidades dos envolvidos em procedimento disciplinar, visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

5.5.2 A tentativa de burla das diretrizes e controles estabelecidos, quando constatada, será tratada como uma violação.

5.6 DISPOSIÇÕES FINAIS

5.6.1 Gerais

5.6.1.1 O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pela **TAG**.

5.6.1.2 Esta Política, bem como os demais documentos que a complementam, encontram-se disponíveis no website www.ntag.com.br e deverão ainda ser disponibilizados na intranet da **TAG** quando implementada. Em caso de indisponibilidade, podem ser solicitadas às áreas que compõem o **Comitê de Segurança da Informação e Privacidade**.

5.6.2 Revisão desta Política

5.6.2.1 A revisão desta Política é realizada pelo **Comitê de Segurança da Informação e Privacidade** a cada dois anos ou quando ocorrerem mudanças significativas na legislação pertinente, na estrutura organizacional, nos objetivos de negócio, nos processos internos, nos riscos à segurança das informações, e nas Políticas da **TAG**.

5.6.2.2 As proposições de alteração desta Política serão validadas **pelo Comitê de Segurança da Informação e Privacidade** e, se acatadas, serão submetidas à **Diretoria** e ao **Conselho de Administração** da **TAG** para apreciação e aprovação.

5.6.2.3 Esta versão da Política de Segurança da Informação da **TAG** entra em vigor na data de sua aprovação.

6. REFERÊNCIAS

6.1 Código de Ética do Grupo ENGIE
6.2 Guia de Práticas Éticas do Grupo ENGIE
6.3 Política de Privacidade e Proteção de Dados Pessoais
6.4 Lei nº 13.709, de 14.08.2018 e suas alterações.

7. ANEXOS

Não aplicável.