1. OBJETIVO

A Política de Segurança da Informação tem por objetivo:

a. Estabelecer diretrizes que permitam aos "*stakeholders*" da green4T seguirem padrões de comportamento desejáveis e aceitáveis sobre o tema de segurança da informação, agindo de acordo com a legalidade e boas práticas mundiais e visa mitigar riscos técnicos, financeiros, administrativos, jurídicos e de imagem/reputação.

b. Nortear a definição de procedimentos específicos de Segurança da Informação, bem como a implantação de controles e processos para atendimento da mesma.

c. Preservar as informações da green4T quanto à confidencialidade, integridade e disponibilidade.

d. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de consumidores e parceiros ou de qualquer outro impacto negativo ao negócio da green4T, resultante de uma ou mais falhas de segurança em seus ambientes, em especial no que diz respeito aos dados produzidos, armazenados, processados ou tratados por seus profissionais, seja em formato físico ou digital.

Esta Política é complementada por procedimentos e documentos anexos, classificados como confidenciais, e que trazem as orientações a serem seguidas na condução dos processos relacionados à esta política, e servem de referência aos profissionais encarregados da sua execução.

2. ABRANGÊNCIA

Este documento aplica-se a todos os Departamentos e empresas coligadas e controladas da green4T e abrange as normas NBR ISO/IEC 27.001 e ISO/IEC 27.002.

3. TERMOS

a) Autenticidade: Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. Traz características de não repúdio e garantias de modificações apenas autorizadas e rastreadas.
b) Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a pessoa, sistema, órgão, entidade não autorizados e credenciados.
c) Disponibilidade: é a garantia de que a informação pode ser obtida sempre que for necessário, isto é, que esteja sempre disponível e utilizável para quem precisar dela no exercício de suas funções. Quando a informação está indisponível, os processos que dela dependem ficam paralisados.

d) Integridade: é a garantia de que a informação armazenada ou transferida está correta e é apresentada de forma íntegra para quem a consulta. Significa que em uma comunicação, a informação não é modificada, suprimida, destruída de maneira não autorizada ou acidental no meio do trajeto entre quem emite a informação e quem a recebe. É uma característica crítica do ponto de vista operacional e indispensável, pois valida todo o processo de comunicação na green4T.
e) Legalidade: é a garantia de que a informação está gravada em conformidade com os procedimentos em vigor, ou seja, o uso da tecnologia de informática e comunicação que gerou a informação está de acordo com as leis vigentes no local ou País.
f) Rastreabilidade (ou Auditabilidade): é a possibilidade de se rastrear as atualizações ocorridas em uma informação sensível para que, em caso de ocorrência de algum problema, se possa esclarecer exatamente o que aconteceu com a informação. Existem situações em que há necessidade de mecanismos capazes de rastrear o processo de volta até a origem.
g) Usuário: Colaborador ou representante (prestador de serviços) que utiliza os recursos tecnológicos pertencentes à companhia.

4. RESPONSABILIDADES

4.1. GESTOR DE TECNOLOGIA DA INFORMAÇÃO

a) Realizar a gestão do uso de tecnologias necessárias ao bom andamento dos negócios da green4T, incluindo ações preventivas e tratamento de incidentes, a fim de promover maior nível de segurança da informação;
b) Realizar as ações direcionadas às questões técnicas relacionadas a gestão da segurança da informação;
c) Propor as metodologias e processos específicos para a Segurança da Informação, em conjunto ao gestor de Segurança de Informação, como por exemplo, Avaliação de Risco;
~~d)~~ Apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços, em conjunto com o Comitê de Segurança da Informação;
e) Tomar medidas imediatas de forma a remediar eventual violação verificada pela área e cessar de imediato o risco à green4T, informando imediatamente ao DPO sobre a violação e medidas implementadas.

4.2. ÁREA DE GESTÃO E DESENVOLVIMENTO DE PESSOAS

a) Entregar para todo colaborador ou prestador de serviços no momento da sua admissão a **PL.00.34** - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.
b) Entregar e coletar assinatura para todo colaborador ou prestador de serviços no momento da sua admissão a **PL.00.22** - POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO;
c) Definir com o gestor da área, o gestor de TI e o gestor de segurança da informação, os recursos informacionais necessários para a execução das

atividades para qual o colaborador ou prestador foi contratado (hardware e software);

d) Solicitar o bloqueio dos acessos aos sistemas de informação da companhia em caso de desligamento e mudança de área.

4.3. COLABORADORES E PRESTADORES TERCEIROS

Todos os colaboradores e prestadores da green4T:

a) Comprometem-se a cumprir fielmente a Política, normas e procedimentos de Segurança da Informação estabelecidos neste documento, assumindo o compromisso de observá-las e aplicá-las, bem como submetendo-se às sanções previstas nas políticas internas e na legislação aplicável;

b) Concordam que todas as operações e acessos efetuados em meios magnéticos são registrados e passíveis de verificação a qualquer momento, independentemente de aviso prévio, por se tratar de ferramentas de trabalho, não havendo que se falar em invasão de privacidade;

c) Ficam cientes de que a green4T, conforme direito que lhe cabe, poderá realizar o monitoramento de todos os seus ambientes, sejam eles físicos, como salas de trabalho; lógicos e/ou eletrônicos, incluindo: e-mail corporativo, rede interna, Internet e Extranet e outros sistemas, armazenando os dados de acesso de cada usuário;

d) Concordam e reconhecem que, no evento de qualquer violação dos termos e condições desta Política, estará sujeito às normas internas e à legislação em vigor. Poderá, ainda, ensejar a demissão por justa causa, nos termos do disposto no Art. 482, alínea "g", da Consolidação das Leis do Trabalho, sem prejuízo das demais sanções legais cabíveis;

e) Ficam cientes que, quando do término de sua relação de trabalho, ou a qualquer momento mediante requerimento da green4T, o mesmo deverá devolver todos e quaisquer materiais fornecidos, ou que contenham Informações produzidas decorrentes do contrato de trabalho;

f) Ficam cientes de que é proibida a reprodução de documentos de uso exclusivo da green4T, para quaisquer finalidades ficando tal atitude caracterizada como divulgação não autorizada de informações confidenciais e produção ilegal de provas;

g) Devem buscar orientação junto ao gestor de segurança da informação quando houver dúvidas relacionadas à Segurança da Informação;

h) Devem fazer o uso de senha segura, devendo alterar a mesma, conforme periodicidade determinada pela green4T;

i) Devem assinar a **PL.00.22** - POLÍTICA DE TECNOLOGIA DE INFORMAÇÃO, formalizando a ciência da Política e das Normas de Segurança da Informação bem como assumindo a responsabilidade pelo seu cumprimento;

j) Devem proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pela green4T;

k) Devem assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse da green4T;
l) Devem comunicar imediatamente ao gestor de segurança da informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos relacionados.

4.4. GERENTE DE ÁREA

É responsabilidade de todo gestor de área da green4T:

a) Ter conhecimento e gerenciar os acessos concedidos aos seus subordinados, sendo, portanto, responsável indireto pelo mau uso dos mesmos;
b) Revisar periodicamente os usuários com acessos a transações críticas sob sua responsabilidade, devendo informar a área de Gestão e Desenvolvimento de Pessoas sobre eventuais mudanças de acesso ou autorização;
c) Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;
d) Cumprir e fazer cumprir esta Política, as Normas e Procedimentos de Segurança da Informação;
e) Assegurar que suas equipes possuam acesso e conheçam esta Política, bem como das Normas e Procedimentos relacionados à Segurança da Informação;
f) Atribuir na fase de contratação de terceirizados e parceiros, quando este necessitar ter contato com informações da companhia, a inserção de cláusula de responsabilidade, ciência da Política de Segurança da Informação, exigindo o repasse das obrigações a seus colaboradores responsáveis pela prestação de serviços dentro da green4T;
g) Especificar e solicitar previamente permissão de acesso, elencando os ativos de informação para os colaboradores em geral que não sejam contratados;
h) Auxiliar o gestor de segurança da Informação na adaptação das Normas, Processos, Procedimentos e sistemas sob sua responsabilidade para atender a esta Política de Segurança da Informação;
i) Comunicar imediatamente ao gestor de segurança da informação, através de Canal específico (dpo@green4t.com), eventuais violações da Segurança da Informação, que acionará e trabalhará em conjunto com a equipe de Segurança da Informação.

4.5. GESTOR DE COMPLIANCE

a) Efetuar testes de monitoramento sobre a aderência às regras estabelecidas nesta política;
b) Auxiliar o DPO na adequação da empresa green4T à lei 13.709/18 (Lei Geral de Proteção de Dados-LGPD), as normas ISO/IEC 27.001, ISO/IEC 27.002 e ISO/IEC 27.701 definindo as melhorias de controles internos a serem implementados pela área de tecnologia da informação e demais exigências descritas na lei.

4.6. DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Cabe ao time de Segurança de Informação da green4T:

a) Submeter ao Comitê de Segurança da Informação e LGPD as versões da Política e das normas de Segurança da Informação, e após a aprovação, publicar e promover as mesmas na intranet da green4T;
b) Propor e apoiar iniciativas que visem à segurança dos ativos de informação da green4T;
c) Promover, junto à área de Gestão e Desenvolvimento de Pessoas, conscientização dos colaboradores e parceiros em relação à relevância da Segurança da Informação para o negócio da green4T, através de campanhas, palestras, treinamentos e outros meios;
d) Analisar criticamente incidentes, com apoio do time de TI, se necessário;
e) Manter comunicação efetiva com o Comitê de Segurança da Informação e LGPD, com o objetivo de mantê-los adequadamente informados sobre assuntos relacionados ao tema, que afetem ou tenham potencial para afetar a green4T;
f) Receber as denúncias sobre violações da Política e das Normas, após concretização das investigações realizadas, devendo promover a tratativa das informações, identificação do plano de ação, mitigação de risco, acionamento do Comitê de Segurança da Informação e LGPD e aplicação da sanção cabível (Penalidades).

4.7 DA ÁREA JURÍDICA

a) Orientar para a melhor forma de coleta e preservação de prova eletrônica, com o objetivo de manter sua eficácia para uso em juízo, quando necessário; e
b) Elaborar e revisar documentos jurídicos relacionados à Segurança da Informação, principalmente à proteção dos dados definidos pela LGPD e assegurar cláusulas que mitiguem os riscos jurídicos.

4.8 DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

O Comitê de Segurança da Informação e LGPD é formado por gestores das principais áreas da Green4T, que devem cumprir as seguintes responsabilidades dentro da organização.

a) Garantir a disponibilidade de recursos para todas as ações de Segurança da Informação;
b) Manter o foco e promover a Segurança da Informação na green4T, aprovando políticas que reflitam o seu papel acima descrito mediante aprovação de material submetido pelo gestor de Segurança de Informação;
c) Garantir que riscos à Segurança de Informação sejam identificados, avaliados, categorizados e gerenciados pelo gestor de Segurança de Informação responsável para tanto;

d) Aprovar ações custo-efetivo para realizar a gestão dos riscos e monitorar a sua implantação;
e) Dar direcionamento, revisar e atualizar a estratégia de Segurança da Informação garantindo que sua Política, normas e procedimentos sejam adequadamente atualizados e continuamente pertinentes ao cenário da green4T;
f) Garantir que treinamento e conscientização sobre Segurança da Informação seja fornecido para colaboradores e, quando pertinente, a terceiros, fornecedores e clientes.

5. DIRETRIZES DESTA POLÍTICA

5.1. DIRETRIZES GERAIS

A informação, produzida ou recebida pelos profissionais da green4T, deverá ser utilizada com senso de responsabilidade e de modo ético e seguro, em benefício exclusivo do negócio corporativo e baseado nos seguintes princípios da integridade, disponibilidade e confidencialidade. Na green4T a informação é considerada como o ativo mais valioso. Sem confidencialidade perde-se vantagem competitiva, sem integridade perde-se lucratividade e sem disponibilidade perde-se a capacidade de operar. Além dos três atributos mencionados, considera-se também a autenticidade, legalidade e rastreabilidade, uma vez que sem autenticidade, perde-se a confiança da origem fidedigna da informação, sem legalidade, há o risco de não aderência às normas regulatórias internas e externas e sem rastreabilidade, perde-se o controle das atualizações ocorridas em dados sensíveis.

A Segurança da Informação na organização estabelece as principais diretrizes e controles para a proteção das informações:

a. As informações de titularidade da green4T devem ser tratadas de forma ética, sigilosa e legal e sempre se atentando aos termos acordados com colaboradores, clientes e parceiros, evitando assim o mau uso e exposição indevida de tais informações;

b. A informação deverá ser utilizada de forma transparente, apenas para a finalidade para a qual foi designada e pelo tempo necessário para atingir a sua finalidade;

c. Todos os usuários concordam em usar as Informações unicamente na execução de seus deveres e devidamente classificadas de acordo com o critério de classificação definido pela organização;

d. Durante sua relação de trabalho ou parceria com a green4T - e mesmo depois de findar esta - o usuário não poderá publicar, revelar, ou de outro modo disponibilizar à qualquer terceiro, quaisquer Informações classificadas como Restritas ou Confidenciais Restritas, exceto: (i) quando

expressamente autorizado por escrito pela green4T, ou (ii) para outros colaboradores ativos que sabidamente estão autorizados a receber Informações Confidenciais e têm necessidade de conhecê-las visando sua utilização para atender às necessidades do negócio;

e. Todos os usuários da informação têm ciência e concordam em agir com toda a diligência necessária para proteger a integridade e o sigilo das informações de propriedade da green4T, ficando vedada a subtração ou a retirada, sob qualquer forma, quaisquer materiais, exceto no que seja necessário em razão de normas ou leis em vigor;

f. Todas as pessoas dentro das dependências físicas da Green4T convém estar identificadas por crachás visíveis (ou outro meio visual de identificação). A identificação (crachá, login, senha, etc.) de cada colaborador é única, pessoal e intransferível, qualificando-o como responsável, civil e criminalmente, pelas ações realizadas;

g. A senha de acesso é de uso pessoal e intransferível e deve ser mantida em sigilo, sendo expressamente proibido o seu compartilhamento, exceto nos casos pré-aprovados pelas áreas de Segurança da Informação;

h. Todos os riscos identificados em relação às informações da green4T devem ser reportados para a equipe de segurança da informação através de canal específico (dpo@green4t.com), para que possam ser tomadas as medidas necessárias de avaliação e mitigação do risco eventualmente identificado. Bem como todos os incidentes que afetem a segurança da informação deverão, de igual maneira, serem reportados à equipe de segurança da informação através de canal específico (dpo@green4t.com), que analisará o incidente e elaborará o relato;

i. Todo procedimento seguirá as diretrizes e normas para incidentes de segurança e, caso necessário, levará à diretoria o relato para que sejam aplicadas as devidas sanções aos envolvidos;

j. O controle de acesso dos usuários aos ativos de informação deve ser devidamente aprovado pelo responsável pela informação, quer seja para simples consulta ou para alteração. Todas as informações relativas à solicitação, aprovação e concessão efetiva do acesso deverão ser armazenadas em um Drive seguro, com o controle de acesso configurado pelos responsáveis de cada área;

k. O uso do e-mail corporativo disponibilizado pela green4T é de propriedade da mesma e será permitido para usuários apenas para fins corporativos e por tempo determinado, definido pela gerência da área solicitante. Quanto à transmissão de dados, este recurso deve ser utilizado para garantir a privacidade na comunicação dos dados;

l. Todos os requisitos de Segurança da Informação, incluindo a necessidade de planos de continuidade do negócio, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema. Estes requisitos devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução;

m. As regras para o desenvolvimento seguro de sistemas e softwares devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro ou fora da organização, estando condicionadas à avaliação de adequação e aprovação do time de Segurança da Informação. No caso de desenvolvimento fora da green4T, o sistema deverá conter ferramentas que permitam auditoria de segurança quanto: autodeterminação informativa de titulares de dados, trilhas de auditoria, políticas de acesso (autenticação, autorização e rastreabilidade) e análise dos códigos fontes;

n. A concessão de acesso remoto aos sistemas e Drives da green4T para os colaboradores, parceiros e fornecedores, deve ser autorizada formalmente. A solicitação deve ser enviada à área de TI, pelo gestor da área solicitante, ocasião em que deverá ser indicado o tipo de acesso, permissão e as informações a serem acessadas. Todo procedimento deve ser apresentado ao gestor de segurança da informação para que tenha ciência das autorizações;

o. O uso do ambiente da internet na green4T é permitido somente para fins profissionais, onde os colaboradores devem ficar atentos aos sites que acessam e cientes que serão monitorados;

p. Um conjunto de regras deverá ser criado para garantir a padronização das técnicas criptográficas, a aplicação adequada das mesmas e responsabilidades para manter a segurança no transporte ou armazenamento das informações, independentemente do meio utilizado. A responsabilidade em relação às regras é do gestor de TI em parceria com o gestor de segurança da informação;

q. O ambiente de desenvolvimento, homologação e produção devem ser segregados e devidamente controlados. Não é permitido no ambiente de testes a utilização de dados pessoais e dados pessoais sensíveis reais;

r. Um processo de gestão de mudanças garante que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo da organização;

s. Os riscos são identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (confidencialidade, integridade e disponibilidade);

t. Todas as informações que estiverem no meio físico (papel) deverão de igual teor serem classificados, armazenados em local seguro, trancado, protegido contra riscos naturais, voluntários e involuntário, com controle de acesso formal por parte dos usuários visando possíveis trilhas de auditorias;

u. Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta Política, o responsável e/ou solicitante deverá reportá-las imediatamente ao gestor de segurança da informação, para que este possibilite a adoção de medidas alternativas que mitiguem os riscos, bem como um plano de ação para corrigi-los, atenuá-los, monitorá-los ou eliminá-los;

v. Todos os colaboradores da green4T devem passar por treinamento e conscientização sobre os procedimentos de segurança e uso correto dos ativos disponibilizados pela green4T periodicamente, de forma a minimizar possíveis riscos de segurança, explicitar suas responsabilidades e comunicar os procedimentos para a notificação de incidentes;

w. Todos os colaboradores da green4T devem cuidar para que os direitos de propriedade intelectual sejam preservados, tais como projetos, marcas, patentes e que o uso de produtos de softwares proprietários esteja em conformidade com a respectiva licença de uso;

x. Todos os colaboradores da green4T devem zelar para o cumprimento da "Política de mesa limpa, tela limpa e lixo limpo", cujo objetivo é evitar:
   1) papéis e mídias de armazenamento removível em cima das mesas;
   2) cestos de lixo contendo informações confidenciais legíveis;
   3) telas com informações de sessões ativas ou de sessões já desativadas.
   Estes cuidados são extensíveis às áreas comuns, tais como corredores, armários, áreas de armazenamento de material, salas de reunião, recintos de espera, áreas comunitárias (copa, cozinha, lazer, etc.).

5.2. DIVULGAÇÃO

A Política de Segurança da Informação é de conhecimento de todos os usuários e divulgada da seguinte forma:

a) Via campanhas periódicas de Segurança da Informação; e
b) Por meio digital, através da intranet corporativa.

A política está disponível em local de fácil acesso dos colaboradores e protegida contra alterações não autorizadas.

Todos os colaboradores, além de prestadores de serviços, parceiros e fornecedores que realizem qualquer forma de acesso ou manipulação das informações (digitais ou físicas) ou utilizem recursos tecnológicos da green4T devem aderir formalmente à "**PL.00.22** - POLÍTICA DE TECNOLOGIA DE INFORMAÇÃO", comprometendo-se a agir de acordo com a regras nela descrita. (Material disponível como um dos volumes da Política de Segurança da Informação).

A **PL.00.34** - Política de Segurança da Informação é revisada e atualizada periodicamente, no mínimo a cada 01 (um) ano e/ou sempre que algum fato relevante ou evento ocorrer que motive a revisão antecipada da mesma, conforme análise e decisão do Comitê de Segurança da Informação e LGPD.

5.3. MONITORAMENTO

A green4T através de sua área de Segurança da Informação monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas na mesma, a qual se reserva no direito de:

a) Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônicos, Internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados.

b) Inspecionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta Política de Segurança da Informação.

c) Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

d) Monitorar as instalações físicas através de câmeras.

5.4. DIRETRIZES PARA LGPD

A empresas Green4T definiu e implementou controles internos necessários para adequação à LGPD, referente a proteção de dados de clientes, colaboradores, fornecedores ou outros que envolvam dados de pessoas físicas, conforme disposto na lei 13.709/18.

5.5. PENALIDADES

Quando entender necessário e relevante, o time de Segurança de Informação submeterá as infrações à Política de Segurança da Informação e às Normas de Segurança da Informação à diretoria, assim como o resultado da apuração validado através do comitê de segurança da informação e LGPD e demais áreas pertinentes, conforme a Política de Apuração de Denúncias da green4T.

Ao suspeito de cometer violações à Política e Normas de Segurança da Informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração, deverá ser aplicada com proporcionalidade à ocorrência com base na Norma de Infrações e Penalidades.

A green4T se exime de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis

6. DOCUMENTOS DE REFERÊNCIAS

P.12.01 - Backup_green4T
P.12.04 - Desligamentos_green4T
PL.00.22 – Política de Tecnologia da Informação_green4T
PL.00.31 – Política de Privacidade Interna_green4T
PL.00.32 – Política de Privacidade Externa_green4T

7. CONTROLE DE REGISTROS

NA.

8. HISTÓRICO DE REVISÕES

Revisão	Data	Descrição da alteração	Aprovado pelo Gestor	Aprovado por Certificações
00	30/05/2022	Emissão	Eduardo Marini	Adriana Moyses
01	15/08/2023	Revisão geral da política, item 5.1.f alterado	Comitê LGPD: Claudio (DPO), Alan Baldo, Eduardo Rasi e Thais Almeida	