1. DOCUMENTOS DE REFERÊNCIA

i. Código de Ética e Conduta (CEC) da Belem Bioenergia Brasil
ii. Norma Brasileira NBR ISO 27000 – Sistemas de gestão de segurança da informação (2018)
iii. Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14/08/2018
iv. Diretrizes e procedimentos estabelecidos para a área Sistema e Tecnologia da Informação, sob as referências:
v. 00-STI-NPA-01 –Tecnologia da Informação
vi. 00-STI-NPA-02 – Rádio Comunicação

2. SIGLAS E DEFINIÇÕES

2.1. Para os fins desta Política, os termos a seguir devem ser entendidos da seguinte forma:

a) **Companhia**: Belem Bioenergia Brasil;

b) **Alta Administração**: membros do Conselho de Administração e Comitês de assessoramento ao Conselho de Administração;

c) **Gestão**: Gerentes, Coordenadores e Supervisores;

d) **Diretoria**: Presidentes e Diretores.

e) **Colaboradores**: empregados devidamente contratados e registrados de acordo com as leis trabalhistas aplicáveis, bem como os executivos da Companhia;

f) **Terceiro:** qualquer pessoa física ou jurídica relacionada à Companhia;

g) **Terceirizado:** qualquer pessoa física ou jurídica contratada para agir pela Companhia ou em nome dela;

h) **Parceiros de negócios:** qualquer pessoa física ou jurídica, que possui relação comercial com à Companhia;

i) **Fornecedor:** qualquer pessoa física ou jurídica, que fornece produto ou serviço à Companhia.

j) **Stakeholders**: partes interessadas ou afetadas pela operação da empresa, podendo ser internos (acionistas, colaboradores etc.) ou externos (clientes, terceirizados, fornecedores, parceiros, comunidades, órgãos governamentais etc.);

k) **Portal de Atendimento (Central de Serviços Bioenergia):** portal disponível na Intranet, ou outro meio de comunicação virtual, no qual os funcionários utilizam para fazer solicitações como: liberação de acesso a sistemas, instalação de desktops e notebooks, serviços de telefonia etc.

l) **Custodiante da Informação:** qualquer área, funcionário ou prestador de serviço responsável pela custódia da informação (guarda) impressa ou digital.

m) **Gestor da Informação:** qualquer área ou funcionário da Belem Bioenergia dono de sua respectiva informação.

n) **Telefonia móvel:** são recursos computacionais pequenos e portáteis, possuindo normalmente uma tela com entrada por toque e/ou um teclado em miniatura. Têm um sistema operacional enxuto

que pode executar vários tipos de software aplicativo, conhecido como “apps”. Conectam à rede de dados sem fio ou de operadoras de serviços móveis celular. Podem ter um recurso de tocar multimídia ou música.

o) **Recursos de TI:** notebooks, desktop, impressoras, smartphones, tablets, rádios, telefonia móvel e fixa, impressoras e videoconferência.

3. ATUALIZAÇÃO

3.1. A área de Tecnologia da Informação acompanhará a conformidade desta Política com as demais normas internas e regulamentações aplicáveis. A atualização e proposta de revisão ocorrerá a cada 2 anos ou quando se mostrar necessário. Enquanto a proposta de revisão não for aprovada pela Diretoria Administrativo-Financeira, a presente Política continuará vigente.

3.2. CONTROLE DE REVISÕES

Revisão	Data	Descrição	Elaborador	Aprovador
00	26/09/2024	Elaboração Inicial	Coordenação de Tecnologia da Informação	Conselho de Administração
01	10/04/2026	Revisão do item 15.1	Coordenação de Tecnologia da Informação/Compliance	Conselho de Administração
02	08/05/2026	Alteração do identificador de 00-STI-POL-01 e convertido para 00-STI-POS-01. Revisão geral do documento e mudança na formatação; alteração dos itens 2, alínea “k”, 3.1, 5.1, 6, 9.18.2.3, 9.18.2.4; inclusão dos itens 9.19, 9.20, 9.21, 9.22, 9.23; e exclusão do item 9.10.	Jhovan Silva / Tiago Nascimento	Tainan Bittencourt

4. OBJETIVOS

4.1. Estabelecer diretrizes e práticas para a proteção da informação, promovendo um ambiente seguro e em conformidade com as melhores práticas de segurança da informação.

5. ABRANGÊNCIA

5.1. Esta Política aplica-se a todos os colaboradores, terceiros, prestadores de serviço e demais partes interessadas que utilizem recursos de tecnologia da informação ou tratem dados e informações da Belem Bioenergia Brasil.

6. COMPETÊNCIAS

6.1. Diretoria Administrativo-Financeira

6.1.1. Aprovar esta Política e suas atualizações;

6.1.2. Assegurar a adequada gestão, efetividade e continuidade desta Política.

6.2. Departamento de Segurança da Informação

6.2.1. Efetivar esta Política.

6.2.2. Avaliar a efetividade desta política de acordo com os processos internos estabelecidos.

6.2.3. Garantir o treinamento e divulgação desta política, podendo ser realizado através de plataformas digitais e vídeos institucionais.

6.2.4. Implementar e manter medidas de segurança da informação.

6.2.5. Realizar avaliações de risco periodicamente.

6.2.6. Atualizar e revisar esta política.

7. PRINCÍPIOS

7.1. A política de segurança da informação da Companhia tem como objetivo proteger os ativos de informação da organização contra ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade das informações.

8. DIRETRIZES

8.1. A Companhia e todos aqueles relacionados às suas atividades deverão sempre e inexoravelmente observar a legislação e a regulamentação aplicáveis, no âmbito local, nacional e internacional, de modo a preservar os elevados padrões éticos e morais de atuação da Belem Bioenergia Brasil.

9. DISPOSIÇÕES GERAIS

9.1. Responsabilidades

9.1.1. Colaboradores

9.1.1.1. Seguir as políticas e procedimentos de segurança da informação.

9.1.1.2. Reportar incidentes de segurança à equipe de TI.

9.1.1.3. Participar de treinamentos regulares de segurança sempre que disponível.

9.2. Utilização de Recursos e Equipamentos de TI

9.2.1. Diretoria Administrativo-FInanceira

9.2.1.1. Definir e revisar periodicamente as regras para o uso sustentável dos recursos e equipamentos de TI.

9.2.2. Gerência de Tecnologia da Informação e Telecomunicações

9.2.2.1. Promover atualizações nos recursos e equipamentos de TI.

9.3. Padrão de Senhas

9.3.1. Coordenação de TI

9.3.1.1. Aprovar periodicamente as regras para o estabelecimento do padrão de senhas de todos os Funcionários, Prestadores de Serviços e Administradores de Sistemas.

3.3.1.1. Estabelecer um padrão de senhas para os usuários de TI.

9.4. Controle de Acesso

9.4.1. O acesso à informação deve ser restrito com base no princípio do mínimo privilégio.

9.4.2. Os direitos de acesso devem ser revisados regularmente.

9.5. Proteção contra Malware e Ameaças

9.5.1. Implementar medidas para proteger os sistemas contra malware, vírus e outras ameaças. Isso inclui a utilização de antivírus e firewalls atualizados.

9.6. Política de Senhas

9.6.1. Implementar requisitos rigorosos para a criação, armazenamento e atualização de senhas. A autenticação de dois fatores deve ser incentivada.

9.7 Monitoramento e Auditoria

9.7.1. A atividade do sistema e do usuário deve ser monitorada regularmente. Auditorias de segurança devem ser realizadas para identificar possíveis vulnerabilidades.

9.8 Resposta a Incidentes

9.8.1. Desenvolver e manter um plano de resposta a incidentes, incluindo procedimentos para notificação, investigação e mitigação de incidentes de segurança.

9.9 Conscientização e Treinamento

9.9.1. Fornecer programas regulares de conscientização e treinamento em segurança da informação a todos os colaboradores.

9.10 Classificação da Informação

9.10.1 Estabelecer as regras e orientações para classificação das informações conforme os requisitos legais, estratégicos e críticos da Belem Bioenergia Brasil.

9.10.2 Coordenação de Tecnologia da Informação

9.10.2.1 Deve Definir regras e orientações para classificação das informações conforme requisitos legais, estratégicos e críticos da Belem Bioenergia Brasil.

9.10.2.2 Responsável por suportar as áreas na classificação e proteção das informações.

9.10.3 Gestor (dono) da Informação

9.10.3.1 Classificar e reclassificar tempestivamente as informações sob sua responsabilidade, sempre observando as diretrizes descritas nesta norma.

9.10.3.2 Definir o tempo de retenção das informações sob a sua responsabilidade, garantindo aderência a requisitos legais, documentos normativos ou requisitos de negócio.

9.10.3.3 Analisar e aprovar a disponibilização e o descarte das informações sob a sua responsabilidade, sempre observando as diretrizes aqui descritas.

9.10.3.4 Orientar o custodiante (guardador) da Informação quanto à necessidade de proteção, contingência, backup ou cópia das informações sob sua gestão.

9.10.3.5 Autorizar a transmissão/transporte de informações corporativas sob sua responsabilidade para fora da Belem Bioenergia.

9.10.4 Custodiante (guardador) da Informação

9.10.4.1 Manter a confidencialidade, disponibilidade e integridade das informações sob sua custódia de acordo com as diretrizes deste documento.

9.10.4.2 Comunicar ao gestor (dono) da Informação a ocorrência de incidentes que possam gerar quebra de confidencialidade, integridade ou disponibilidade das informações sob sua custódia.

9.10.5 Todos os Funcionários e Prestadores de Serviços

9.10.5.1 Rotular as informações físicas ou digitais da Belem Bioenergia, de acordo com sua classificação, contendo:

9.10.5.2 A classificação da informação.

9.10.5.3 Gestor (dono) da Informação.

9.10.5.4 O público-alvo a quem se destina o conteúdo, apenas para informações classificadas como confidencial ou restrita.

9.10.5.5 Obedecer aos critérios de armazenamento, transporte e descarte das informações da Belem Bioenergia, conforme a Tabela 1.

Tabela 1 – Armazenamento, Transporte e Descarte

Classificação	Armazenamento	Transporte	Descarte
Confidencial ou Restrita	Implementar controles para limitar o acesso lógico e físico somente aos usuários com a devida permissão. Para documentos impressos, utilizar mecanismos que garantam a confidencialidade e a integridade das informações, como envelopes lacrados. Para informações digitais, utilizar controle de acesso sempre que houver meios disponíveis	Quando transportados para fora da Companhia, documentos impressos devem ser protegidos por mecanismos que garantam sua confidencialidade e integridade. Para informações digitais, utilizar controle de acesso sempre que houver meios disponíveis.	Documentos impressos devem ser fragmentados. Garantir a correta exclusão de informações em mídias de armazenamento após o uso.
Uso Interno	Implementar controles para limitar o acesso lógico e físico visando garantir acesso à informação somente aos usuários com a devida permissão.	Quando transportados para fora da Companhia, documentos impressos devem ser protegidos por mecanismos que garantam sua confidencialidade e integridade. Para informações digitais, utilizar controle de acesso sempre que houver meios disponíveis.	Documentos que podem ser lidos somente por membros da companhia dentro da rede interna.

Pública	Sem critérios específicos.	Sem critérios específicos.	Sem critérios específicos.

9.10.6 Recomendações e regras

9.10.6.1 Análises de risco e viabilidade podem ser consideradas, apontando para a necessidade de controles mais rígidos (no caso, por exemplo, de ambientes de alta exposição a riscos) ou controles menos rígidos para o armazenamento, transporte e descarte de informações.

9.10.6.2 A violação de qualquer item dessa norma caracteriza o uso indevido de informações e é considerado violação de contrato de trabalho, sujeito a medidas administrativas disciplinares de acordo com a sua gravidade.

9.11. Utilização de Recursos e Equipamentos de TI

9.11.1. Estabelecer as principais regras para uso sustentável dos recursos e equipamentos de Tecnologia da Informação e Telecomunicações.

9.11.1.1. Diretoria Administrativo-Financeira

9.11.1.1.1. Revisar periodicamente as regras para o uso sustentável dos recursos e equipamentos de TI, de forma a garantir que estejam sendo utilizados de maneira eficiente, responsável, segura e econômica.

9.11.1.2. Gerência de Tecnologia da Informação e Telecomunicações

9.12.1.2.1. Promover atualizações nos recursos e equipamentos de TI para garantir o uso seguro das informações da Belem Bioenergia.

9.11.1.2.2. Recolher ou desativar quaisquer recursos e equipamentos de TI que não estejam sendo utilizados pelos funcionários ou prestadores de serviço.

9.11.1.2.3. Deverá restringir a utilização de recursos e equipamentos de TI para evitar comportamentos inadequados, conteúdo impróprio ou não profissional como:

9.11.1.2.4. Baixar, armazenar ou instalar, localmente ou na rede, arquivos de vídeos, áudios, imagens, jogos ou qualquer tipo de software pirata;

9.11.1.2.5 Acessar chats, blogs, redes sociais e outros;

9.11.1.2.6 Acessar rádio, TV e jogos via web

9.11.1.2.7 Garantir todas as questões de segurança da informação, transparência e compliance relacionadas aos produtos, realizando a gestão plena do produto quanto a:

9.11.1.2.8. Atualização da versão;

9.11.1.2.9. Erros de sincronização;

9.11.1.2.10. Alertas de segurança e licenciamento.

9.11.1.2.11. Disponibilizar toda infraestrutura e equipamentos corporativos necessários para atuação do funcionário em sua área.

9.11.1.2.12. Fornecer capacitação necessária para utilização das ferramentas corporativas de TI.

9.11.1.2.13. Ter ciência que todo recurso de TI disponibilizado pela Companhia é de sua propriedade e, portanto, restringe-se a execução das atividades relacionadas ao trabalho, sendo assim fica vedado o uso dos recursos disponibilizados para uso pessoal.

9.11.1.2.14. Monitorar colaborador via PRTG e outras ferramentas de gerência de hosts.

9.11.1.2.15. Manter o inventário de ativos de TI, incluindo aqueles utilizados por prestadores de serviço.

9.11.1.3. Todos os Funcionários e/ou Prestadores de Serviços da Belem Bioenergia

9.11.1.3.1. Solicitar serviços e recursos de TI, de acordo com a necessidade e natureza do negócio, através do portal de atendimento (Central de Serviços Bioenergia).

9.11.1.3.2. Receber os equipamentos e recursos solicitados somente com o Termo de Responsabilidade devidamente assinado.

9.11.1.3.3. Enviar para análise das lideranças de TI as solicitações de serviços e recursos não disponibilizados no portal de atendimento. O atendimento dessas solicitações está sujeito a custos e prazos de atendimento específicos, que devem ser aprovados pela área solicitante.

9.11.1.3.4. Devolver imediatamente os recursos de TI que não estejam em uso, para a área de Tecnologia da Informação através de abertura de chamado no portal de atendimento (Central de Serviços Bioenergia).

9.11.1.3.5. No caso de desligamento, os equipamentos disponibilizados para o funcionário devem ser imediatamente devolvidos para a TI. Não é permitida a cópia de informações profissionais. No caso de informações pessoais, caso o colaborador deseje realizar cópia, estas devem ser avaliadas e autorizadas pelo gestor imediato, através do portal de atendimento (Central de Serviços Bioenergia).

9.11.1.3.6. Em caso de furto, roubo ou extravio dos equipamentos, cabe ao usuário:

9.11.1.3.6.1. Solicitar, imediatamente à TI o bloqueio dos equipamentos;

9.11.1.3.6.2. Registrar boletim de ocorrência no prazo máximo de 24 horas, comunicar formalmente o fato à Gerência de TI para que sejam adotadas, se for o caso, as providências relacionadas com a apuração de responsabilidade, na forma da legislação pertinente. No caso de viagem internacional a comunicação deverá ser feita junto à autoridade local competente.

9.11.1.3.6.3. Além das providências estabelecidas no item anterior, comprovada a sua responsabilidade pelo extravio ou dano causado ao aparelho, o detentor do equipamento deverá promover a sua reposição por outro da mesma marca e modelo ou similar, com a respectiva nota fiscal para comprovar a sua procedência.

9.11.1.3.6.4. Testar o funcionamento dos recursos de TI no momento do recebimento dos mesmos. Em caso de falta de algum item, dano ou mau funcionamento, o usuário deve rejeitar o recebimento.

9.11.1.3.6.5. Abrir chamado no portal de atendimento (Central de Serviços Bioenergia), caso seja necessário transferir a responsabilidade de um recurso de TI (transferência entre colaboradores da Belem Bioenergia). Caso o recurso precise ser movimentado fisicamente, por exemplo um notebook, deve-se envolver a área de gestão de ativos (patrimônio), além da própria área de TI.

9.11.1.3.6.6. Não utilizar recursos de TI de forma a violar os princípios estabelecidos no Código de Ética e Conduta e na Política de Segurança da Informação.

9.11.1.3.6.7. Não armazenar informações corporativas confidencias, restritas ou de uso interno em repositórios que não possuam acesso controlado. Exceções devem ser submetidas à aprovação da gerência e/ou diretoria imediata mediante conhecimento e tratativa da área de TI.

9.11.1.3.6.8. Não infringir copyright ou outros direitos de propriedade intelectual (ex: músicas digitais, vídeos, softwares etc.).

9.11.1.3.6.9. Não abrir fisicamente os recursos de TI para tentar reparar qualquer problema. Esta conduta pode gerar incidentes de segurança e quebra de garantia.

9.11.1.3.6.10. Não solicitar suporte de TI para funções de caráter pessoal.

9.11.1.3.6.11. Não tentar obter acessos não autorizados ou interferir na operação normal de qualquer recurso de TI do ambiente tecnológico da Belem Bioenergia.

9.11.1.4. Gestor do Usuário

9.12.1.4.1. Garantir que os recursos e serviços de TI dos funcionários e prestadores de serviços desligados sob sua responsabilidade sejam devolvidos, revogados ou transferidos para usuários ativos através do portal de atendimento (Central de Serviços Bioenergia).

9.11.1.5. Recomendações e Regras

9.11.1.5.1. É proibido o uso de dispositivos de armazenamento externo (pen drives, cartões de memória, HDs externos etc.) nos computadores de propriedade da Belem Bioenergia.

9.11.1.5.2. É expressamente proibido o armazenamento em qualquer recurso de Tecnologia, documentos ou arquivos de áudio ou vídeo, que violem as leis de direitos autorais.

9.11.1.5.3. Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

9.11.1.5.4. O usuário deve fazer manutenção periodicamente nos recursos de armazenamento disponibilizados, tais como diretório local, diretórios de rede, pastas da intranet, evitando o acúmulo de informações desnecessárias.

9.11.1.5.5. Não são permitidas alterações das configurações de rede e inicialização das máquinas, bem como demais modificações que não sejam justificadas e efetuadas pela área de TI.

9.11.1.5.6. A área de TI não se responsabiliza pelo mau funcionamento de equipamentos ou softwares pessoais ou de terceiros.

9.11.1.5.7. Todos os equipamentos difusores de radiofrequência devem possuir homologação e licenciamento respeitando a legislação dos órgãos reguladores, não sendo permitida a instalação e operação de qualquer equipamento ou estrutura nas dependências da Belem Bioenergia sem as devidas tratativas de licenciamento junto aos órgãos reguladores e autorizados pela área de TI.

9.11.1.6. Os recursos de responsabilidade de TI estão listados abaixo:

Tabela 2 - Recursos de TI

Recursos de responsabilidade da TI	
Notebooks	Rádios
Aparelhos móveis (smartphones)	Computadores, Notebooks e seus periféricos (mouse, monitor, teclado)
Tablets	Impressoras

9.12. Padrão de Senhas:

9.12.1. Estabelecer um padrão de senhas para os usuários de TI no ambiente tecnológico da Companhia.

9.12.1.1. Diretoria Administrativo-Financeira

9.12.1.1.1. Aprovar periodicamente as regras para o estabelecimento do padrão de senhas no ambiente tecnológico da Belem Bioenergia.

9.12.1.2. Todos os Funcionários, Prestadores de Serviços e Administradores de Sistemas

9.12.1.2.1. Não anotar as senhas do ambiente corporativo em meios inseguros como bloco de notas, papel, smartphone etc.

9.12.1.2.2. A senha é de uso pessoal e intransferível, sendo proibido o seu empréstimo ou compartilhamento com terceiros, dentro ou fora da organização.

9.12.1.2.3. Não reutilizar senhas corporativas em ambientes tecnológicos pessoais.

9.12.1.2.4. Providenciar imediatamente a alteração de senhas, caso haja suspeita do comprometimento delas.

Tabela 3 – Padrão de Senhas

Atributo	Descrição	Configuração
Histórico de senhas	Número de senhas até que seja permitido reaproveitar uma senha já utilizada.	10 senhas

Duração máxima de senha	Tempo para que seja necessário alterar a senha. Após esse período, caso a senha não seja alterada pelo usuário, a conta de acesso será bloqueada até que a senha seja alterada ou que um administrador a desbloqueie.	90 dias corridos
Duração mínima de senha	Duração mínima em que o usuário deve permanecer com a mesma senha sem poder alterá-la.	0 dias corridos
Senha inicial e reinicialização (reset)	Senha inicial é a senha definida para o primeiro *logon* do usuário. A reinicialização ocorre quando o usuário esquece sua senha e solicita uma nova.	A senha inicial ou reinicializada deve ser gerada aleatoriamente e o usuário deve alterá-la em seu primeiro *logon*.
Tamanho mínimo da senha	Número mínimo de caracteres de uma senha.	8 caracteres
Complexidade	Requisita que a senha possua números, letras, maiúsculas, minúsculas e caracteres especiais, quando nativamente suportado pelo ambiente tecnológico.	3 ou mais requisitos de complexidade: • 1 letra maiúscula. • 1 letra minúscula. • 1 número. • 1 caractere especial. Bloqueio de palavras ou combinações comumente usadas e não permitidas.
Armazenamento de senhas	Define como a senha é armazenada no Ambiente Tecnológico Companhia.	Senhas devem ser armazenadas utilizando criptografia e algoritmos atualizados.
Tentativas incorretas de acesso	Número máximo de tentativas de acesso incorretas antes que seja efetuado o bloqueio da conta.	10 tentativas
Duração do bloqueio	Duração mínima do bloqueio de conta caso seja atingido o número de tentativas incorretas de acesso.	Até ser desbloqueada por um ADM de REDE

Duração do histórico de tentativas incorretas	Tempo durante o qual o histórico de tentativas incorretas de acesso é mantido. Após tal período o número de tentativas incorretas de acesso é zerado.	10 minutos

9.12.2. Regras de Privacidade

9.12.2.1. Quaisquer tentativas de monitorar, acessar áreas restritas, utilizar senha de terceiros ou capturar dados sem autorização, serão consideradas violação das diretrizes deste procedimento e poderão ocorrer sansões administrativas.

9.13.2.2. Em nenhuma hipótese os funcionários da Belem Bioenergia devem enviar por e-mail senhas, nomes de usuário ou outras informações relacionadas à rede corporativa.

9.13. Gestão de Acesso

9.13.1. Diretoria Administrativo-Financeira

9.13.1.1. Garantir que os direitos de uso do e-mail e internet sejam estabelecidos de acordo com as funções de negócio e necessidades do processo, devidamente aprovadas pelos gestores responsáveis.

9.13.1.2. Gerenciar e aprovar os gastos com os recursos de e-mail e internet.

9.13.2. Área de Tecnologia da Informação e Telecomunicações

9.13.2.1. Garantir que os acessos a banco de dados e aos sistemas de negócio em produção ou durante implementação (fase de projeto), cuja administração esteja sob a responsabilidade da área de Tecnologia da Informação, sejam concedidos somente a funcionários da Belem Bioenergia ou prestadores de serviço que possuam autorização formal, mediante solicitação. Coordenar o processo de revisão de acessos aos sistemas, garantindo que todos os direitos de acessos dos funcionários (e quando for o caso, prestadores de serviços) sejam revisados pelos seus gestores imediatos.

9.13.2.2. Monitorar periodicamente a existência de funcionários com conflitos não aprovados nos sistemas corporativos e coordenar o processo de tratamento com os gestores dos usuários (segregação de função).

9.13.2.3. Revogar, a qualquer momento, acessos e perfis de funcionários desligados.

9.13.2.4. Revogar, a qualquer momento, acessos e perfis por conta de realização de saneamento, diminuição de custos de licenças e demais motivações que justifiquem revogações.

9.13.2.5. Garantir que os acessos de suporte e manutenção, utilizados pela área de Tecnologia da Informação e Telecomunicações durante o período de operação assistida, sejam concedidos com data de validade previamente definidas e utilizados somente pela área de TI.

9.13.2.6. Gerir os perfis de acessos privilegiados, de acordo com matriz de responsabilidade definida pela área de TI, para gestão administrativa dos recursos e sistemas de TI.

9.13.2.7. Validar ou revisar os riscos de conflitos dos acessos relacionados aos sistemas de informação.

9.13.2.8. Garantir que usuários convidados possuam acesso restrito aos recursos corporativos.

9.13.3. Usuários dos Sistemas

9.13.3.1 Solicitar, quando necessário, a concessão ou revogação de credenciais e acessos aos sistemas de negócio através do portal de atendimento (Central de Serviços Bioenergia), de acordo com as funções de negócio desempenhadas pelo funcionário e baseado no princípio de mínimo acesso necessário.

9.13.4. Gestores dos Usuários dos Sistemas

9.13.4.1. Garantir que os acessos aprovados sejam compatíveis com as atividades executadas pelos funcionários ou prestadores de serviços.

9.13.4.2. Garantir a devida utilização das credenciais dos funcionários ou prestadores de serviços sob sua responsabilidade.

9.13.4.3. Garantir que as credenciais e acessos aos sistemas de negócio dos funcionários ou prestadores de serviços desligados sob sua responsabilidade sejam revogados imediatamente.

9.13.4.4. Indicar, para os prestadores de serviços quando for o caso, no momento da criação da credencial, a data correta de expiração dela, bem como a exclusão nos casos em que o prestador de serviço deixe a empresa antes do prazo de expiração previsto.

9.13.4.5. Solicitar, quando necessário, a revogação dos acessos de funcionários ou prestadores de serviços quando estes mudarem de função, de área ou de gestor.

9.13.4.6. Garantir que as credenciais dos respectivos funcionários ou prestadores de serviços sob sua responsabilidade não sejam compartilhadas.

9.13.4.7. Nomear os representantes de processos que devem validar, aprovar ou reprovar as alterações em perfis de acesso aos sistemas.

9.13.4.8. Validar ou revisar os riscos da segregação de função, relacionados aos sistemas de informação que suportam os processos sob sua responsabilidade, quando necessário.

9.13.5. Observações Importantes

9.13.5.1. Portal de Atendimento (Central de Serviços Bioenergia)

9.13.5.1.1. Portal disponível na Intranet, no qual os funcionários utilizam para fazer solicitações como: liberação de acesso a sistemas, instalação de desktops e notebooks, serviços de telefonia etc.

9.14. Recursos de Telefonia

9.14.1. Estabelecer diretrizes, responsabilidades e critérios para solicitação e utilização de serviços telefônicos na Companhia.

9.14.1.1. Diretoria Administrativo-Financeira

9.14.1.1.1. Garantir que os direitos ao uso dos recursos de telefonia móvel e fixa sejam estabelecidos de acordo com as funções de negócio e necessidades do processo, devidamente aprovadas pelos gestores responsáveis.

9.14.1.1.2. Gerenciar e aprovar os gastos com os recursos de telefonia móvel e fixa.

9.14.1.2. Usuários de Telefonia Companhia

9.14.1.2.1. Manter atualizadas as respectivas informações cadastrais.

9.14.1.2.2. Garantir a guarda e o bom estado de conservação dos equipamentos de telefonia.

9.14.1.2.3. Bloquear o acesso aos dados de seu smartphone e/ou placa de dados e priorizar o uso de redes sem fio (WI-FI) em viagens internacionais. Caso não seja possível, solicitar aprovação da diretoria para liberação de roaming de sinal.

9.14.1.2.4. Não alterar as configurações de software e/ou hardware, de forma que sejam utilizados fora do padrão da Belem Bioenergia ou que violem a garantia do equipamento.

9.14.1.2.5. Não fazer uso de equipamentos e softwares de comunicação que não sejam homologados pela TI.

9.14.1.3 Gestor dos Usuários de Telefonia da Belem Bioenergia

9.14.1.3.1. Acompanhar os gastos e o uso de linhas telefônicas fixas e móveis oferecidas pela Companhia aos seus funcionários, incluindo linhas compartilhadas, tratando os casos com desvio em relação aos limites estabelecidos.

9.14.1.3.2. Garantir que as linhas telefônicas sob sua responsabilidade tenham sempre um responsável associado no Grupo BBB, para garantir o controle do uso dos aparelhos individuais e compartilhados.

9.14.1.3.3. Aprovar serviços de telefonia condizentes com a utilização do negócio, baseado nas recomendações das tabelas abaixo de classes de serviço.

9.14.1.3.4. Arcar com as multas previstas em contrato, em seu respectivo centro de custo, em caso de cancelamento de serviço ou do aparelho antes do prazo contratual, quando solicitado pela área usuária.

9.14.1.3.5. Arcar com custos, em seu respectivo centro de custo, decorrente do mau uso dos recursos de telefonia pelos seus funcionários.

9.14.1.3.6. Não permitir que um aparelho móvel seja solicitado em nome de um funcionário da Belem Bioenergia e disponibilizado para utilização de um prestador de serviço.

Tabela 4 – Regras de Concessão de Serviços de Telefonia Móvel

Tipos de Serviços / Aparelhos	Perfil de Utilização	Nível de Aprovação	Exceções
Coletor	Líderes de equipe Agrícolas	Superior imediato com cargo gerencial.	Aprovação da gerência imediata.
Básico	Funcionários que expressem a necessidade para uso corporativo	Superior imediato com cargo gerencial.	Aprovação da gerência imediata.
Completo	Gerentes e superiores	Superior imediato	-

Tabela 5 – Classes de Serviços Disponíveis para Telefonia Fixa

Classes de Serviços	Ligações Internas	Ligações Locais	Ligações para Celular	DDD	DDI
Básico	X	X	X	X	
Completo	X	X	X	X	X

Tabela 6 – Perfis de Utilização para Telefonia Móvel

Classes de Serviço	Ligações Locais	DDD	DDI	Dados Móveis Locais	Dados Móveis Internacional
Coletores				X	
Básico	X	X		X	
Completo	X	X	X	X	X

9.14.1.4. Recomendações e Regras

9.15.1.4.1. O não cumprimento das regras e limites estabelecidos para recursos de telefonia poderá acarretar penalidades ao funcionário.

9.14.1.4.2. Smartphones devem ser utilizados por funcionários com frequente mobilidade nacional e internacional e que demandem comunicação fora dos escritórios da Belem Bioenergia.

9.14.1.4.3. A telefonia móvel somente será entregue após a devida assinatura do Termo de Responsabilidade digital/físico.

9.14.1.4.4. É importante ressaltar que a utilização de todos estes recursos poderá ser monitorada, e eventuais abusos serão analisados e reportados aos gestores imediatos.

9.14.1.4.5. A seleção da operadora é baseada na área de cobertura da região e política de preços praticados. A escolha de uma operadora diferente da indicada pela área de Tecnologia e Telecomunicações só deve ser feita quando houver inviabilidade técnica da operadora preferencial.

9.15. Serviços de E-mail e Internet

9.15.1. Estabelecer diretrizes, responsabilidades e critérios de utilização de serviços de e-mail e internet no Grupo Belem Bioenergia Brasil.

9.15.1.1. Diretoria Administrativo-Financeira

9.15.1.1.1. Garantir que os direitos de uso do e-mail e internet sejam estabelecidos de acordo com as funções de negócio e necessidades do processo, devidamente aprovadas pelos gestores responsáveis.

9.15.1.1.2. Gerenciar e aprovar os gastos com os recursos de e-mail e internet.

9.15.1.2. Área de Tecnologia da Informação e Telecomunicações:

9.15.1.2.1. Prover acesso à internet às localidades da Belem Bioenergia em que a operação demande conectividade e que necessitem dessa tecnologia.

9.15.1.2.2. Garantir a comunicação de dados entre as localidades da Belem Bioenergia.

9.15.1.2.3. Bloquear o acesso a sites e páginas restritas, garantindo a execução das atividades relacionadas ao trabalho, sendo assim fica vedado o uso dos recursos disponibilizados para uso pessoal.

9.15.1.2.4. Implementar mecanismos de segurança de prevenção contra possíveis ataques cibernéticos e vazamento de informação corporativa.

9.15.1.3. Todos os Funcionários, Prestadores de Serviços e Administradores de Sistemas

9.15.1.3.1. Utilizar o correio eletrônico corporativo para os objetivos e funções inerentes as suas atribuições funcionais, uso restrito ao cunho profissional.

9.15.1.3.2. Considera-se o uso inapropriado o envio de mensagens de correio eletrônico contendo:

9.15.1.3.2.1. Materiais obscenos, ilegais ou antiéticos;

9.15.1.3.2.2. Materiais preconceituosos ou discriminatórios;

9.15.1.3.2.3. Materiais caluniosos ou difamatórios;

9.15.1.3.2.4. Propagandas com objetivos comerciais;

9.15.1.3.2.5. Lista de endereços eletrônicos dos colaboradores da Belem Bioenergia;

9.15.1.3.2.6. Vírus, SPAM ou qualquer programa danoso;

9.15.1.3.2.7. Material de natureza político-partidária ou sindical;

9.15.1.3.2.8. Material protegido por leis de propriedade intelectual;

9.15.1.3.2.9. Entretenimentos e “correntes”;

9.15.1.3.2.10. Assuntos ofensivos;

9.15.1.3.2.11. Músicas, vídeos ou animações que não sejam de interesse específico do trabalho.

9.15.1.3.3. Considera-se o uso inapropriado a abertura de mensagens de correio eletrônico contendo:

9.15.1.3.3.1. Materiais obscenos, ilegais ou antiéticos;

9.15.1.3.3.2. Materiais preconceituosos ou discriminatórios;

9.15.1.3.3.3. Materiais caluniosos ou difamatórios;

9.15.1.3.3.4 Propagandas com objetivos comerciais;

9.15.1.3.3.5. Lista de endereços eletrônicos dos colaboradores da Belem Bioenergia;

9.15.1.3.3.6. Vírus, SPAM ou qualquer programa danoso;

9.15.1.3.3.7. Material de natureza político-partidária ou sindical;

9.15.1.3.3.8. Material protegido por leis de propriedade intelectual;

9.15.1.3.3.9. Entretenimentos e “correntes”;

9.15.1.3.3.10. Assuntos ofensivos;

9.15.1.3.3.11. Músicas, vídeos ou animações que não sejam de interesse específico do trabalho.

9.15.1.3.3.12. E-mail suspeito;

9.15.1.3.3.13. Mensagens que caracterizem phishing (mensagens recebidas com propósito de obter ilegalmente informações confidenciais, como senhas, logins etc.)

9.15.1.3.3.14. Faz parte da operação de TI enviar e-mail do tipo phishing para testar e monitorar a atenção dos colaboradores.

9.15.1.3.3.15. Em caso de dúvidas sobre e-mails suspeitos recebidos, o funcionário não deve abri-los e deve imediatamente entrar em contato com a área de TI.

9.15.1.4. Recomendações e Regras

9.15.1.4.1. É permitido o acesso à internet somente para fins de trabalho da Belem Bioenergia, sendo vedado o seu uso para assuntos pessoais.

9.15.1.4.2. O endereço eletrônico não deve ser divulgado ou utilizado para assuntos particulares.

9.15.1.4.3. A utilização de e-mail corporativo (envio e recebimento de mensagens) pelo funcionário está sujeita à auditoria em qualquer instante, mediante aprovação da área de Compliance ou Jurídica.

9.15.1.4.4. Toda mensagem eletrônica recebida poderá ser verificada em busca de vírus no momento de seu recebimento. Caso uma mensagem eletrônica seja recebida de um remetente desconhecido ou não habitual, a mesma deve ser excluída imediatamente, salvo mediante expressa instrução contrária pela área de TI.

9.15.1.4.5. Em nenhuma hipótese os funcionários devem trocar por e-mail senhas, nomes de usuários ou outras informações relacionadas às redes corporativas da Belem Bioenergia.

9.15.1.4.6. É proibida a divulgação, transmissão ou compartilhamento, de arquivos, programas, senhas e/ou nomes de usuários com destinatários não autorizados.

9.15.1.4.7. O colaborador não poderá anunciar ou associar assuntos relacionados a negócios (ou outros) da Belem Bioenergia em sites externos.

9.16 Serviços de Radiocomunicação VHF

9.16.1. Estabelecer diretrizes, responsabilidades e critérios de utilização de serviços de rádio comunicação VHF da Companhia.

9.16.1.1. Diretoria Administrativo-Financeira

9.16.1.1.1. Garantir que os direitos de uso dos serviços de radiocomunicação VHF sejam estabelecidos de acordo com as funções de negócio e necessidades do processo, devidamente aprovadas pelos gestores responsáveis.

9.16.1.1.2. Gerenciar e aprovar os gastos com os recursos de radiocomunicação VHF.

9.16.1.2. Área de Tecnologia da Informação e Telecomunicações

9.16.1.2.1. Prover comunicação às localidades da Belem Bioenergia em que a operação demande conectividade e que necessitem dessa tecnologia.

9.16.1.2.2. Controlar a distribuição dos radiocomunicadores VHF.

9.16.1.2.3. Garantir e zelar pelas infraestruturas de telecomunicação como torres, abrigos e links de dados para o pleno funcionamento do sistema de radiocomunicação.

9.16.1.2.4. Bloquear o acesso as comunicações, garantindo a plena execução das atividades relacionadas ao trabalho, sendo assim fica vedado o uso dos recursos disponibilizados para uso pessoal, bem como qualquer forma de utilização cujo conteúdo seja de natureza adulta, racista, religiosa, preconceituosa ou ofensiva.

9.16.1.2.5. Implementar mecanismos de segurança de prevenção contra falhas de comunicação VHF.

9.16.1.2.6. Garantir o pleno licenciamento dos equipamentos, frequências e estruturas junto aos órgãos reguladores.

9.16.1.3. Todos os Funcionários, Prestadores de Serviços e Administradores de Sistemas

9.16.1.3.1. Toda solicitação de novos equipamentos deverá ser feita mediante chamado através do portal de atendimento (Central de Serviços Bioenergia), e submetê-lo à aprovação do seu gestor imediato para posterior aquisição do hardware pela área de TI.

9.16.1.3.2. Deve-se tomar particular atenção com a salvaguarda destes equipamentos, devido à maior possibilidade de perda, em caso apurado de responsabilidade do funcionário, o mesmo deverá arcar com os custos e reposição do ativo. Os usuários de tais dispositivos são responsáveis pela sua conservação e manutenção geral do equipamento e seus acessórios.

9.16.1.3.3. Toda solicitação de manutenção deverá ser feita mediante chamado através do portal de atendimento (Central de Serviços Bioenergia), e o equipamento deverá ser encaminhado para a área de TI do respectivo polo para manutenção externa.

9.16.1.3.4. Caberá ao detentor, uma vez cessados os motivos e as condições pelos quais os equipamentos lhe foram destinados, devolver o equipamento sob sua responsabilidade, sendo dada baixa no respectivo Termo de Responsabilidade.

9.16.1.3.5. Certifique-se sempre de que a estação está sintonizada no canal correto de sua operação.

9.17.2. Recomendações e Regras

9.16.2.1. Fica vedado o compartilhamento de canais de radiocomunicação VHF que pertençam ao Grupo Belem Bioenergia para empresas terceiras sem a autorização da gerência de TI.

9.16.2.2. A comunicação via rádio é de uso exclusivo em atividades da Belem Bioenergia e o funcionário será o responsável pela guarda e segurança do aparelho.

9.16.2.3. É proibido a divulgação das frequências e licenças utilizadas nos equipamentos da Belem Bioenergia.

9.16.2.4. Fica vedado qualquer alteração das configurações de frequência, potência e modulação dos rádios portáteis e móveis que não sejam justificadas, autorizadas e efetuadas pela área de TI.

9.16.2.5. Não é permitido a utilização de equipamentos de radiofrequência não homologados e licenciados pelos órgãos reguladores (ex. Anatel).

9.16.2.6. Em nenhuma hipótese os funcionários ou prestadores de serviço devem encaminhar o equipamento de sua posse para manutenção em empresas terceiras. Esta atividade é de responsabilidade de TI.

9.17. Novas Solicitações / Demandas

9.17.1. Estabelecer diretrizes, responsabilidades e critérios para novas solicitações no ambiente tecnológico, incluindo hardware e software.

9.17.1.1. Coordenação de Tecnologia da Informação

9.17.1.1.1. Receber a nova solicitação, identificando se todas as informações necessárias foram inseridas.

9.17.1.1.2. Avaliar esforço e custo para atender a demanda solicitada.

9.17.1.1.3. Para novas solicitações de ativos e acessos, garantir que a necessidade seja avaliada de acordo com as funções de negócio e necessidades do processo.

9.17.1.1.4. Garantir a entrega adequada de acordo com a solicitação / demanda.

9.17.1.2. Todos os Funcionários, Prestadores de Serviços e Administradores de Sistemas

9.17.1.2.1 Identificar a necessidade, avaliando grau de urgência e impacto.

9.17.1.2.2 Criar requisição, detalhando todo o escopo da necessidade, para melhor avaliação da área de TI.

9.17.2. Recomendações e Regras

9.17.2.1. Em nenhuma hipótese os funcionários ou prestadores de serviço devem iniciar uma nova solicitação / demanda, sem o conhecimento prévio da Gerência de TI.

9.17.2.2. Todo desenvolvimento de software deve ser realizado pela área de TI, não sendo permitido as áreas realizarem qualquer tipo de desenvolvimento sem conhecimento prévio e a autorização pela área de TI.

9.17.2.3. É proibido realizar novas solicitações / demandas sem o devido registro no portal de atendimento (Central de Serviços Bioenergia).

9.17.2.4. O chamado pode ser rejeitado caso não tenha o formulário anexado ou não esteja preenchido as informações de forma clara, objetiva e com detalhes funcionais suficientes para análise.

9.17.2.5. Para novas contratações, a gerência responsável pela vaga, deverá solicitar com previsibilidade mínima de 15 dias úteis, antes do início do colaborador, todos os ativos necessários para desempenho das suas atividades, através de abertura de chamado no portal de atendimento (Central de Serviços Bioenergia).

9.18. Contratos de Tecnologia

9.18.1. Estabelecer diretrizes, responsabilidades e critérios para novos contratos de Tecnologia & Telecomunicações.

9.18.1.2. Gerência de Tecnologia da Informação

9.18.1.2.1. Identificar todos os contratos de TI.

9.18.1.2.2. Identificar todos os status sendo eles vencidos, a vencer ou vigentes.

9.18.1.2.3. Identificar necessidade de novos contratos.

9.18.1.2.4. Avaliar fornecedores para identificar necessidade de alteração, melhoria de regras contratuais, melhoria dos serviços e otimização de custos.

9.18.1.3. Todos os Funcionários, Prestadores de Serviços e Administradores de Sistemas

9.18.1.3.1. Identificar e informar a Gestão de TI a necessidade de contratação de software, hardware ou serviço de tecnologia.

9.18.2. Recomendações e Regras

9.18.2.1. É vetado a solicitação de novas contratações de software, hardware ou serviços de Tecnologia por qualquer área, sem o devido conhecimento e envolvimento da Gestão de TI.

9.18.2.2. Para renovação de contratos, é necessário que o pedido seja realizado com 6 (seis) meses de antecedência pela Gestão de TI, assim, as áreas envolvidas devem observar este prazo.

9.18.2.3. Para renovação ou novos contratos, é necessário que a Gerência de Suprimentos e Gestão Jurídica realizem todo processo dentro do prazo máximo de 6 (seis) meses, para mantermos o devido funcionamento dos serviços, respeitando assim, os prazos citados no item anterior.

9.19. Proteção de Dados Pessoais

9.19.1. Princípios

A Belem Bioenergia Brasil adota, no tratamento de dados pessoais, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, comprometendo-se a observá-los em todas as suas operações.

9.19.2. Agentes de Tratamento

A Belem Bioenergia Brasil atua como Controladora dos dados pessoais que coleta e trata no exercício de suas atividades. Fornecedores, terceirizados e parceiros que tratem dados pessoais por conta da Companhia são considerados operadores e devem fazê-lo estritamente conforme as instruções da Controladora, adotando medidas de segurança compatíveis com esta Política e observando as obrigações previstas nos respectivos instrumentos contratuais.

9.19.3. Encarregado pelo Tratamento de Dados

O Encarregado pelo Tratamento de Dados Pessoais (DPO) da Belem Bioenergia Brasil é Mateus Albuquerque Silva, Gestor do Departamento Jurídico, responsável por atuar como canal de comunicação entre a Companhia, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD). O contato com o DPO pode ser realizado pelo e-mail

mateus.silva@belembioenergia.com.br. As informações sobre o canal de atendimento ao titular e demais detalhes operacionais serão definidos em normativo específico.

9.19.4. Bases Legais

O tratamento de dados pessoais pela Companhia ocorre com fundamento nas bases legais admitidas pela legislação aplicável, podendo incluir, conforme o caso: cumprimento de obrigação legal ou regulatória, execução de contrato, proteção da vida, legítimo interesse da Controladora e consentimento do titular.

9.19.5. Direitos dos Titulares

São assegurados aos titulares de dados pessoais tratados pela Companhia os direitos previstos na legislação aplicável, incluindo acesso, correção, eliminação, portabilidade, revogação do consentimento e oposição ao tratamento. O exercício desses direitos será viabilizado por meio de canal próprio, cujas informações e fluxo de atendimento serão definidos em normativo específico.

9.19.6. Incidentes de Segurança envolvendo Dados Pessoais

Incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais devem ser comunicados à ANPD no prazo legal. Os responsáveis pela gestão de incidentes e o procedimento detalhado de resposta, incluindo prazos, notificações e registros, serão definidos em normativo específico.

9.19.7. Obrigação dos Operadores

No que se refere ao tratamento de dados pessoais, os fornecedores e terceirizados que atuem como Operadores devem: adotar medidas técnicas e administrativas de segurança compatíveis com esta Política; tratar os dados pessoais somente conforme as instruções da Companhia e para as finalidades contratualmente previstas; não subcontratar o tratamento de dados pessoais sem autorização prévia e por escrito da Belem Bioenergia Brasil; e cooperar com a Companhia no atendimento a solicitações de titulares e autoridades competentes.

9.20. Regras de Mesa Limpa e Tela Limpa

9.20.1. Estabelecer diretrizes para proteção de informações físicas e digitais em ambientes de trabalho:

9.20.1.1. Gerência de Políticas de Bloqueio de Tela

9.20.1.1.1. Configurar bloqueio automático de tela nos dispositivos corporativos após período máximo de inatividade de 15 (quinze) minutos.

9.20.1.1.2. Garantir que todas as estações de trabalho bloqueiem a tela e, ao abrir, que a tela esteja com autenticação habilitada.

9.20.1.2. Todos os Funcionários

9.20.1.2.1. Manter a área de trabalho livre de documentos físicos contendo informações corporativas ao se ausentar do posto, mesmo que temporariamente.

9.20.1.2.2. Bloquear a tela do computador (via função de teclado) sempre que se afastar do equipamento.

9.20.1.2.3. Guardar documentos impressos sensíveis em gavetas ou armários com fechadura ao término do expediente ou ao se ausentar por período prolongado.

9.20.1.2.4. Não deixar senhas, credenciais ou informações de acesso anotadas em locais visíveis, como monitores, teclados ou superfícies da mesa de trabalho.

9.20.1.2.5. Recolher imediatamente documentos impressos de impressoras compartilhadas, não permitindo que permaneçam disponíveis para acesso por terceiros.

9.20.1.3. Regras e Recomendações

9.20.1.3.1. O descumprimento das regras de mesa limpa e tela limpa será tratado como incidente de segurança da informação, sujeitando o responsável às medidas disciplinares previstas nesta Política.

9.20.1.3.2. A área de TI poderá realizar verificações periódicas de conformidade, sem aviso prévio, para fins de auditoria interna.

9.21. Gestão de Vulnerabilidades

9.21.1. Estabelecer diretrizes para identificação, avaliação, priorização e tratamento de vulnerabilidades no ambiente tecnológico da Companhia.

9.21.1.1. Gestão de relatórios Mensais

9.21.1.1.1. Realizar varreduras periódicas de vulnerabilidades em ativos críticos de TI, com frequência mínima bimestral, utilizando ferramentas homologadas pela área de TI.

9.21.1.1.2. Conduzir ou contratar testes de intrusão (Pentest) ao menos uma vez ao ano, ou após mudanças significativas na infraestrutura.

9.21.1.1.3. Classificar as vulnerabilidades identificadas por critério de criticidade (crítica, alta, média, baixa), estabelecendo os seguintes prazos máximos de tratamento a partir da identificação: crítica até 30 dias corridos; alta até 60 dias corridos; média até 120 dias corridos; baixa com planejamento no ciclo seguinte.

9.21.1.1.4. Manter processo de gestão de patches (atualizações de segurança) com janelas de manutenção previamente definidas e comunicadas às áreas impactadas.

9.21.1.1.5. Registrar e documentar todas as vulnerabilidades identificadas, ações de remediação adotadas e justificativas para eventuais exceções aceitas formalmente pela Diretoria.

9.21.1.2. Vulnerabilidades não tratadas dentro dos prazos estabelecidos deverão ser formalmente reportadas à Gestão da TI, com plano de mitigação e prazo revisado.

9.21.1.2.1. É vedada a divulgação de vulnerabilidades identificadas fora dos canais internos autorizados, sendo considerada violação desta Política.

9.22. Gestão de Mudanças

9.22.1. Estabelecer diretrizes para o gerenciamento formal de mudanças no ambiente tecnológico da Companhia, assegurando que alterações em ambientes produtivos sejam avaliadas, aprovadas e executadas de forma controlada, minimizando riscos operacionais. O registro e acompanhamento das mudanças é realizado através da Central de Serviços Bioenergia.

9.22.1.1. Gestão de Mudanças

9.22.1.1.1. Garantir que toda mudança em ambiente de produção seja registrada previamente no portal de atendimento (Central de Serviços Bioenergia), com descrição do escopo, impacto esperado, plano de rollback e responsável pela execução.

9.22.1.1.2. Classificar as mudanças conforme sua natureza: Mudança Padrão/urgente.

9.22.1.1.3. Submeter mudanças normais à avaliação do gestor responsável e, quando de alto impacto, à aprovação da Diretoria Administrativo-Financeira, antes de qualquer implementação.

9.22.1.1.4. Definir e comunicar às áreas impactadas a janela de manutenção planejada para execução da mudança, preferencialmente em horários de menor criticidade operacional.

9.22.1.1.5. Garantir a existência e o teste prévio do plano de rollback para toda mudança classificada como normal ou emergencial.

9.22.1.2. Todos os Funcionários

9.22.1.2.1. Não realizar alterações em ambientes de produção sem o devido registro e aprovação no portal de atendimento (Central de Serviços Bioenergia), conforme previsto no item 9.18.

9.22.1.3. Recomendações e Regras

9.22.1.3.1. Mudanças realizadas sem o processo formal estabelecido neste item serão consideradas não autorizadas e sujeitas às medidas disciplinares previstas nesta Política.

9.22.1.3.2. Todo incidente originado por mudança não autorizada implicará apuração de responsabilidade do executor.

9.23. Trabalho Remoto e Uso de Dispositivos Pessoais (BYOD)

9.23.1. Estabelecer diretrizes para o acesso remoto seguro aos sistemas e recursos corporativos da Companhia, bem como para o uso de dispositivos pessoais (BYOD — Bring Your Own Device) no exercício das atividades profissionais.

9.23.1.1. Gerência de Tecnologia da Informação e Telecomunicações

9.23.1.1.1. Prover solução de acesso remoto corporativo (VPN ou equivalente homologado) para s colaboradores autorizados a trabalhar remotamente.

9.23.1.1.2. Garantir que o acesso remoto seja protegido por autenticação multifator (MFA), sendo vedado o acesso remoto a sistemas corporativos sem esse controle.

10. MECANISMOS DE EFETIVAÇÃO

10.1. Implementação de Tecnologias de Segurança: Utilização de firewalls, sistemas de detecção de intrusões (IDS), sistemas de prevenção de intrusões (IPS), antivírus e criptografia para proteger sistemas e dados contra ameaças cibernéticas.

10.2. Controle de Acesso Avançado: Implementação de políticas de senhas fortes e períodos de expiração, além de monitoramento contínuo de acesso para garantir que apenas usuários autorizados tenham acesso aos recursos adequados.

10.3. Auditorias e Avaliações Regulares: Realização de auditorias de segurança periódicas e avaliações de vulnerabilidades para identificar e corrigir possíveis brechas de segurança antes que se tornem problemas sérios.

10.4. Gestão de Identidades e Acessos (IAM): Utilização de soluções de IAM para centralizar o gerenciamento de identidades de usuários, políticas de acesso e revisões periódicas de privilégios.

10.5. Treinamento Contínuo em Segurança: Implementação de programas regulares de treinamento e conscientização em segurança da informação para todos os funcionários, focando em ameaças atuais, práticas seguras e políticas organizacionais.

10.6. Resposta a Incidentes e Planos de Continuidade de Negócios: Desenvolvimento e teste de planos de resposta a incidentes detalhados, que incluam procedimentos claros para detectar, conter, mitigar e recuperar-se de violações de segurança. Além disso, é essencial ter planos de continuidade de negócios para manter operações críticas durante e após incidentes.

10.7. Monitoramento e Relatórios: Implementação de sistemas de monitoramento contínuo de segurança da informação para detectar comportamentos suspeitos e incidentes em tempo real. Além disso, elaboração de relatórios regulares para a alta administração sobre o estado da segurança da informação e as ações tomadas.

10.8. Revisão e Atualização Constantes: Revisão periódica da política de segurança da informação para garantir que esteja alinhada com novas ameaças, regulamentações e mudanças no ambiente operacional da organização. Isso inclui atualizações para refletir novas tecnologias, práticas de segurança emergentes e lições aprendidas com incidentes anteriores.

11. GESTÃO DE CONSEQUÊNCIAS

11.1. A todos os abrangidos por esta Política que observarem quaisquer desvios às premissas estabelecidas aqui, poderão relatar o fato aos canais disponíveis na empresa, conforme norma específica com a disponibilização dos meios de comunicação, podendo ou não se identificar.

11.2. Não serão permitidas retaliações contra aquele que, de boa-fé, denunciar ou manifestar queixa, suspeita, dúvida ou preocupação relativa a possíveis violações às diretrizes desta política;

11.3. Internamente, o não cumprimento das premissas desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem conforme a respectiva gravidade do descumprimento.

12. DIVULGAÇÃO

12.1. Após aprovada pela Diretoria Administrativo-Financeira, a presente Política será divulgada pela área de Segurança da Informação às áreas e partes interessadas;

12.2. Quaisquer situações, exceções e/ou esclarecimentos sobre a aplicação desta Política devem ser enviadas à área de Segurança da Informação;

12.3. A presente Política deve ser observada em conjunto com outras políticas, normas e procedimentos adotados pela Companhia.

13. CASOS OMISSOS

13.1. Casos omissos a esta Política deverão ser tratados pela área de Segurança da Informação.

14. EXCEÇÕES

14.1. As exceções a essa Política deverão ser claras, transparentes, taxativas e aprovadas pela Diretoria Administrativo-Financeira.

15. DISPOSIÇÕES FINAIS

15.1. A presente Política entrará em vigor na data de sua aprovação pela Diretoria Administrativo-Financeira. Sua atualização e vigência observarão o disposto no item 3.1

16. ANEXOS

Termo de Responsabilidade: Documento impresso ou digital que deve ser assinado pelos colaboradores, prestadores de serviços e administradores de sistemas, confirmando que estão cientes e concordam em seguir a Política de Segurança da Informação da Belem Bioenergia Brasil.