POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A política de Segurança da Informação da Belfort tem como objetivo estabelecer os princípios, diretrizes e responsabilidades em relação aos ativos da informação e informações clínicas, visando proteger suas propriedades de confidencialidade, disponibilidade e integridade.

2. ÂMBITO E VALIDADE

As diretrizes estabelecidas neste documento devem ser observadas pela Belfort e aplicam-se também a todos os ativos, equipamentos, software básico e aplicativos de propriedade da Belfort ou de entidade parceira, assim como aqueles contratados em qualquer regime.

Ela se aplica a todas as pessoas físicas e jurídicas, inclusive administradores, prestadores de serviços, parceiros e/ou quaisquer outros terceiros que mantenham um relacionamento com a Belfort e que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da referida empresa e de seus clientes, cujo acesso seja controlado.

Esta política possui validade de dois anos, a contar do dia seguinte à sua publicação, e deverá ser cumprida por todos os empregados, parceiros, consultores, especialistas ou pessoas contratadas em regime temporário, estagiários, menores aprendizes e pessoas integrantes do quadro de pessoal de empresas contratadas.

Ao final da sua vigência, ela será revisada e renovada para o mesmo período subsequente (dois anos), sem prejuízo de ser alterada em período anterior conforme a determinação da Diretoria.

3. DIRETRIZES

Esta política foi formulada de acordo com a missão, valores corporativos, e visão estratégica da Belfort, além da objetivar a conformidade com as legislações vigentes e melhores práticas com relação a segurança da informação.

Desse modo, 3 pilares devem ser estabelecidos com a finalidade de garantia da segurança da informação:

- Confidencialidade: Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário.

- Integridade: Garante que a Informação esteja íntegra e completa durante todo o seu ciclo de vida.

- Disponibilidade: Garante que a Informação esteja disponível para as pessoas autorizadas, sempre que se fizer necessária.

4. DEFINIÇÕES

Informação: Dados (eletrônicos ou físicos), ou registros de um sistema devidamente processados.

Dados pessoais: Dados específicos a um indivíduo, definidos através da LGPD.

Tratamento de dados: Toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Titular dos dados: pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento.

Ativo: Tudo aquilo que possui ou constitui valor para a organização.

Ativos de Informação: Conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa. Trata-se de patrimônio intangível da empresa, constituído por suas informações de qualquer natureza, incluindo aquelas de caráter estratégico, técnico, administrativo, mercadológico, financeiro, de recursos humanos ou legais, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, compra, licenciamento, ou confiadas a organização por funcionários, parceiros, clientes, fornecedores, terceiros, em formato escrito, verbal, físico, digitalizado, que seja armazenado, transitado ou trafegado pelas estruturas da empresa , além de documentos em suporte físico ou mídia eletrônica que transitarem interna ou externamente a estrutura física da empresa.

Sistemas de Informação: Sistemas computacionais utilizados pela empresa para suportar suas operações. Pode haver exceções que, mesmo não sendo sistemas informáticos, suportem operações da empresa.

Ameaça: Causa potencial de um acidente, que possa vir a comprometer ou prejudicar da organização.

Confidencialidade: Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário.

Acordo de Confidencialidade: É o documento formal, juridicamente respaldado, contendo a descrição de uso permitido da informação, tempo de duração, responsabilidades, utilização da informação e consequências por violação do acordo.

Integridade: Garante que a Informação esteja íntegra, exata e completa durante todo o seu ciclo de vida.

Disponibilidade: Garante que a Informação esteja disponível para as pessoas ou organismos autorizados, sempre que se fizer necessária.

Risco de Segurança da Informação: Efeito da incerteza sobre os objetivos da Segurança da Informação da organização.

Incidente de Segurança: É toda a ação que viole as políticas internas, tais como: quaisquer ações ou situações que possam expor a Belfort a perdas financeiras ou de imagem, direta ou indiretamente, potenciais ou reais, uso indevido de dados corporativos ou institucionais, divulgação não autorizada de informações ou de segredos comerciais e industriais sem a autorização expressa dos proprietários ou área competente, uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, a não comunicação imediata de quaisquer violações ou atitudes

Controle: medida de segurança adotada pela organização, para tratamento de um risco específico.

Segregação de funções: Consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de maneira que nenhum colaborador, visitante, estagiário ou prestador de serviços, detenha poderes e atribuições em desacordo com este princípio, ou conflitantes entre si.

Informações da organização: Ativos de Informação que se relacionem diretamente à organização, suas atividades, dados de clientes, fornecedores, funcionários, estagiários, visitantes ou terceiros, e qualquer tipo de dado ou informação gerada ou alterada por membros da empresa, no exercício de suas funções.

Diretoria: órgão responsável pela administração geral da Belfort cabendo-lhe, precipuamente, cumprir e fazer cumprir normas legais e regulamentares.

Recursos Humanos: Setor responsável pelo processo de seleção e administração dos empregados, inclusive das contratações pontuais para suprir eventuais faltas e/ou limitação de pessoal.

Contas a Pagar e a Receber: Setor responsável pelo pagamento dos fornecedores e elaboração da DRE, mas que também, quando necessário, atua na área de Recursos Humanos.

Administrativo da Usina: Setor responsável pela administração dos empregados da Usina, cumprimento das obrigações legais, e a gestão da referida unidade como, por exemplo, a compra de materiais, controle dos carros, dentre outros pontos.

LGPD – Lei Geral de Proteção de Dados: Lei n. 13.709/18, promulgada em 14 de agosto de 2018, que define as normas e procedimentos para o tratamento de dados pessoais.

Aplicativos de Mensagens: WhatsApp, Telegram, face time, Skype, Facebook, Messenger, Instagram, Twitter e outros que tenham finalidade igual ou similar.

Gestor: Supervisor, Coordenador, Gerente ou Diretor.

5. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Em caso de violação desta Política e Normas de Segurança da Informação:

- O usuário da informação deverá comunicar imediatamente o seu gestor e o Setor de Recursos Humanos qualquer incidente que possa trazer impactos na segurança dos ativos organizacionais (informação ou recursos de processamento).

- A comunicação com o Setor de Recursos Humanos deverá ser feita por e-mail para o endereço eletrônico: seguranca@belfortambiental.com.br

- Após a comunicação, o Setor de Recursos Humanos, em conjunto com o de Contas a Pagar e a Receber, recomendará aos Diretores uma ação disciplinar a ser tomada.

- Os usuários da informação não deverão testar fragilidades de segurança, pois tais eventos serão interpretados como uso impróprio do sistema/exploração de vulnerabilidades.

- Os demais casos serão tratados pelo fluxo normal de resposta a incidentes.

6. RESPONSABILIDADES

As responsabilidades relativas a esta Política são pertinentes a todos os colaboradores, estagiários, visitantes, fornecedores e prestadores de serviço, cabendo ressaltar que todos deverão

- Ler, compreender, e cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da informação da organização, como também, quaisquer outras leis ou normas de segurança aplicáveis;

- Encaminhar quaisquer dúvidas e/ou pedido de esclarecimento sobre a atual política, suas normas e procedimentos, ao Setor de Recursos Humanos ou Contas a Pagar e a Receber;

- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela organização;

- Assegurar que os recursos tecnológicos, as informações, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização;

- Cumprir as normas que regulamentam a propriedade intelectual;

- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou áreas expostas (aviões, transporte, restaurantes, encontros sociais, etc.) incluindo a emissão de comentários e opiniões em blogs, páginas e redes sociais;

- Não compartilhar informações confidenciais de qualquer tipo;

- Comunicar imediatamente ao Setor de Logística qualquer descumprimento ou violação desta política e/ou de suas Normas e Procedimentos, ou qualquer evento que coloque ou possa colocar em risco a segurança das informações da organização.

6.1 Diretoria

- Prover os recursos necessários para o cumprimento da Política de segurança da Informação;

- Assegurar que a Política de Segurança da Informação é compatível com os objetivos e estratégias corporativas.

- Demonstrar liderança e comprometimento com a Política de Segurança da Informação, incentivando sua aplicação, e dando suporte moral e executivo para a execução da mesma;

- Assegurar que a Política de Segurança da Informação consegue atingir seus objetivos.

- Avaliar, rejeitar e/ou aprovar eventuais alterações da Política de Segurança da Informação sugeridas pela Logística em conjunto com o Setor de Recursos Humanos e o de Contas Pagar e a Receber.

6.2 Comitê de Proteção de Dados e da Segurança da Informação

- Atuar como enlace fundamental entre a Diretoria da Belfort e as demais área de Segurança da Informação, garantindo a fluidez de comunicação entre as mesmas;

- Reunir-se periodicamente ou extraordinariamente, analisando e tomando decisões sobre eventos e incidentes de Segurança da Informação;

- Observar as modificações políticas, estruturais e estratégicas da empresa, levando tais mudanças para que sejam refletidas na Política de Segurança da Informação.

6.3 Recursos Humanos

- Adequar e configurar equipamentos e aplicativos para correta utilização dos recursos de Tecnologia da Informação, atentando inclusive para que os requisitos de segurança para os negócios da Belfort sejam identificados e que os controles de segurança estejam adequadamente implementados, operados e mantidos de acordo com esses padrões;

- Viabilizar condições tecnológicas para monitoração da utilização dos recursos de Tecnologia da Informação disponíveis aos usuários, informando a ocorrência de incidentes de segurança e a percepção de violações desta política, visando a aplicação das penalidades e/ou providências cabíveis.

- Desenvolver e manter atualizada a política de Segurança da Informação;

- Monitorar o seu cumprimento, de forma proativa e sob demanda, sempre que solicitado por alguma área de negócio da Belfort;

- Definir e executar e/ou coordenar o programa de conscientização de usuários em Segurança da Informação;

- Identificar, planejar e coordenar programas para melhoria da segurança das informações, implementando e aprimorando os controles em todos os recursos tecnológicos e em projetos e processos de negócio;

- Prover consultoria e suporte às áreas, sob quaisquer requerimentos de segurança para as áreas de negócios, análises técnicas e seleção de controles apropriados, e verificar/auditar a implementação, manutenção e operação destes controles;

- Homologar em conjunto com as demais áreas de tecnologia todos os recursos de Tecnologia da Informação, com foco em segurança, atentando sempre para Disponibilidade, Integridade e Confidencialidade das Informações;

- Revisar os impactos na segurança do ambiente tecnológico quando da alteração dos atuais recursos, inclusão de novos recursos, ou devido à aquisição de serviços e ativos da informação, emitindo parecer sobre as necessidades de adequação dos mesmos antes de iniciarem suas operações;

- Comunicar às áreas responsáveis a identificação de ocorrências de incidentes de segurança, para que medidas disciplinares cabíveis sejam adotadas;

- Manter registros e documentação de segurança em nível corporativo, incluindo um banco de dados de riscos e assuntos de segurança;

- Avaliar o risco de assuntos relacionados à segurança e comunicar os eventuais problemas às áreas competentes, provendo suporte nas eventuais ações preventivas e/ou corretivas;

- Registrar formalmente todos os incidentes de segurança da informação identificados e/ou reportados;

- Detectar, identificar e registrar violações, ou, tentativas de acessos relevantes e significativas não autorizadas, para tomada de providências corretivas, legal e de auditoria;

- Monitorar os acessos visando verificar: vazamento de informações; acessos ou tentativas de acessos a sites com conteúdo inadequado, repasse de conteúdo inadequado, tentativa de quebra de controles de segurança da informação e armazenamento de arquivos multimídia que não façam parte do negócio da Belfort;

- Revisar anualmente as regras de proteção estabelecidas;

- Restringir e controlar os acessos e os privilégios de usuários, incluindo os daqueles com privilégios de acesso remoto e externo;

- Em qualquer tempo ou momento, solicitar a restrição, bloqueio, suspensão e/ou cancelamento de acessos e/ou tecnologias (hardware e/ou software) que estejam infringindo as políticas de segurança ou nos casos em que sejam verificados incidentes de segurança, ou em que haja identificação de vulnerabilidades que necessitem de tempo para serem analisadas e se possível, corrigidas.

- Analisar, juntamente com o Setor de Contas e, se for o caso, o Administrativo da USINA, eventuais alterações na Política de Segurança da Informação, com o envio da minuta para a Diretoria Colegiada para fins de aprovação.

- Obter a ciência do colaborador no termo de compromisso e responsabilidade sobre a política de Segurança da Informação no ato da admissão, e mantê-lo arquivado no prontuário dele;

- Orientar a Gerência das áreas na aplicação das medidas disciplinares quando cabíveis;

- Desenvolver e implementar, em conjunto com a área de Segurança da Informação, programas de capacitação e conscientização dos usuários sobre o uso adequado dos recursos disponibilizados pela empresa e sobre Segurança da Informação;

- Comprometer-se com o suporte estratégico no desenvolvimento de ações de divulgação desta política;

- Divulgar no processo de integração (treinamento) para todos os usuários (colaboradores, prestadores de serviços e terceiros) que tiverem acesso aos ativos da informação, as principais diretrizes definidas por esta política.

6.4 Contas a Pagar e a Receber

- Dar apoio ao Setor de Recursos Humanos nas atribuições acima delineadas, inclusive assumindo tais tarefas quando não puderem ser realizadas pelo RH;

- Monitorar o cumprimento de Políticas, Normas e Procedimentos internos;

- Avaliar os riscos e suficiência dos controles envolvidos nas falhas operacionais e, quando aplicável, registrar ocorrência de risco;

- Comunicar os eventuais problemas às áreas competentes, provendo suporte nas eventuais ações preventivas e/ou corretivas;

- Encaminhar para registro formal pelo Setor de Recursos Humanos todos os incidentes de segurança da informação identificados e/ou reportados.

6.5 Administrativo da USINA

- Dar apoio na USINA quanto a adequação e configuração de equipamentos e aplicativos para correta utilização dos recursos de Tecnologia da Informação, atentando inclusive para que os requisitos de segurança para os negócios da Belfort sejam identificados e que os controles de segurança estejam adequadamente implementados, operados e mantidos de acordo com esses padrões;

- Viabilizar na USINA condições tecnológicas para monitoração da utilização dos recursos de Tecnologia da Informação disponíveis aos usuários, informando a ocorrência de incidentes de segurança e a percepção de

violações desta política, visando a aplicação das penalidades e/ou providências cabíveis.

- Monitorar na USINA o cumprimento da Política de Segurança da Informação, de forma proativa e sob demanda, sempre que solicitado por alguma área de negócio da Belfort;

- Auxiliar no âmbito da USINA o Setor de Recursos Humanos a identificar, planejar e coordenar programas para melhoria da segurança das informações, implementando e aprimorando os controles em todos os recursos tecnológicos e em projetos e processos de negócio;

- Comunicar às áreas responsáveis da USINA, após comunicação aos Setor de Recursos Humanos, a identificação de ocorrências de incidentes de segurança, para que medidas disciplinares cabíveis sejam adotadas;

- Detectar, identificar e comunicar violações, ou, tentativas de acessos relevantes e significativas não autorizadas na USINA, para tomada de providências corretivas, legal e de auditoria;

- Em qualquer tempo ou momento, solicitar a restrição, bloqueio, suspensão e/ou cancelamento de acessos e/ou tecnologias (hardware e/ou software) na USINA que estejam infringindo as políticas de segurança ou nos casos em que sejam verificados incidentes de segurança, ou em que haja identificação de vulnerabilidades que necessitem de tempo para serem analisadas e se possível, corrigidas.

- Auxiliar o Setor de Recursos Humanos a desenvolver e implementar, no âmbito da USINA, programas de capacitação e conscientização dos usuários sobre o uso adequado dos recursos disponibilizados pela empresa e sobre Segurança da Informação;

- Comprometer-se com o suporte estratégico no desenvolvimento de ações de divulgação desta política;

- Divulgar no processo de integração (treinamento) para todos os usuários (colaboradores, prestadores de serviços e terceiros) que tiverem acesso aos ativos da informação, as principais diretrizes definidas por esta política.

6.6 Gestores/Líderes de Áreas

- Assegurar que os colaboradores estejam conscientes da importância da prática da boa segurança nas atividades diárias, e solicitar/providenciar educação e treinamento adequados e apropriados às suas responsabilidades, incluindo aspectos relevantes da legislação, regulamentos, direitos autorais e contratos;

- Segregar as funções de aprovação de operações, execução e controle das mesmas, de modo que nenhuma pessoa possa ter completa autoridade sobre uma parcela significativa de qualquer processo;

- Assegurar que as permissões de acesso aos sistemas dos seus colaboradores estejam sempre atualizadas, contendo as devidas solicitações e aprovações de acesso, revendo-as também em caso de transferências e/ou desligamentos;

- Acompanhar o cumprimento dessa política e assegurar que os riscos de Segurança em suas áreas de atuação estejam avaliados e controlados adequadamente;

- Orientar suas equipes sobre o uso adequado das informações e recursos de informações disponibilizados pela empresa;

- Sempre que necessário, devem documentar orientações específicas, regulamentando os níveis de confidencialidade das informações que geram e processam, bem como os direitos de acesso a essas informações;

- Comunicar ao Setor de Recursos Humanos, o Setor de Contas a Pagar e/ou o Setor Administrativo da USINA os casos de descumprimento de Políticas, Normas ou Procedimentos internos, e os casos de falhas na execução de atividades operacionais.

- Prover informações necessárias para a identificação e tratamento de riscos e incidentes de Segurança da Informação.

6.7 Usuários dos recursos de TI

Entende-se por usuário todos que obtiverem acesso aos recursos e ativos de informação da Belfort.

- Manter-se atualizado com relação às políticas da Belfort, devendo periodicamente consultar os documentos normativos, disponíveis na intranet;

- Obedecer a legislação e os regulamentos vigentes, padrões de conduta da Belfort e determinações existentes nesta política;

- Fazer uso adequado das informações e dos recursos tecnológicos e/ou físicos disponibilizados pela empresa em suas atividades diárias;

- Utilizar somente softwares e hardwares disponibilizados pela Belfort, devidamente homologados e com autorização de uso;

- Assegurar que não haverá má utilização dos recursos tecnológicos e/ou físicos sob sua guarda e protegê-los de mau uso por terceiros;

- Zelar por ter uma postura ética e segura na utilização dos recursos e informações da Belfort;

- Ter postura zelosa, diligente e evitar excesso de exposição;

- Reportar à sua gerência e à área de Segurança da Informação quaisquer suspeitas de falha de segurança, em quaisquer de seus controles.

7. AUDITORIA E GOVERNANÇA CORPORATIVA

Todas as informações produzidas, acessadas, armazenadas ou distribuídas pelos recursos disponibilizados pela Belfort poderão ser monitoradas e controladas.

O acesso e uso das informações corporativas e pessoais para o desempenho de atividades de monitoramento e auditoria na Belfort são restritas às áreas de Tecnologia da Informação e Segurança da Informação.

Os recursos disponibilizados pelo sistema Belfort são para uso dos colaboradores no desempenho das atividades profissionais.

O processo de monitoramento e auditoria é autorizado exclusivamente para atender o objetivo de averiguar o cumprimento das diretrizes corporativas, identificar conteúdo e/ou acessos indevidos, detectar fraudes ou coletar evidências para suportar a companhia em processos judiciais ou em atendimento às auditorias externas, órgãos reguladores e fiscalizadores.

Os acessos às informações com finalidade diversa das acima citadas serão interpretados como uso impróprio.

Em caso de ocorrência de incidente de segurança ou fraude as áreas competentes deverão ser imediatamente notificadas pelo gestor responsável para, em conjunto com a área jurídica estabelecer critérios de guarda de provas eletrônicas.

A Belfort reserva o direito de registrar e examinar todos os eventos relacionados ao acesso à Internet, a fim de garantir que os recursos não estejam sendo utilizados de forma indevida, ou, para fins não autorizados.

Relatórios regulares são emitidos, constando os comportamentos de acesso que podem vir a interferir no tráfego de dados, e tentativas de acessos a sites de conteúdos considerados impróprios para o ambiente corporativo. A navegação e o conteúdo exibido nos recursos computacionais da Organização são controlados e armazenados para auditoria, sendo possível, gerar relatórios de acesso por usuário.

8. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações classificam-se em duas categorias:

I – Ostensivas: são dados ou informações cujo acesso é irrestrito e não há precauções adicionais a serem tomadas quanto ao seu manuseio. Subdividem-se em:

a) Públicas: informação que não expõe a Belfort a riscos e que, por imposição legal ou quando autorizada por seu gestor, pode ser divulgada sem restrição ao público em geral e distribuição externa. Ex.: informações voltadas ao público externo (clientes, mercado, imprensa etc.), documentos e contratos públicos etc.;

b) Internas: informação com base em interesse negocial e de acordo com as normas internas, que pode ser divulgada sem restrição, apenas, ao público interno e partes externas interessadas, com anuência do gestor da informação ou por imposição legal. Todos os documentos não classificados serão considerados com essa classificação. Ex.: Manuais e outros normativos da Instituição.

II – Sigilosas: são dados ou informações cujo conhecimento irrestrito ou divulgação pode acarretar qualquer risco à segurança da Instituição, do Estado e da sociedade, como os necessários ao resguardo da inviolabilidade da intimidade, da honra e da imagem das pessoas. Quando estritamente necessária a divulgação, o acesso deverá ser autorizado por seu gestor e monitorado. Caso a matéria seja encaminhada para fora da Organização, padrões de segurança adicionais devem ser estabelecidos. O material contendo essa informação deve ser rotulado com a expressão “Informação Sigilosa”. Subdividem-se em:

a) Reservadas: informação que exige cuidados especiais quanto à preservação das suas propriedades e cuja divulgação indevida expõe a Belfort a riscos significativos. Ex.: Votos, Atas de Reuniões da Diretoria, informações sobre o balanço contábil da Belfort antes de sua divulgação oficial, etc.;

b) Secretas: informação cuja preservação das suas propriedades é fundamental para a continuidade dos negócios da Belfort e de seus objetivos e que a divulgação indevida sujeita a Instituição a riscos elevados. Ex.: documentos ou informações de cunho estratégico.

c) Sigilo Legal: informação cujo sigilo é previsto em lei específica. Tais informações não são classificadas, pois já têm seu sigilo garantido por outras legislações. Exemplo: sigilo fiscal, sigilo bancário, sigilo comercial, entre outros.

9. NÃO CONFORMIDADE

Definição

A não conformidade está definida na presente Política como a violação, omissão, tentativa não consumada, ou ausência de cumprimento com quaisquer das definições, diretrizes, normas, procedimentos ou conceitos definidos nesta Política de Segurança da Informação, voluntária ou involuntariamente, por parte de um colaborador, estagiário, visitante, fornecedor ou prestador de serviços.

Determinação

Qualquer colaborador, estagiário, visitante, fornecedor ou prestador de serviços pode denunciar uma suspeita de não conformidade com a Política de Segurança da Informação.

A referida denúncia deve ser efetuada verbalmente, ou (preferencialmente) por escrito, para a de Recursos Humanos ou para um gestor de qualquer área da empresa, que, por sua, vez, deve encaminhar a denúncia ao Setor de Recursos Humanos.

Dispositivos e procedimentos de monitoramento e verificação de Segurança da Informação também, podem indicar possíveis violações ou não cumprimentos. As formas de comunicação através destes dispositivos ou procedimentos devem estar definidas nas Normas e Procedimento da Segurança da Informação.

A determinação final sobre a procedência da suspeita, ou veracidade das informações relativas à Segurança da Informação cabe somente ao Setor de Recursos Humanos, que em conjunto com o Setor de Contas a Pagar e a Receber e o Administrativo da USINA, este último apenas quando o caso envolver a USINA, encaminhará à Diretoria as informações sobre o ocorrido e as sugestões para as medidas cabíveis.

Ação

As regras que estabelecem o controle e o tratamento de situações de não conformidade relativas à Política de Segurança da Informação da organização devem ser tratadas conforme as leis vigentes no país, que regulamentem as punições correspondentes ao evento.

Na ocorrência de violação desta Política ou das Normas de Segurança da Informação, a Diretoria poderá adotar, com apoio da Área de Recursos Humanos e o Setor de Contas a Pagar e a Receber, as sanções administrativas e/ou legais, conforme os parágrafos a seguir:

Colaboradores e Estagiários

As punições serão aplicadas conforme análise da Área de Recursos Humanos, o Setor de Contas a Pagar e a Receber, e o Administrativo da USINA (este último quando o caso se referir à USINA), devendo-se considerar a gravidade da

infração, efeito alcançado, recorrência, e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho.

10. CASOS OMISSOS

O presente documento, e a totalidade dos responsáveis citados no mesmo, devem considerar que a tecnologia e as ameaças à Segurança da Informação se intensificam e se atualizam todos os dias.

Portanto, não se constitui rol enumerativo, sendo obrigação do usuário da organização adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir a proteção às informações da empresa.

Os eventuais casos que não estejam contemplados neste documento, ou nos documentos auxiliares que o compõem, devem ser analisados, em primeira instância, pela Área de Recursos Humanos, o Setor de Contas a Pagar e a Receber, e o Administrativo da USINA (este último quando o caso se referir à USINA), e, caso o mesmo não tenha uma solução ou medida plausível para o evento, caberá à Diretoria decidir o procedimento para cada caso específico.

11. DOCUMENTOS DE REFERÊNCIA

- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação, incluindo sua versão original e posteriores atualizações.
- NBR 11.175/90.
- Lei do Marco Civil da Internet e suas respectivas alterações
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, “LGPD”.
- Lei federal 11.846 – Anticorrupção e Política de Relacionamento com Órgãos Públicos.
- Contrato Social da Belfort.
- Lei Estadual de Goiás n. 13.123/1997.
- Resolução CONAMA n. 313/02.

12. GESTÃO DA POLÍTICA

Esta Política da Segurança da Informação foi homologada pelo Comitê de Privacidade e Segurança da Informação, sendo aprovada pela Diretoria no dia 09/12/2021

APROVAÇÕES

Elaboração:	**Revisão**	**Aprovação**
Por: Encarregada Em: Ass:	Por: Comitê de PD e SI Em: Ass:	Pela: Diretoria Em: Ass: