BELFORT

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

BE PL 01-01

Política de Segurança da Informação - PSI

1. OBJETIVO.

A **Política de Segurança da Informação - PSI** do **GRUPO BELFORT** tem por objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, assegurando os princípios básicos de segurança da informação: disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam os objetivos estratégicos do **GRUPO BELFORT**, protegendo-as contra acessos não autorizados, uso indevido, divulgação, perda, alteração ou destruição.

2. ABRANGÊNCIA E DESTINATÁRIOS.

Esta Política se aplica a todos os colaboradores, empregados, estagiários, aprendizes prestadores de serviços e aos eventuais visitantes que tenham acesso a quaisquer informações ou que lidam com as informações do **GRUPO BELFORT**, independentemente do formato em que se encontram (física, digital ou eletrônica).

Todos, indistintamente, são responsáveis pela observação e cumprimento da Política de Segurança da Informação.

3. DAS DEFINIÇÕES, DIRETRIZES E PRINCÍPIOS.

3.1. Definições.

Para os efeitos desta **Política de Segurança da Informação** consideram-se as seguintes definições:

- **Ativo de informação:** Patrimônio intangível do **GRUPO BELFORT**, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas à Organização por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da Organização ou por infraestrutura

externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física;

- **Segurança da Informação:** conjunto de ações que tem como principal objetivo a proteção de um grupo de informações, para que seja preservado o valor que estas possuem ante um indivíduo ou empresa;
- **Informação:** conjunto de conhecimento adquirido por meio do tratamento de dados;
- **Dados:**
  - **Dado:** todo e qualquer registro existente, englobando, inclusive, os Dados Pessoais;
  - **Dado Pessoal:** registro relacionado a pessoa natural identificada ou identificável;
  - **Dado Pessoal Sensível:** registro sobre origem racial/étnica, saúde, vida sexual, caráter religioso, filosófico, político, sindical, e dados genéticos e biométricos;
  - **Titular:** pessoa a quem se referem os dados objeto de tratamento;
  - **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados para uma determinada finalidade.
- **Tratamento de Dados:** qualquer operação realizada com os dados;
- **Risco:** riscos associados à violação da confidencialidade, disponibilidade e integridade das informações tratadas pela empresa;
- **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da Organização;
- **Comitê de Segurança da Informação:** grupo formado por membros da Diretoria, da Equipe de Tecnologia da Informação, Equipe de Segurança da Informação, Equipe de Compliance e Jurídico, sendo no mínimo 3 e no máximo 5;
- **Encarregado de Segurança da Informação:** Membro do Comitê de Segurança da Informação responsável por receber e responder quaisquer demandas decorrentes desta Política, ainda que oriundas de órgãos e pessoas externas da empresa; e
- **Usuário:** Empregados (Colaboradores) com vínculo empregatício de qualquer área da Organização ou terceiros alocados na prestação de serviços, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar ou manipular qualquer ativo de informação da Organização para o desempenho de suas atividades profissionais.

3.2. Princípios.

Firmam-se como bases desta Política os seguintes **princípios**:

- **Confidencialidade:** garantir que o acesso ao banco de dados e às informações tratadas pela empresa será feito apenas por pessoal devidamente autorizado;

- **Integridade:** garantir que os dados contidos na empresa serão tratados com ética, para a finalidade pela qual foram coletados, e que com segurança quanto à sua qualidade; e
- **Disponibilidade:** garantir que os dados e as informações estejam disponíveis para acesso do pessoal autorizado sempre que necessário.

3.3. Diretrizes.

Para instruir o processo de tratamento dos dados, devem ser observadas as seguintes **diretrizes**:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **Livre Acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados;
- **Qualidade:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não Discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos e/ou abusivos; e
- **Responsabilização:** adoção de medidas eficazes, capazes de comprovar a observância e cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4. DAS MEDIDAS PREVENTIVAS E DE SEGURANÇA.

Estabelece-se a Gestão de Acessos, definindo quem pode acessar, como pode acessar e quando pode acessar o banco de dados da empresa, no intuito de garantir a confidencialidade dos dados ali armazenados.

- **Classificação de Dados:** os dados são categorizados de acordo com sua criticidade para o negócio, a fim de abrandar vulnerabilidades, conforme as seguintes classes:
  - Irrestrito
  - Restrito (uso interno)
  - Confidencial
  - Secreto
- **Níveis de Acesso aos Dados:** conforme as classificações apontadas acima, o Comitê de Segurança da Informação define e cataloga, deixando saber os colaboradores:
  - Qual(is) colaborador(s) pode(m) acessar o banco de dados;
  - A maneira com que estes dados podem ser acessados pelo pessoal autorizado;
  - A frequência com que estes dados podem ser acessados pelo pessoal autorizado.
- **Controle de Acessos:** ratifica-se a necessidade de os acessos serem rastreáveis, para o referido controle destes.

4.1. Procedimentos.

Para assegurar a aplicabilidade dos princípios e diretrizes dispostos nesta Política, devem ser observados por todos os colaboradores, no mínimo, os seguintes **procedimentos**:

- A troca de senhas (tanto do computador quanto dos softwares utilizados pela empresa) de todo e qualquer colaborador deverá ser feita, obrigatoriamente, a cada 90 (noventa) dias corridos, ou em prazo menor quando solicitado;
- O Setor de Tecnologia da Informação será o responsável por atestar que a troca de senhas foi realizada com sucesso junto a todos os colaboradores da empresa;
- Caberá ao Setor de Tecnologia promover a alteração das senhas do wi-fi da empresa e dos servidores a cada 90 (noventa) dias, não podendo essa senha ser informada a qualquer colaborador. Eventual necessidade de se utilizar o wi-fi deverá ser solicitada ao Setor de Tecnologia da Informação, ao qual caberá anotar a senha diretamente no computador do solicitante;
- Os colaboradores não deverão acessar sites que não sejam estritamente vinculados ao trabalho realizado na empresa, sendo vedado, por exemplo, o acesso a e-mails particulares, sites de notícias, músicas, redes sociais, esportivos, entretenimento e quaisquer outros que não tenham justificativa profissional para o acesso;

- Os colaboradores não deverão utilizar a rede da empresa (inclusive wi-fi) para fins particulares;
- Os colaboradores não deverão clicar em links e anexos suspeitos, tanto de sites quanto recebidos em e-mails. Na dúvida, deverão contatar o Setor de Tecnologia da Informação para buscarem maiores informações sobre os links e anexos;
- Os colaboradores não deverão disponibilizar o e-mail de trabalho para fins particulares, tendo ciência de que o e-mail profissional poderá ser acessado, a qualquer tempo, pela Diretoria da empresa, sem que isso caracterize violação de sigilo ou privacidade;
- Os colaboradores não poderão, de forma alguma, disponibilizar a terceiros toda a produção realizada pela empresa, estando cientes que responderão por perdas e danos caso o façam, sem prejuízo de demais penalidades aplicáveis;
- Os colaboradores não deverão salvar em arquivos particulares (e inclusive enviar para e-mails particulares) quaisquer dados e informações da empresa e de seus clientes, independente do formato;
- Os colaboradores não deverão utilizar *pendrives* ou outros hardwares particulares nos computadores da empresa, visando a evitar eventuais contaminações de vírus;
- Os colaboradores não deverão utilizar *pendrives* ou outros hardwares da empresa para fins particulares, observando que a propriedade deles é da empresa, podendo ser acessados a qualquer tempo pela Diretoria;
- Os colaboradores não deverão instalar softwares particulares (ou que não tenham vinculação alguma com o trabalho profissional desenvolvido na empresa) nos computadores da empresa, sendo que toda e qualquer instalação de software deve ser feita exclusivamente pelo Setor de Tecnologia da Informação;
- Os colaboradores deverão armazenar as informações na rede da empresa;
- Os colaboradores deverão se assegurar de descartar devidamente informações que não sejam mais necessárias;
- Os colaboradores deverão identificar eventuais vulnerabilidades e nomeá-las ao Comitê de Segurança da Informação;
- Os colaboradores deverão denunciar imediatamente incidentes ao Comitê de Segurança da Informação;
- Os colaboradores que utilizarem seus computadores da empresa de forma externa deverão estar cientes da responsabilidade de guarda e conservação sobre o bem, respondendo objetivamente por todo e qualquer problema, vício, perda, extravio, furto ou roubo que ocorrer;
- Os colaboradores não deverão utilizar o telefone da empresa (fixo ou celular eventualmente disponibilizado) para fins particulares;

- Os colaboradores devem evitar deixar líquidos destampados e comidas em suas mesas, evitando, com isso, incidentes nos materiais da empresa;
- Os coordenadores deverão observar o comportamento de sua equipe, além de inspecionar o bom uso de seus recursos.
- Os colaboradores devem se manter cientes do monitoramento integral dos dispositivos fornecidos pela empresa.
- A empresa fornece aos seus Colaboradores o uso de seus ativos, incluindo, equipamentos, dispositivos eletrônicos e sistemas de tecnologia da informação, que devem ser usados apenas para fins comerciais legítimos;
- A empresa reserva-se o direito de inspecionar, monitorar e controlar o uso desses ativos a qualquer momento, incluindo os sistemas de e-mail e demais formas de comunicação eletrônica.
- A equipe de tecnologia poderá auditar qualquer computador sem prévia comunicação, verificando: Que tipo de informação o usuário pode acessar; Quem está autorizado a acessar determinada rotina e/ou informação; Quem acessou determinada rotina e informação; Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação; Que informação ou rotina determinado usuário acessou; Quem tentou acessar qualquer rotina ou informação sem estar autorizado.
- O colaborador não deverá copiar, gravar, fotografar ou reproduzir as informações de segredos comerciais, industriais, financeiro e de pessoal do Grupo Belfort de outra forma que não com a finalidade de utilizar tais informações ou materiais de obra atribuída ao colaborador para o exercício de seus deveres e responsabilidades, independentemente da função exercida.

Qualquer informação gerada, recebida ou armazenada em um desses sistemas é propriedade do GRUPO BELFORT.

4.1.1. Política Interna para Armazenamento de Dados.

Para que os dados, informações, documentos e arquivos sejam armazenados de forma adequada, as regras abaixo devem ser seguidas.

As regras descritas nesta política se aplicam tanto aos documentos e arquivos, seja em formato físico ou digital.

- Documentos que contenham dados pessoais e informações de clientes e colaborares, devem ser salvos/armazenados dentro da pasta específica de cada cliente e colaborador.

- É expressamente proibido salvar/armazenar qualquer documento que contenha dados e informações de clientes e colaboradores, fora de suas respectivas pastas/fichas ou fora do servidor.
- Os colaboradores do **GRUPO BELFORT** são proibidos de salvar qualquer conteúdo com dados e informações de clientes e colaboradores em suas máquinas pessoais, pen drives, HD externo, CD/ROM, etc...
- O objetivo dessas regras é evitar o acesso aos arquivos/documentos/informações por pessoas não autorizadas.
- Os dados pessoais de clientes e colaboradores devem sempre ser armazenados em formato que favoreça o exercício do direito de acesso do titular.
- Os colaboradores devem garantir que todas as informações físicas e eletrônicas, sejam mantidas em local seguro quando não estiverem em uso.
- O colaborador do **GRUPO BELFORT** ao armazenar documentos físicos, deverá garantir que o conteúdo do documento não seja acessado por pessoas desautorizadas.
- Os documentos físicos devem ficar armazenados em ambientes seguros. Não podem ser deixados em cima de sua mesa de trabalho quando não estiver em uso, ou em locais onde mais de uma pessoa, que não estão autorizadas a ler seu conteúdo, tenham o acesso facilitado.
- Armários com documentos de clientes e colaboradores devem ser mantidos trancados quando não estiverem em uso.
- As chaves de acesso para as informações, devem estar somente na posse das pessoas autorizadas.

4.1.2. Política de E-mail Corporativo.

A presente Política de E-mails ("Política") define as diretrizes para o uso aceitável do e-mail da empresa ("E-mail Corporativo") pelos funcionários, incluindo acesso à intranet. O objetivo desta Política é promover uma comunicação profissional, eficiente e segura, proteger informações confidenciais e preservar a imagem da empresa.

Esta Política se aplica a todos os funcionários da empresa, independentemente de cargo ou função. O uso do E-mail Corporativo é um privilégio e não um direito, e o funcionário se responsabiliza por seguir as normas aqui descritas.

- **E-mail Corporativo:** Refere-se ao endereço de e-mail fornecido pela empresa ao funcionário, na forma [nome.sobrenome]@[URL inválido removido].br.
- **Intranet:** Refere-se à rede interna da empresa, acessível através do E-mail Corporativo.

- **Conteúdo Inaceitável:** Refere-se a qualquer conteúdo que viole as leis ou regulamentações aplicáveis, os princípios éticos da empresa ou que possa prejudicar a imagem da empresa ou de terceiros.

- **Uso Aceitável do E-mail Corporativo:** O E-mail Corporativo deve ser utilizado exclusivamente para fins profissionais relacionados à atividade do funcionário na empresa. São exemplos de uso aceitável:
  - Comunicação interna com colegas, clientes e fornecedores;
  - Envio e recebimento de documentos relacionados ao trabalho; e
  - Acesso à intranet.

- **Conteúdo Inaceitável:** É proibido o envio ou recebimento de e-mails com conteúdo inaceitável, incluindo, mas não se limitando a:
  - Linguagem ofensiva, difamatória ou ameaçadora;
  - Conteúdo pornográfico ou obsceno;
  - Conteúdo ilegal ou que viole direitos autorais;
  - Spam, correntes ou mensagens promocionais não solicitadas;
  - Vírus, malwares ou outros softwares maliciosos; e
  - Informações confidenciais da empresa ou de terceiros.

- **Segurança e Confidencialidade:** O funcionário é responsável por proteger a confidencialidade das informações acessadas ou transmitidas através do E-mail Corporativo. São exemplos de medidas de segurança:
  - Manter senha forte e confidencial;
  - Não compartilhar a conta de e-mail com terceiros; e
  - Sair da conta de e-mail ao finalizar o uso.

- **Responsabilidades:**
  - Seguir as normas desta Política;
  - Utilizar o E-mail Corporativo de forma responsável e profissional;
  - Proteger a confidencialidade das informações acessadas ou transmitidas; e
  - Denunciar imediatamente qualquer violação desta Política.

4.1.3. Política da "Mesa Limpa".

Também visando à implementação de medidas simples de segurança da informação, instaura-se, de imediato, a **política da "mesa limpa",** por meio da qual nenhum tipo de dado ou

informação pode ser deixado à vista, independente da forma, observando-se, ainda, o seguinte:

- É obrigação de cada colaborador providenciar o bloqueio do computador sempre que se retirar da sua mesa, ainda que por curto período. Ao se ausentarem da empresa para retorno em outro dia, deverão desligar seu computador e também a tela utilizada se for apartada;
- É obrigação de cada colaborador providenciar para que papéis, lembretes, documentos e outros sejam guardados sempre que o responsável por estes se retirar da mesa.
- Visando à confidencialidade das informações da empresa, de seus colaboradores e de seus clientes, não é permitido utilizar como rascunhos papéis que contenham ou possa conter informações sigilosas ou protegidas por lei, tais como: contratos privados, cópias de documentos pessoais, extratos bancários, documentos que contenham algum dado sobre menores, documentos que contenham dados sensíveis de quaisquer pessoas físicas, informações pessoais de qualquer indivíduo etc.
- Os papéis deverão ser previamente rasgados em partes mínimas (preferencialmente em fragmentadora) e posteriormente descartados de forma a impossibilitar seu uso ou a extração de quaisquer dados e informações.

4.1.4. Política de Redes Sociais.

Devido ao fato de serem utilizadas mundialmente e armazenarem dados pessoais, as redes sociais devem ser usadas com cautela e segurança, evitando, assim, o vazamento de informações e imagens sem autorização.
O **GRUPO BELFORT** possui contas oficiais nas principais redes e mídias sociais que servem como uma importante ferramenta de comunicação com o público e de divulgação e transparência das suas ações.

O uso do nome e/ou da imagem do **GRUPO BELFORT** e de suas Marcas em redes sociais deverá observar estritamente as normas dessa Política e não poderá ser associado a partidos políticos/campanhas político-partidárias, bebidas alcoólicas, cigarros, drogas, jogos de azar, agressividade, violência, armas, exploração sexual, exploração de mão-de obra escrava ou infantil, redes/sites de relacionamento e paquera, operações/atividades fraudulentas ou ilícitas, ou qualquer iniciativa considerada inapropriada, a critério exclusivo do **GRUPO BELFORT**.

Para fins de publicação nas redes sociais, antes da divulgação de qualquer conteúdo, o solicitante deverá encaminhar ao **GRUPO BELFORT** o layout das peças (cards, vídeos,

banners, peças animadas, etc.) para a prévia aprovação.

O **GRUPO BELFORT** não autoriza o uso do nome e da imagem de suas Marcas em contas/perfis de redes sociais com conteúdo em desacordo com a presente Política.

Por isso, alguns cuidados devem ser tomados. Seguem algumas recomendações:

- Não publicar dados e informações internas da organização tanto de colaboradores quanto de clientes. Em caso de violação destas diretrizes, o **GRUPO BELFORT** realizará a denúncia da publicação e seguirá com processos internos para garantir a exclusão da mesma.
- Não clicar em qualquer link que seja enviado por outras pessoas ou que apareça na tela, sem antes saber do que se trata.
- Não repassar informações ou dados pessoais para terceiros.
- Todos os colaboradores são responsáveis pelos conteúdos publicados e escritos nas mídias sociais. Portanto, orientamos que as publicações sejam feitas na primeira pessoa do singular (eu) para deixar claro que você está falando por si próprio e que todos os conteúdos que está publicando não representam oficialmente o posicionamento da empresa.
- As informações sigilosas e de propriedade exclusiva (como apresentações, planilhas, novos produtos e materiais internos) do **GRUPO BELFORT** não podem ser divulgadas e nem detalhadas para terceiros. Portanto, não comente a respeito de informações confidenciais, planos ou perspectivas relacionadas ao **GRUPO BELFORT**. Os materiais de comunicação interna recebidos podem ser compartilhados de acordo com a orientação do **GRUPO BELFORT**. Além disso, não faça referência ou cite qualquer um de nossos clientes ou parceiros sem que haja uma prévia autorização por parte deles.
- Não é permitido posicionamento algum em nome do **GRUPO BELFORT**, independentemente do seu cargo e/ou hierarquia. Há perfis designados pelos setores de Marketing das unidades de negócio ou Comunicação Corporativa, que possuem autorização para falar em nome do **GRUPO BELFORT** nas mídias sociais.
- O uso da nossa marca do **GRUPO BELFORT** ou de qualquer elemento referente a ela, em materiais como roupas, brindes, impressos ou mídias eletrônicas, só será permitido quando houver uma autorização da Diretoria. Caso contrário, a utilização da marca e de seus elementos não será permitida.
- O uso do aparelho celular durante o horário de trabalho nas áreas produtivas não é permitido. Assim, garantimos a sua segurança e a de seus colegas, evitando acidentes.

- É proibido fotografar o ambiente de trabalho, materiais com informações estratégicas, slides de apresentação, telas de computador e tudo o que esteja dentro da empresa. Isso garante mais segurança e privacidade aos nossos colaboradores, bem como aos nossos processos internos.

5. SANÇÕES E PUNIÇÕES.

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições será realizada conforme a análise do Comitê Diretivo, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o **Comitê de Segurança da Informação**, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

No caso de terceiros contratados ou prestadores de serviço, o Comitê Diretivo deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao **GRUPO BELFORT**, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

6. CASOS OMISSOS.

Os casos omissos serão avaliados pelo **Comitê de Segurança da Informação** para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do **GRUPO BELFORT** adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção das informações.

7. COMPROMISSO.

Os colaboradores declaram-se cientes que toda e qualquer situação que envolva ou tenha o potencial de envolver os pontos tratados nesta Política deverá ser comunicada de imediato ao **Comitê de Segurança da Informação** ou ao **Encarregado de Segurança da Informação**, ainda que por meio de aviso anônimo.

8. DISPOSIÇÕES FINAIS.

A presente **Política de Segurança da Informação** deverá, obrigatoriamente, ser revista em periodicidade anual, ou, quando necessário, em menor prazo, para que esteja sempre em conformidade com a legislação em vigor, inclusive a Lei Geral de Proteção de Dados.

9. HISTÓRICO DAS REVISÕES.

Elaborado por:	Aprovado por:
DocuSigned by: Bruno Gobb 552977007D64469... 06 de maio de 2024 Jurídico	DocuSigned by: Marcus Sandin A3EA711E3E4348E... 08 May 2024 CEO

Data	Revisão	Descrição
27/10/2023	02	Inclusão do Histórico de Revisões.
06/05/2024	03	Revisão Geral.