



Título

Política de Segurança da Informação

Data de Emissão	Data de Revisão	Versão	Páginas	Classificação Segurança
22/04/2025	22/04/2025	1.0	14	Público

Sumário

1. Introdução
2. Aplicação
3. Objetivo
4. Normas legais aplicáveis à Política
5. Diretrizes Gerais
 - 5.1. Gestão de usuário
 - 5.1.1. Responsabilidades
 - 5.1.1.1. Tecnologia da Informação
 - 5.1.1.2. Recursos Humanos
 - 5.1.1.3. Gerentes e Gestores
 - 5.1.1.4. Usuários – **Stakeholders** internos e externos
 - 5.2. Uso do **e-mail**
 - 5.3. Uso da **internet** e outros meios virtuais
 - 5.4. Cuidados com o ambiente digital e documentos eletrônicos
 - 5.5. Cuidados com o ambiente de trabalho e documentos físicos
 - 5.6. Cuidados com **Usuários** e **Senhas**
6. Violações e sanções
7. Canais de atendimento dos titulares de Dados
8. Atualizações e **Status** da Política

1. INTRODUÇÃO

A **Incopostes Indústria e Comércio de Postes Ltda.**, doravante denominada como "**Incopostes**" ou "**Empresa**" pessoa jurídica de direito privado inscrita no CNPJ/MF sob nº 05.433.048/00001-07, com sede na Rodovia BR 376, s/nº, km 11, Lotes 08 e 09 e 03 e 04, Distrito Industrial de Sumaré, na cidade de Paranaíba-PR, que com profissionalismo e seriedade permanece no mercado há 38 anos, comungando dos preceitos legais e visando conferir a transparência aos procedimentos de tratamento de dados pessoais, aderindo, observando e cumprindo integralmente a Lei Geral de Proteção de Dados, doravante denominada de "**LGPD**", **INSTITUI** a presente **Política de Segurança da Informação**, doravante denominada de "**Política**", contendo regras simples e claras para o suas partes interessadas, **stakeholders** internos e externos, a fim de evidenciar o seu compromisso com a privacidade e proteção de dados pessoais.

2. APLICAÇÃO

Elaboradora da Política	Kayamut Consultoria em Sustentabilidade Empresarial- CNPJ/MF 52.742.014/0001-84 Responsável técnica: Marcela Virginia Thomaz-Advogada OAB/PR 18.095
Aprovador da Política	Fabio Belmonte Pimentel / Laisi F. M. Garrido / Vilmar Jose Marques
Organização	Incopostes Indústria e Comércio de Postes Ltda.
Titulares Impactados	Funcionários, Colaboradores, Estagiários, Aprendizes, Prestadores de Serviços, Contratados, Temporários, Fornecedores, Terceiros, Sócios, Parceiros de negócio, Sócios, Clientes, Cadeia de Suprimento/Fornecimento e qualquer indivíduo ou organização que possua vínculo com a Incopostes Indústria e Comércio de Postes Ltda.

3. OBJETIVO

A finalidade da presente **Política** é a de estabelecer normas e diretrizes que garantam a segurança das informações que circulam na **Empresa**, garantindo a integridade digital, física e verbal destas informações.

Ao estabelecer esta **Política**, a **Empresa** não só cumpre com a legislação em vigor, como também enriquece seu Programa de Integridade, trazendo robustez para sua Governança e se alinhando à Agenda ESG que está em construção na **Empresa**, mas principalmente, consolida a sua seriedade com o compromisso, que aqui declara, de garantir a gestão da informação para alcançar os resultados desejados, no que se refere à mitigação de riscos, prevenção e redução de efeitos indesejados e contínua melhoria no acesso às informações disponíveis em seus ambientes.

Para garantir a segurança desses ativos, esta **Política** será pautada nos seguintes pilares:

1. **Confidencialidade:** informação acessível apenas para pessoas autorizadas;
2. **Integridade:** informação correta, confiável, sem a ocorrência de mudanças não autorizadas;
3. **Disponibilidade:** informação sempre acessível para uso legítimo de pessoas autorizadas.

4. NORMAS LEGAIS APLICÁVEIS À POLÍTICA

As normas legais aplicáveis nesta **Política** são:

- Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais-LGPD;
- Lei nº 12.965/2014, o Marco Civil da Internet;
- NBR ISO/IEC 27.001, 27.002 e 27.701; e
- Outras normas e procedimentos internos que são constantemente revisados e aprovados pelas alçadas competentes e disponibilizados a todos os colaboradores, prestadores de serviços e terceiros, aplicáveis ao caso.

5. DIRETRIZES GERAIS

Considerando os pilares desta **Política**, a **Empresa** determina padrões e diretrizes para orientar todos os **stakeholders** internos e externos que de forma diária, rotineira ou eventualmente, tenham acesso às informações, dados pessoais e sistemas da **Empresa**.

Para tanto, todos os **stakeholders** internos e externos, sem exceção, devem observar as seguintes diretrizes:

5.1. GESTÃO DE USUÁRIOS

O controle de acesso tem acolhida no **Princípio da Necessidade**, conforme redação do art. 6º, III, da **LGPD**, que determina que o acesso à informação, aos dados pessoais e informações de titulares terceiros só poderá e deverá ocorrer quando constatar que a permissão de acesso é indispensável para o desempenho das funções e atividades laborais.

Por este motivo, a concessão de acesso será definida tanto de acordo com a necessidade como pela análise da atividade desempenhada pelo colaborador ou pelo prestador de serviço e será realizada mediante solicitação do Setor de Recursos Humanos ou gestor imediato à equipe de Tecnologia da Informação, podendo, inclusive, se dar por um período limitado, para realizar atividades pontuais que não estão no escopo de atuação do funcionário.

As regras abaixo deverão ser observadas no controle de acesso:

- a) Somente usuários previamente identificados e autorizados podem ter acesso aos ativos de informação da **Empresa**;
- b) Para acessar os sistemas, aplicativos ou demais ativos de informação, **os usuários deverão digitar seu login e senha**, servindo como modo de identificação e autenticação;
- c) Para a definição dos critérios a serem usados no controle de acesso, deve-se considerar o seguinte:
 - c.1) A natureza do utilizador (isto é, colaborador ou terceiros relacionados à empresa);
 - c.2) As funções existentes na empresa (por exemplo, diretores, gerentes, colaboradores etc.).
- d) As aplicações controlarão o acesso do usuário através de mecanismos que regulem o acesso, evitando permissões privilegiadas;
- e) Não se deve permitir o acesso anônimo a qualquer recurso dentro da plataforma de tecnologia disponível na **Empresa**;
- f) As telas de abertura de programas/aplicativos que solicitam credenciais **devem mostrar o mínimo de informação na tela de login, além disso, as senhas não devem ser exibidas no procedimento de entrada**;
- g) Os identificadores serão automaticamente bloqueados após três tentativas de acesso fracassadas. Bloqueios automáticos podem ser mais restritivos se as aplicações os garantem com base na importância dos ativos de informação que gerenciam;
- h) Todas as tentativas de conexão, sejam autorizadas ou falhas, devem gerar um registro.

5.1.1 PAPÉIS E RESPONSABILIDADES

5.1.1.1. TECNOLOGIA DA INFORMAÇÃO

A equipe de Tecnologia da Informação será responsável pela criação e atualização dos acessos, separados por função, evidenciando o cargo e a necessidade, ou, prestação de serviço. É imprescindível que a equipe Tecnologia da Informação alinhe diálogo horizontal com o Setor de Recursos Humanos e com gestores internos para garantir que todos os acessos sejam concedidos, alterados ou bloqueados de forma regular e em conformidade com as diretrizes impostas.

Desse modo, a equipe também será responsável por conceder, alterar e cancelar os acessos de usuários a diretórios e sistemas após o recebimento da solicitação, constatando informações para realizar os ajustes das permissões quando verificado que o acesso é excessivo e não condiz com a necessidade do usuário – como pode ocorrer, por exemplo, quando há uma mudança interna de cargo/função e o acesso tenha se tornado desnecessário.

A **EMPRESA** deverá estabelecer procedimentos para o controle do uso de recursos computacionais e de acesso à rede local por clientes, prestadores de serviços, fornecedores ou terceiros que, eventualmente, estejam realizando algum serviço nas instalações da **EMPRESA**.

Estes procedimentos devem definir barreiras lógicas, procedimentos de vigilância e outras medidas que se façam necessárias para controlar ou impedir o acesso de pessoas não pertencentes ao quadro de colaboradores ou prestadores de serviços da **EMPRESA**.

5.1.1.2. RECURSOS HUMANOS

Caberá ao Setor de Recursos Humanos comunicar, através do e-mail, à equipe de Tecnologia da Informação sobre a necessidade de criação, concessão, alteração ou cancelamento de acessos de usuários, além de informar, de forma imediata, a alteração de cargo ou o desligamento de colaboradores, como uma medida de controlar de forma célere o acesso aos sistemas de informações.

5.1.1.3. GERENTES OU GESTORES

Assim como ao Setor de Recursos Humanos, caberá ao gerente ou gestor do colaborador comunicar, através do e-mail, à equipe de Tecnologia da

Informação sobre a necessidade de criação, concessão ou alteração de acessos de usuários, garantindo que cada usuário acesse somente as informações de que necessite para o desempenho de sua função ou da prestação de serviços.

Ademais, os gerentes ou gestores deverão solicitar ao Setor de Recursos Humanos que, por sua vez, solicitará à equipe de Tecnologia da Informação, mediante prévia justificativa e por tempo determinado, a liberação de acessos privilegiados aos usuários, em casos específicos em que se julgue necessária a liberação de tal acesso.

5.1.1.4. USUÁRIOS – STAKEHOLDERS INTERNOS E EXTERNOS

O usuário terá o acesso necessário para executar as suas funções laborais ou prestação de serviços, devendo informar ao gestor responsável ou ao Setor de Recursos Humanos caso sejam constatadas permissões excedentes.

5.2. USO DO E-MAIL

O e-mail corporativo é a forma oficial de comunicação da **EMPRESA**. Assim, o e-mail deve ser utilizado pelos usuários exclusivamente para fins relacionados ao desempenho de suas funções e atividades laborais, obedecendo às seguintes regras:

- Deve-se utilizar o e-mail corporativo como meio de comunicação oficial com agentes externos (fornecedores, prestadores de serviços, terceiros etc.);
- O usuário deve verificar, sempre que uma nova mensagem for recebida, a origem das mensagens e, em caso de suspeita de ação irregular, deverá comunicar imediatamente à equipe de Tecnologia da Informação;
- E-mails suspeitos, com mensagens ou imagens inadequadas e/ou spams não devem ser respondidos;
- E-mails que contenham links suspeitos, devem ser ignorados. Na dúvida, o colaborador deve consultar a equipe de Tecnologia da Informação.

É expressamente PROIBIDO:

- **Enviar mensagens de e-mail em nome de seu setor, colegas ou quaisquer terceiros que não tenham autorizado essa comunicação;**
- **Enviar mensagens de e-mail não solicitadas divulgando informações a terceiros sem autorização ou ainda para múltiplos destinatários, exceto se relacionadas a uso legítimo da EMPRESA;**
- **Falsificar ou adulterar o conteúdo de mensagens de e-mails ou endereço do remetente, fazendo-se passar por outra pessoa;**

- **Acessar sem autorização os e-mails de outros usuários, incluindo a caixa de backup;**
- **Utilizar o e-mail para prática de crimes e infrações de qualquer natureza;**
- **Emitir comunicados que representem a opinião pessoal do colaborador em nome da EMPRESA;**
- **Reproduzir, transmitir ou divulgar mensagens que contenham qualquer ato ou orientação que conflite com os interesses da EMPRESA;**
- **Reproduzir e/ou encaminhar mensagens que contenham ameaças eletrônicas, tais como: vírus, spam e demais malwares;**
- **Abrir, executar ou compartilhar mensagens que contenham arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, .wsf etc.) ou qualquer outra extensão que apresente riscos à segurança dos equipamentos, sistemas e redes internas da EMPRESA.**

5.3. USO DA INTERNET E OUTROS MEIOS VIRTUAIS

O uso da internet deve acatar os princípios acima mencionados, em consonância com as funções dos colaboradores e a devida finalidade do acesso. Todas as tecnologias, ferramentas, equipamentos e serviços disponibilizados para acesso à internet são de propriedade da **EMPRESA**.

Desse modo, a **EMPRESA** poderá, sempre que julgar necessário e a seu exclusivo critério, suspender ou bloquear o acesso a quaisquer arquivos, domínios, aplicações, websites e/ou correios eletrônicos, por exemplo.

As redes de internet, servidores e sistemas internos devem ser controlados com acessos privados por meio de usuário e senha dos colaboradores, os quais precisam moderar sua utilização no bom senso, principalmente no que se refere aos sites acessados, tempo de utilização e conteúdo baixado.

O acesso à internet, por meio da rede corporativa, deve ser efetuado por usuários autorizados pela equipe de Tecnologia da Informação. Ademais, as solicitações de liberação de sites que sejam úteis às tarefas diárias deverão ser feitas através de chamado para análise e liberação da equipe de Tecnologia da Informação.

É expressamente PROIBIDO:

- **Acessar, armazenar, divulgar e repassar qualquer material ilícito ligado à pornografia, pedofilia, jogos, racismo, homofobia, religião, bitcoins, formatos de áudio e vídeos (mp3, mp4, AVI etc.), entre outros;**

- **Efetuar tentativas de lograr os controles de internet, usando software, plug-in ou outros métodos;**
- **Utilizar programas (como por exemplo: µTorrent, BitTorrent, eMule etc.) para download/upload de arquivos peer-to-peer (sistema de compartilhamento sem necessidade de um servidor centralizado) de qualquer natureza;**
- **Divulgar ou compartilhar informações internas pertencentes à EMPRESA e referentes às suas operações, sobretudo em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que utilize a internet.**

5.4. CUIDADOS COM O AMBIENTE DIGITAL E DOCUMENTOS ELETRÔNICOS

Todos os arquivos relativos ao desempenho da função do colaborador e à atividade da **EMPRESA** deverão ser armazenados no diretório adequado de cada setor, sendo necessária a realização de backups rotineiros para evitar risco de perda dos arquivos. De tal forma, é expressamente proibido armazenar arquivos nos diretórios dos computadores de cada colaborador (exemplo: "Área de Trabalho" ou pasta "Downloads").

As instalações da **EMPRESA**, especialmente as áreas de maior criticidade, deverão ser monitoradas por meio de circuito interno de câmeras de segurança, sendo estes ambientes devidamente sinalizados a respeito das gravações de vídeo. Os arquivos de imagem também serão armazenados internamente com segurança e possuirão acesso restrito à equipe de Tecnologia da Informação, além de haver eliminação periódica.

Ademais, todos os usuários devem observar as seguintes regras em seu dia a dia:

- **Ao se ausentar da sua estação de trabalho, o colaborador ou o prestador de serviços que esteja alocado nas dependências da EMPRESA deverá bloquear a tela ou guardar os dispositivos que não for levar consigo, de modo que não seja possível outros usuários visualizarem informações expostas nos dispositivos;**
- **Todo e qualquer tipo de mídia removível deve ser desconectada ao término do uso e permanecer armazenada em ambiente seguro e controlado;**
- **Na eventualidade de permissão do uso de computadores particulares para o desenvolvimento das funções de determinados**

colaboradores, fica estabelecido que os computadores devem estar bloqueados caso o colaborador responsável não esteja presente;

- **Na eventualidade de utilização de computadores corporativos pelos colaboradores em modalidade home office, deverão ser tomadas as mesmas medidas de segurança que seriam tomadas nas dependências da Empresa, ficando proibida a utilização desses equipamentos para fins pessoais.**

5.5. CUIDADOS COM AMBIENTE DE TRABALHO E DOCUMENTOS FÍSICOS

Os acessos físicos aos ativos de informação da **EMPRESA** e seus respectivos usos também devem ser pautados pela devida necessidade. Além de observar o correto manuseio das informações em locais físicos como, por exemplo, a própria estação de trabalho do colaborador, exige a adoção das seguintes diretrizes:

- **Documentos em papéis ou mídias impressas não devem permanecer sobre a estação de trabalho enquanto o colaborador não estiver realizando o manuseio;**
- **Os documentos escaneados, após utilizados pelos usuários, devem ser imediatamente deletados das pastas destinadas para este fim. De igual forma, os usuários deverão esvaziar as lixeiras eletrônicas diariamente;**
- **Todo o material deve ser recolhido e armazenado em armários locais ou gavetas – preferencialmente com chave. Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, o colaborador deve limpar a estação de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar o computador;**
- **Durante o expediente, o computador deverá ser bloqueado, caso o colaborador se ausente da sua estação de trabalho, independente do período de ausência;**
- **Caso seja necessário o uso de documentos de outras áreas, estes deverão ser devolvidos, descartados ou excluídos ao término de sua utilização, preferencialmente mediante protocolo formal;**

- **Papéis do tipo lembrete devem ser evitados, ficando expressamente proibido concentrar informações pessoais, senhas, ou outros dados que identifiquem ou possam identificar uma pessoa;**
- **Não devem ser utilizados quadros de aviso, editais ou outros meios físicos para anotação de senhas, lembretes, informações confidenciais e sensíveis;**
- **Crachás de identificação devem ser mantidos em posse do próprio colaborador, que deve notificar o Setor de Recursos Humanos, imediatamente, em caso de suspeita ou extravio;**
- **O colaborador deve dar preferência à leitura de documentos em formato digital, ficando vedado o uso de impressoras e fotocopiadoras não autorizadas (ou seja, aquelas que não sejam de uso da Empresa), durante e fora do horário de expediente;**
- **Documentos impressos devem ser eliminados de maneira adequada. É vedado o uso de rascunhos para impressão de documentos, inclusive aqueles que sejam apenas para uma rápida conferência;**
- **O responsável pela ordem de impressão deve retirar o documento da impressora imediatamente. Documentos não retirados da impressora deverão ser descartados de forma adequada.**

5.6. CUIDADOS COM USUÁRIOS E SENHAS

Os cuidados com os usuários e senhas utilizados pelos colaboradores ou prestadores de serviços para acesso à internet, redes e sistemas internos da **EMPRESA** são de total e exclusiva responsabilidade do próprio colaborador ou prestador de serviço, por isso, as seguintes diretrizes deverão ser observadas:

- **O compartilhamento, divulgação e/ou empréstimo de qualquer forma da senha de cada usuário é expressamente proibido, devendo o Encarregado pelo Tratamento de Dados Pessoais serem informados imediatamente caso haja suspeita de descumprimento da diretriz;**
- **A senha inicial será desenvolvida pela equipe de Tecnologia da Informação logo na admissão do colaborador, devendo ser fornecida ao próprio colaborador pessoalmente sem mostrar ou informar a**

terceiros e deverá ser alterada no primeiro processo de autenticação realizado;

- **Ao criar uma senha, o colaborador deve observar: o tamanho mínimo de 08 (oito) caracteres, a utilização de letras/caracteres minúsculos e maiúsculos, caracteres especiais e números, sendo proibida a utilização de informações públicas e pessoais (ex.: data de aniversário ou nome do cônjuge). Não será permitida a reutilização da última senha;**

- **As alterações de senha deverão ocorrer, obrigatoriamente, a cada 180 (cento e oitenta) dias. Após este período, não será possível que o colaborador acesse o sistema sem alterar a sua senha de acesso, devendo acionar a equipe de Tecnologia da Informação pelos canais de suporte para regularização;**

- **Por fim, é expressamente vedada a anotação de usuários e senhas de logins em locais de fácil acesso, principalmente perto das estações de trabalho do colaborador (ex.: anotações no monitor do computador, embaixo do teclado ou até anotações na tela do computador).**

O cancelamento de usuários deverá ocorrer, obrigatoriamente, de maneira imediata ao desligamento, devendo o Setor de Recursos Humanos informar, via e-mail, a equipe de Tecnologia da Informação para que este proceda com a inativação do usuário.

6. VIOLAÇÕES E SANÇÕES

Deverão ser analisadas quaisquer violações a esta **Política**, suas normas e princípios correlatos, enquanto incidentes de segurança da informação. Tais incidentes serão tratados de acordo com o processo de gestão de incidentes e com apoio da equipe de Tecnologia da Informação, do Encarregado pelo Tratamento de Dados Pessoais e demais áreas que sejam necessárias.

Ao colaborador ou prestador de serviços envolvido na violação à Política e/ou respectivas diretrizes ou normas será assegurado tratamento justo, correto e confidencial, de modo que qualquer medida tomada deverá ser proporcional e aplicada de acordo com o contrato de trabalho ou prestação de serviços, com a presente **Política** e com as normas e legislação vigente.

As violações que impliquem em atividades ilegais ou que possam incorrer em riscos aos titulares de dados pessoais ou danos à **EMPRESA** ensejarão a responsabilização pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

7. CANAIS DE ATENDIMENTO DOS TITULARES DE DADOS

A **EMPRESA** está preparada para receber e atender suas demandas, em caso de necessidade, por qualquer motivo, ou para exercer seus direitos sobre o tratamento dos dados pessoais, entre em contato com nosso Encarregado pelo Tratamento de Dados Pessoais:

FABIO BELMONTE PIMENTEL

(suporte@incopostes.com.br)

O contato também pode ocorrer pelo envio de cartas ou outros meios físicos através do endereço:

Rodovia BR 376, Km 111, s/nº - Distrito Industrial

CEP: 87.720-140

Paranavaí - Paraná

8. ATUALIZAÇÕES E STATUS DA POLÍTICA

Esta **Política** está sujeita a alterações a qualquer momento, sempre buscando aperfeiçoar os serviços em benefício do titular de dados.

Toda e qualquer alteração visa se adequar às eventuais modificações, sejam de adequação de sua redação aos procedimentos internos, bem como novos requisitos legais, regulatórios ou contratuais.

Assim, é importante para garantir a preservação e proteção das informações, que os usuários sigam a ação de comportamento seguro, verificando constantemente a **Política**, para assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

Sem prejuízo, a **Política** e suas atualizações estarão disponíveis na **intranet** ou fisicamente junto ao Encarregado pelo Tratamento de Dados Pessoais. Para prestadores de serviços ou terceiros, o documento será disponibilizado no momento da integração.

Empresa	Aprovado por	Data	Assinatura
Incopostes Indústria e Comércio de Postes Ltda.	Fabio Belmonte Pimentel Laisi F.M. Garrido Vilmar Jose Marques	22/04/2025	