Elaboração:	Análise Crítica/Aprovação:	Rev:	Data	Natureza das Alterações
Thales Rollo	Mariana Duardes	00	07/05/2025	Versão inicial

1. Apresentação

A **TELTEX TECNOLOGIA S.A,** vem por meio desta política estabelecer as diretrizes para implementação de medidas para regular a segurança no acesso físico de pessoas aos recursos de processamento, armazenamento e tratamento de dados corporativos de Tecnologia da Informação e Comunicação (TIC) pertencentes à **TELTEX** e aqueles pertencentes à seus clientes que estejam sob seu controle e proteção, de forma a minimizarem os riscos à segurança das informações corporativas.

Estas diretrizes devem ser lidas, compreendidas e seguidas em todos os níveis da organização, para que os principais ativos da **TELTEX**, incluindo informação, software e hardware, tenham o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

2. Escopo para aplicação

O escopo da presente Política se aplica às instalações da **TELTEX TECNOLOGIA S.A** (CNPJ 73.442.360/0001-17), localizada à Rua Franca Pinto, N°1089, Andar 1 e 2, Vila Mariana, São Paulo/SP – CEP 04016-034, em especial aos ambientes:

- Recepção (1° andar)
- Showroom (1° andar)
- Sala Técnica (1° andar)
- Sala Administrativa (2° andar)
- Sala Comercial e CPD (3° andar)

3. Público alvo

A presente Política busca atingir em especial o seguinte público:

- Colaboradores diretos e indiretos
- Prestadores de serviço
- Visitantes

4. Segurança de Acesso Físico

4.1 São utilizados perímetros físicos de segurança (barreiras tais como paredes e portões de entrada controlados) para proteger as áreas que contenham instalações de processamento, armazenamento e tratamento de dados além de controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferências com o suprimento de energia elétrica, interferência nas comunicações, radiação eletromagnética e vandalismo.

4.1.1 Os perímetros de segurança são claramente definidos e sua localização e a capacidade de resistência dos mesmos se ajustam aos requisitos de segurança dos ativos existentes no interior do perímetro, podendo incluir controles de monitoramento e vigilância por meio de câmeras de segurança, alarmes de presença por infravermelho e registro de acessos.

4.1.2 É mantida área de recepção monitorada pelo pessoal ou outros meios para controlar o acesso físico ao local ou edifício da **TELTEX.**

4.1.3 As instalações físicas são monitoradas por sistemas de vigilância e alarmes de presença por infravermelho para detectar acesso não autorizado ou comportamento suspeito, que podem incluir guardas, alarmes de intrusos, sistemas de videomonitoramento, como de circuito fechado de TV e software de gerenciamento de informações de segurança física, gerenciados internamente ou por um provedor de serviços de monitoramento, conforme apropriado.

4.2 A área de Tecnologia da Informação T.I. avalia e providencia constantemente, com o auxílio das áreas competentes, a manutenção e/ou melhoria dos recursos de segurança de seus centros de processamento, armazenamento e tratamento de dados corporativos.

4.3 As áreas de processamento, armazenamento e tratamento de dados são protegidas por controles apropriados de entrada, para assegurar que somente pessoas autorizadas tenham acesso, incluindo biometria ou cartões de proximidade para acesso a áreas restritas.

4.3.1 São providos controles de autenticação que utilizam, sempre que possível, autenticação mínima de dois fatores, para autorizar e validar todos os acessos.

4.3.2 É mantido, de forma segura, um registro de todos os acessos para fins de auditoria;

4.3.3 A data e hora de entrada e saída de visitantes são registradas, e todos os visitantes são acompanhados por um colaborador, a não ser que o seu acesso tenha sido previamente aprovado.

4.3.4 As permissões de acesso são concedidas somente para finalidades específicas, devendo a pessoa autorizada, receber instruções sobre os requisitos de segurança da área e os procedimentos de emergência.

4.3.5 Os direitos de acesso às áreas seguras são revistos e atualizados em intervalos de tempo regulares, e revogados quando necessário.

4.3.6 Aos terceirizados que realizam serviços de suporte, é concedido acesso restrito às áreas seguras ou às instalações de processamento, armazenamento e tratamento da informação sensível somente quando necessário. O acesso é sempre autorizado e monitorado.

4.4 As áreas de processamento, armazenamento e tratamento de dados estão localizadas de forma discreta, sem indicação de sua finalidade e sem letreiros evidentes que identifiquem a presença de suas atividades, quando aplicável.

4.5 As listas de funcionários e guias telefônicos internos que identifiquem a localização das instalações de processamento, armazenamento e tratamento de dados sensíveis não são de fácil acesso ao público.

4.6 Existem equipamentos para contingência no processamento, armazenamento e tratamento de dados em nuvem e eventuais mídias de backup, para que não sejam danificadas por um desastre que afete o local principal.

4.7 Não é permitido, nas localizações dos centros de processamento, armazenamento e tratamento de dados, o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado e registrado.

4.8 Fica estabelecida como diretriz a **Política de Mesa Limpa** para evitar que documentos sensíveis fiquem expostos em locais de trabalho, seja fisicamente sobre as mesas ou eletronicamente em áreas de trabalho de computadores e dispositivos móveis.

4.8.1 Aplicação da **Política de Mesa Limpa** no Ambiente Físico:

- Remoção de documentos sensíveis: Papéis contendo informações confidenciais devem ser guardados em locais seguros, como gavetas trancadas.
- Uso de armários e cofres: Materiais importantes devem ser armazenados em locais protegidos quando não estiverem em uso.
- Evitar anotações visíveis: Senhas e dados estratégicos não devem ser deixados em post-its ou cadernos sobre a mesa.
- Controle de acesso: Apenas pessoas autorizadas devem ter acesso a áreas onde informações críticas são manipuladas.

4.8.2 Aplicação da Política de Mesa Limpa no Ambiente Eletrônico:

- Bloqueio automático de tela: Computadores devem ser configurados para bloquear a tela após um período de inatividade.
- Autenticação segura: Uso de senhas fortes e autenticação multifator para acesso a sistemas.
- Proteção contra olhares curiosos: Telas devem ser posicionadas de forma que terceiros não possam visualizar informações sensíveis.
- Criptografia de dados: Arquivos e comunicações devem ser protegidos para evitar interceptações.

4.9 É proibido o consumo de bebidas, comidas e fumo nas proximidades das instalações principais de processamento, armazenamento e tratamento de dados.