

AVISO DE MONITORAMENTO ELETRÔNICO DE COLABORADORES, CIÊNCIA E AUTORIZAÇÕES LIMITADAS

Brasil - modelo informativo para uso com CleverControl

Modelo informativo para empresas que pretendem implementar ou revisar práticas de monitoramento com CleverControl. Use este formulário antes de ativar o monitoramento. Marque apenas as funções realmente habilitadas na configuração do CleverControl. Anexe a política completa, prazo de retenção, aviso de privacidade e qualquer aviso específico exigido por lei, acordo coletivo ou norma setorial.

Empregador	
Colaborador	
Cargo / departamento	
Local principal de trabalho	
Data do aviso	Início do monitoramento:

1. FINALIDADES EMPRESARIAIS

☐ segurança cibernética e resposta a incidentes	☐ proteção de informações confidenciais
☐ controle de jornada, presença ou acesso	☐ garantia de qualidade e auditoria operacional
☐ obrigações legais, regulatórias ou de registro	☐ análise de produtividade e fluxo de trabalho
☐ investigação de suspeita de conduta indevida	☐ prevenção de uso indevido de sistemas da empresa
☐ segurança da informação e prevenção de vazamentos	☐ outro: _____

O uso do CleverControl deve estar vinculado a finalidade profissional clara e configurado para coletar apenas os dados necessários.

2. SISTEMAS, DISPOSITIVOS E ATIVIDADES QUE PODEM SER MONITORADOS

☐ login/logout; tempo ativo e inativo	☐ aplicativos, processos e títulos de janelas
☐ sites, URLs e pesquisa em sistemas de trabalho	☐ e-mail, chat e colaboração corporativa
☐ acesso, transferência, nuvem, USB e impressão de arquivos	☐ capturas de tela ou visualização de tela
☐ atividade de teclado/entrada, sem captura intencional de senhas	☐ telemetria de rede, segurança, autenticação e dispositivo
☐ áudio ou chamadas - somente se autorizado abaixo	☐ câmera/webcam/video - somente se autorizado abaixo
☐ GPS/localização/veículo - somente se autorizado	☐ dado biométrico - somente se justificado e autorizado
☐ perfil de trabalho em dispositivo pessoal (BYOD)	☐ pontuação automatizada ou relatórios de apoio à decisão

Equipamentos/contas abrangidos: ☐ dispositivos/redes do empregador ☐ contas corporativas ☐ veículos do empregador ☐ apenas perfil de trabalho em dispositivo pessoal ☐ outro: _____

Período: ☐ durante a jornada ☐ quando sistema coberto for usado ☐ registro contínuo de segurança ☐ investigação limitada: _____

3. LIMITES E EXCLUSÕES

O empregador não deverá monitorar intencionalmente banheiros, vestiários, áreas de troca de roupa ou outros locais com expectativa reforçada de privacidade. A empresa não deverá coletar intencionalmente senhas pessoais, credenciais bancárias pessoais, informações de saúde, conteúdo de contas pessoais ou comunicações privadas, salvo quando houver base legal, necessidade específica e autorização adequada. Monitoramento fora do horário de trabalho ou em residência deve ser limitado a sistemas de trabalho cobertos e a finalidades profissionais legítimas.

USO PESSOAL EM EQUIPAMENTOS CORPORATIVOS

Para reduzir o risco de exposição acidental de dados pessoais, o colaborador não deverá utilizar dispositivos, redes ou contas corporativas para acessar contas pessoais, armazenar arquivos pessoais ou realizar comunicações privadas, salvo quando o uso pessoal ocasional for expressamente permitido pela política interna da empresa. Informações pessoais exibidas em sistemas monitorados poderão ser registradas incidentalmente, mesmo que sua coleta não seja intencional.

4. USO, ACESSO, RETENÇÃO E SEGURANÇA DOS DADOS

Usuários/cargos autorizados	
Prazo de retenção	
Fornecedor / operador	
Usos internos	☐ segurança ☐ orientação ☐ jornada ☐ investigação ☐ decisões disciplinares ☐ outro: _____
Dúvidas / solicitações	Contato: _____ E-mail/telefone: _____

5. PERFIL LEGAL DO BRASIL

LGPD: avaliar finalidade, necessidade, transparência, segurança, hipótese legal, retenção e direitos dos titulares. Constituição Federal: considerar intimidade, vida privada, honra, imagem e sigilo das comunicações. CLT: o poder de direção pode contextualizar ferramentas corporativas, mas não autoriza vigilância ilimitada. NR-1 / GRO / PGR: práticas de controle digital e metas também devem ser avaliadas sob saúde, segurança e fatores de risco psicossociais relacionados ao trabalho.

Referências para revisão jurídica: LGPD - Lei nº 13.709/2018; Constituição Federal; CLT - Decreto-Lei nº 5.452/1943; NR-1; orientações da ANPD; materiais do MTE e do TST.

BRASIL - CIÊNCIA DO COLABORADOR E AUTORIZAÇÕES OPCIONAIS

A. CIÊNCIA DO AVISO

Declaro que recebi este aviso antes do início do monitoramento; que pude revisar métodos, finalidades, limites, usos, retenção e contato; e que entendo que atividades de trabalho cobertas podem ser monitoradas na medida permitida pela legislação aplicável. Esta ciência não renuncia a direitos irrenunciáveis nem autoriza monitoramento proibido por lei, norma coletiva ou política aplicável.

☐ Confirmo o recebimento do aviso e da política anexa. Iniciais: _____

B. ÁUDIO / GRAVAÇÃO DE CHAMADAS - SOMENTE SE HABILITADO

☐ Não habilitado. ☐ Habilitado apenas para estes canais/finalidades: _____

Comunicações das quais eu participe só poderão ser gravadas após a empresa implementar avisos, autorizações ou bases legais exigidos para cada participante e jurisdição aplicável. Minha assinatura não autoriza gravação de clientes, colegas ou terceiros sem os avisos ou consentimentos necessários.

Iniciais para áudio: _____ Responsável de compliance: _____

C. CÂMERA / VÍDEO / TRABALHO REMOTO

☐ Não habilitado. ☐ Áreas comuns/segurança. ☐ Webcam para função específica: _____

☐ Monitoramento audiovisual remoto aprovado para esta função: _____

Nenhuma câmera ou gravação é autorizada em banheiros, vestiários ou espaços privados legalmente protegidos. Em trabalho remoto, a ativação deve ser visível ou claramente informada e limitada à finalidade e ao período declarados.

Iniciais para câmera/vídeo: _____

D. GPS / LOCALIZAÇÃO / RASTREAMENTO DE VEÍCULO

☐ Não habilitado. ☐ Veículo/dispositivo do empregador durante atividade de trabalho. ☐ Veículo/dispositivo pessoal apenas com autorização específica.

Horários: _____ Finalidade: _____. Fora do trabalho desativado/limitado: _____

Iniciais para localização: _____

E. DISPOSITIVO PESSOAL / BYOD

☐ Nenhum software de monitoramento será instalado em dispositivo pessoal. ☐ Autorizo apenas estes controles/dados do perfil de trabalho:

Fotos, mensagens, contas pessoais e aplicativos não relacionados ao trabalho ficam excluídos. Posso revogar esta autorização, sujeito à devolução ou remoção de dados e acessos da empresa.

Iniciais para BYOD: _____

F. DADO BIOMÉTRICO - PREENCHER SOMENTE SE USADO

Tipo coletado	☐ impressão digital ☐ geometria facial ☐ voz ☐ retina/íris ☐ outro: _____
Finalidade específica	_____
Coleta / início	_____ Prazo esperado / término: _____
Retenção / eliminação	_____
Fornecedor / base legal	Fornecedor: _____ Base legal avaliada: _____

Este modelo pode acompanhar uma implementação do CleverControl, mas não substitui a análise jurídica da empresa. Dados biométricos vinculados a pessoa natural devem ser tratados como dados pessoais sensíveis. Antes da coleta, avaliar finalidade, necessidade, hipótese legal, segurança, retenção, acesso restrito e eliminação quando aplicável.

Iniciais para biometria: _____

G. ASSINATURAS

Assinatura do colaborador	Data
_____	_____
Representante do empregador (certifica configuração e avisos necessários)	Data
_____	_____

Aviso: Este modelo é apenas um auxílio informativo para empresas que usam ou avaliam o CleverControl e não substitui aconselhamento jurídico. Revise com advogado qualificado no Brasil antes de usar.