# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – WORKMONITOR

## SUMÁRIO


INTRODUÇÃO 03
ABRANGÊNCIA 03
COMPROMETIMENTO DA ALTA DIREÇÃO 03
OBJETIVOS 03
DEFINIÇÕES 04
RESPONSABILIDADES 05
Funcionários 06
Gestores 06
PRINCÍPIOS 06
DA SEGURANÇA DA INFORMAÇÃO 07
Classificação das informações 07
Nomenclatura de acesso único 08
Das regras dos usuários (Política de Usuários) 08
Do acesso remoto 10
Correio eletrônico 11
Internet 12
Identificação 13
Computadores 14
Sistemas internos e de terceiros 16
Compartilhamento de informações 16
Dispositivos móveis 17
Proteção de dados pessoais e pessoais sensíveis 18
Desenvolvimento de software 18
Backup físico dentro da organização 19
Servidor de e-mail 19
Dados em nuvem 20
Manutenção preventiva e corretiva 21
TREINAMENTO E VERIFICAÇÕES 22
RESPOSTA A INCIDENTES 22

GESTÃO DE TERCEIROS 23

PENALIDADES 23

ENCARREGADO DE DADOS 23

ATUALIZAÇÕES 24

## INTRODUÇÃO

A presente política reflete o respeito e objetivos da WORKMONITOR com a segurança dos ativos custodiados em sua posse, traça diretrizes e orientações a serem seguidas, todas com o comprometimento da alta Direção e dos responsáveis.

Este instrumento deve ser interpretado em consonância com outras diretrizes internas, além das regulações profissionais de cada categoria.

A busca pela segurança da informação passa a ser uma constante na ORGANIZAÇÃO e uma cultura a ser seguida e sempre melhorada.

## ABRANGÊNCIA

A presente política abrange toda alta direção, colaboradores, terceirizados e demais pessoas que possuam vínculo com o **WORKMONITOR**, bem como é aplicado em todas as unidades existentes e que vierem a ser criadas, independente de base territorial.

O presente documento passa a ter visibilidade pública, sendo de conhecimento obrigatório da alta direção, colaboradores, terceirizados e demais pessoas que possuam vínculo com o **WORKMONITOR**.

## COMPROMETIMENTO DA ALTA DIREÇÃO

A alta direção do **WORKMONITOR**, nas pessoas de seus sócios, se comprometem com os termos da presente política, bem como, com a segurança e integralidade dos dados confiados a ORGANIZAÇÃO.

## OBJETIVOS

Os principais objetivos da Política de Segurança da Informação – PSI são estabelecer diretrizes que permitam aos empregados, colaboradores e clientes seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e proteção legal da Organização e do indivíduo:

- Conscientizar os usuários de informação sobre sua segurança e privacidade;

- Definir normas, responsabilidades, obrigações e sanções para todos que tiverem acesso a algum tipo de informação;
- Proteger e preservar a integridade, confiabilidade e disponibilidade da informação, protegendo e preservando os dados confiados.

## DEFINIÇÕES

- ATIVO: qualquer coisa que tenha valor para a organização
- DISPONIBILIDADE: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada
- CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados
- LGPD: Lei Geral de Proteção de Dados
- INTEGRIDADE: propriedade de salvaguarda da exatidão e completeza de ativos
- DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;
- DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- DADO ANONIMIZADO: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- BANCO DE DADOS: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

- ENCARREGADO: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
- TRATAMENTO: toda operação realizada com dados pessoais, 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;
- ELIMINAÇÃO: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- SEGURANÇA DA INFORMAÇÃO: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas
- EVENTO DE SEGURANÇA DA INFORMAÇÃO: uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

**RESPONSABILIDADES:**

A **WORKMONITOR** entende que a Política de Segurança da Informação somente será eficaz com o comprometimento de todos os usuários:

**Funcionários:**

Respeitar esta Política de Segurança da Informação;

Responder pela guarda e proteção dos equipamentos e recursos computacionais colocados à sua disposição para execução de suas tarefas;

Responder pelo uso exclusivo e intransferível de suas senhas acesso

Adquirir conhecimento necessário para a correta utilização dos recursos de hardware e software;

Comunicar prontamente à área de TI ou ENCARREGADO DE DADOS qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;

Certificar que as informações e dados de propriedade da ORGANIZAÇÃO e principalmente de clientes não sejam disponibilizados para terceiros, a não ser com autorização, por escrito do superior hierárquico;

**Gestores:**

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os empregados, estagiários e colaboradores;

Atribuir aos empregados, estagiários e colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da WORKMONITOR, mediante assinatura de Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Organização;

Antes de conceder o acesso às informações da Organização a colaboradores eventuais e prestadores de serviços, exigir assinatura do Acordo de Confidencialidade;

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI;

Autorizar o acesso e definir o perfil e mudança de perfil do usuário junto ao responsável pela área de TI;

Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.

## PRINCÍPIOS

A presente política tem por base as normas da Associação Brasileira de Normas Técnicas, Lei Geral de Proteção de Dados, normas correlatas e princípios a seguir expostos:

Preservar e proteger as informações sob a responsabilidade da **WORKMONITOR**, inclusive as contidas nos recursos de Tecnologia da Informação e Comunicação (TIC), dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato.

Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

Assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade, assim como a legalidade no desenvolvimento das atividades do negócio.

Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da Instituição no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

## DA SEGURANÇA DA INFORMAÇÃO

### Classificação das informações:

A classificação de informações na organização segue as diretrizes da ISO/IEC 27001 e ISO/IEC 27002, garantindo a proteção adequada dos ativos de informação utilizados no desenvolvimento de software. Esse processo estabelece categorias baseadas no nível de sensibilidade e no impacto potencial em caso de acesso não autorizado, modificação ou destruição. A política de classificação adota um modelo estruturado, segmentando as informações em Pública, Interna, Restrita e Confidencial, assegurando que cada tipo de dado receba controles de segurança apropriados.

A definição do nível de classificação considera critérios como regulamentações aplicáveis (LGPD e GDPR), criticidade para o negócio, impacto operacional e requisitos contratuais. Informações Confidenciais incluem código-fonte proprietário, credenciais de acesso, dados sensíveis de clientes

e relatórios estratégicos, exigindo criptografia em repouso e em trânsito, conforme a ISO/IEC 27040 (Segurança para Armazenamento de Dados). Já informações Públicas, como materiais institucionais e conteúdos divulgados no site da empresa, não requerem controles rigorosos de acesso. Todas as informações classificadas são armazenadas, processadas e compartilhadas com base nos princípios de Least Privilege Access (Princípio do Menor Privilégio) e Need-to-Know (Necessidade de Conhecimento).

A organização mantém um processo contínuo de revisão e atualização da classificação das informações, garantindo que os controles aplicados estejam sempre alinhados com os riscos e as necessidades do negócio. Auditorias periódicas, treinamentos para os colaboradores e a adoção de soluções tecnológicas, como Data Loss Prevention (DLP) e Rights Management Services (RMS), são utilizadas para reforçar a proteção contra acessos indevidos e vazamentos de dados. Dessa forma, a política de classificação de informações contribui para a conformidade regulatória, a mitigação de riscos e a preservação da integridade, confidencialidade e disponibilidade das informações essenciais à organização.

**Nomenclatura de acesso único**

A nomenclatura de acesso único na organização segue as diretrizes da ISO/IEC 27001 e ISO/IEC 27002, garantindo a padronização e rastreabilidade das credenciais utilizadas nos sistemas corporativos. Cada usuário recebe um identificador único, intransferível e associado ao princípio de Least Privilege Access (Princípio do Menor Privilégio), conforme definido na ISO/IEC 27701 para proteção da privacidade. O formato dos identificadores deve seguir uma estrutura padronizada que permita a identificação do usuário sem expor informações sensíveis, respeitando requisitos da ISO/IEC 24760 (Estruturas de Gerenciamento de Identidade). Além disso, para reforçar a segurança, os acessos são gerenciados por um Identity and Access Management (IAM) centralizado, garantindo conformidade com os controles de autenticação e autorização descritos na ISO/IEC 29115 (Framework para Autenticação Segura), assegurando que cada credencial seja utilizada exclusivamente pelo usuário autorizado e monitorada em tempo real para detectar atividades suspeitas.

**Das regras dos usuários (Política de Usuários)**

A política de usuários da organização é baseada nas diretrizes da ISO/IEC 27001 e ISO/IEC 27002, garantindo a gestão segura das contas, acessos e permissões dentro dos sistemas corporativos. O gerenciamento de usuários segue o princípio de Least Privilege Access (Princípio do Menor Privilégio), conforme a ISO/IEC 27701, assegurando que cada colaborador tenha apenas as permissões estritamente necessárias para a execução de suas funções. A criação, modificação e revogação de contas são realizadas por meio de um processo estruturado e documentado, garantindo conformidade com os controles de segurança da informação e minimizando riscos de acessos indevidos.

O ciclo de vida das contas de usuários segue um fluxo definido de provisionamento, monitoramento e desprovisionamento, alinhado às melhores práticas da ISO/IEC 24760 (Gerenciamento de Identidade e Autenticação). Cada usuário recebe uma credencial única e intransferível, e a autenticação é reforçada por mecanismos como Multi-Factor Authentication (MFA), conforme recomendado pela ISO/IEC 29115 (Framework para Autenticação Segura). O uso de contas compartilhadas ou genéricas é estritamente proibido, e todos os acessos são registrados em logs auditáveis, garantindo rastreabilidade e conformidade com a ISO/IEC 27035 (Gerenciamento de Incidentes).

Para reduzir riscos associados a credenciais comprometidas, a organização implementa políticas de senha robustas, seguindo os requisitos da ISO/IEC 27001 e diretrizes do NIST SP 800-63B. As senhas devem possuir complexidade mínima, serem trocadas periodicamente e armazenadas de forma segura por meio de algoritmos de hash e criptografia em conformidade com a ISO/IEC 27040 (Segurança para Armazenamento de Dados). Além disso, políticas de bloqueio automático de contas são aplicadas após tentativas consecutivas de login malsucedidas, mitigando riscos de ataques de força bruta.

A revisão periódica de acessos é realizada de acordo com a ISO/IEC 27004 (Medição da Segurança da Informação), garantindo que permissões sejam revogadas ou ajustadas conforme mudanças no perfil do usuário ou desligamento da organização. O processo de auditoria de contas é conduzido por um Identity and Access Management (IAM) centralizado, garantindo a conformidade com regulamentações como LGPD e GDPR.

Por fim, todos os usuários devem aderir a termos de uso e confidencialidade, formalizando seu compromisso com a segurança da informação e a privacidade dos dados. Treinamentos regulares são realizados para conscientização sobre boas práticas e riscos de segurança, conforme

recomendado pela ISO/IEC 27002, fortalecendo a cultura de proteção da informação dentro da organização.

**Do acesso remoto**

O acesso remoto à infraestrutura da organização é regulamentado conforme as diretrizes da ISO/IEC 27001 e ISO/IEC 27002, garantindo a segurança na conexão de usuários externos aos sistemas internos. Para mitigar riscos de acessos não autorizados e vazamento de dados, a organização utiliza Virtual Private Network (VPN) como método exclusivo de acesso remoto, seguindo os requisitos da ISO/IEC 27033 (Segurança de Redes). A VPN emprega criptografia de ponta a ponta baseada em TLS 1.2+ ou IPsec, assegurando a integridade e confidencialidade dos dados transmitidos.

A autenticação de usuários na VPN segue o princípio de Least Privilege Access (Princípio do Menor Privilégio), conforme descrito na ISO/IEC 27701, garantindo que cada colaborador tenha acesso apenas aos recursos necessários para sua função. Além disso, é implementado um mecanismo de Multi-Factor Authentication (MFA), em conformidade com a ISO/IEC 29115 (Framework para Autenticação Segura), adicionando camadas extras de proteção contra acessos indevidos. Os dispositivos utilizados para acesso remoto devem ser previamente autorizados e monitorados por um Endpoint Detection and Response (EDR), conforme as recomendações da ISO/IEC 27035 (Gerenciamento de Incidentes).

Todas as conexões remotas são registradas e monitoradas em tempo real por meio de um Security Information and Event Management (SIEM), garantindo auditoria contínua e detecção de comportamentos anômalos, conforme os princípios da ISO/IEC 27005 (Gestão de Riscos de Segurança da Informação). Logs de acesso são armazenados de forma segura e analisados periodicamente para identificar possíveis tentativas de exploração ou comprometimento das credenciais. A retenção desses registros segue as diretrizes da ISO/IEC 27040 (Segurança para Armazenamento de Dados).

Para reduzir a superfície de ataque, a VPN opera sob um modelo de Zero Trust Architecture (ZTA), garantindo que cada solicitação de acesso remoto seja verificada antes da liberação do tráfego para a rede interna. Dispositivos não gerenciados são isolados em uma zona desmilitarizada (DMZ), prevenindo acessos diretos aos sistemas críticos da organização. Adicionalmente, a comunicação

entre a VPN e os servidores corporativos é segmentada por políticas de Network Access Control (NAC), conforme recomendado na ISO/IEC 27033-2.

Por fim, políticas de conformidade e boas práticas de acesso remoto são comunicadas regularmente aos colaboradores por meio de treinamentos baseados na ISO/IEC 27002, reforçando a conscientização sobre segurança cibernética. Auditorias periódicas são conduzidas para avaliar a eficácia das medidas de proteção e garantir que a VPN esteja sempre atualizada contra novas ameaças. Dessa forma, a organização assegura um acesso remoto seguro, confiável e alinhado com as melhores práticas internacionais de segurança da informação.

**Correio eletrônico**

O uso do correio eletrônico do **WORKMONITOR** é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Organização e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do **WORKMONITOR** para:

- enviar mensagem com resultado para e-mail não cadastrado no sistema;
- utilizar o e-mail profissional para cadastro em qualquer site ou para recebimento de propagandas;
- utilizar o e-mail profissional para assuntos particulares, salvo autorização expressa do superior hierárquico;
- acessar conta de e-mail particular nas instalações e equipamento do **WORKMONITOR**.
- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- produzir, transmitir ou divulgar mensagem que:
  - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - vise acessar informações confidenciais sem explícita autorização do proprietário;
  - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
  - tenha fins políticos locais ou do país (propaganda política);
  - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

**Internet**

Todas as regras atuais do **WORKMONITOR** visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a **WORKMONITOR**, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Neste sentido, fica vedada a utilização da internet conforme orientações a seguir:

- Alterar configurações padrões dos sistemas, máquinas ou ferramentas de acesso a internet;

- Utilizar a internet para atividades ilícitas ou que violem os bons costumes, integridade dos dados e reputação da Organização.
- Utilização para fins pessoais, salvo autorização expressa de superior hierárquico;
- O compartilhamento de qualquer forma via internet, de imagens, listas, senhas ou quaisquer documentos, independente da extensão, para terceiros não autorizados;
- Entrar em sites de discussão, bate-papo/chat, comunicação instantânea (ex. whatsapp e telegram), com cunho pessoal;
- Realizar qualquer download sem expressa autorização;
- Acessar qualquer site através de links desconhecidos;
- Atualizar programas sem a expressa autorização da equipe técnica ou superior hierárquico;
- Acesso, divulgação ou qualquer outro contato com material de cunho sexual;
- Upload de informações para programas e/ou sites não autorizados;
- Não compartilhar de forma nenhuma: vírus, spam, malware, conteúdo de ódio, assédio, perturbação, etc...
- Atitudes que não estejam exemplificadas aqui mas que confrontem essa política e seus princípios;
- O cometimento de atos que infrijam a presente política ou seus princípios acarretará sanções de ordem civil e penal, de acordo com o ato cometido, além das penalidades e consequências trabalhistas.

**Identificação**

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a **WORKMONITOR** e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Neste sentido, devem ser seguidas as seguintes regras:

- A utilização de crachá nas dependências da organização é obrigatória, assim como o uniforme e EPI;
- Os logins e senhas são de uso pessoal e intransferível, não podendo em hipótese nenhuma ser compartilhada;
- O acesso a sistemas web fora de equipamentos da organização deve ser feita de preferência através de abas anônimas nos navegadores, sendo expressamente proibido salvar senha e dados de acesso. Tal situação deve ser considerada exceção e ocorrer somente com autorização expressa.
- É responsabilidade do superior hierárquico a solicitação de criação de login e senha para funcionários;
- Visitante e terceiros somente devem adentrar as instalações da Organização após a assinatura de termo de responsabilidade e confidencialidade;
- A criação de senhas deve obedecer a critérios de dificuldade, utilizando caracteres alfanuméricos, especiais, caixa-alta e caixa-baixa, obrigatoriamente.
- Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.
- O acesso de clientes se dará através de senha pessoal e intransferível, entregue no ato do cadastro, a qual não poderá ser fornecida posteriormente por qualquer meio tecnológico.

**Computadores e rede**

Os equipamentos disponíveis aos colaboradores são de propriedade do **WORKMONITOR**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da organização e com as observações abaixo:

- É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico;
- Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente.
- O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável.

- Arquivos pessoais e/ou não pertinentes ao negócio do **WORKMONITOR** (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.
- Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
- Os equipamentos de testes e diagnósticos somente devem ser operados por profissionais qualificados, sendo que que eventual prejuízo poderá ser cobrado diretamente de quem causar;
- Os colaboradores do **WORKMONITOR** e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização.
- No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.
    - ✓ Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
    - ✓ É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do suporte de tecnologia da informação do **WORKMONITOR** ou por terceiros devidamente contratados para o serviço.
    - ✓ É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
    - ✓ O colaborador deverá manter a configuração do equipamento disponibilizado pelo **WORKMONITOR**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
    - ✓ Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

- ✓ Todos os recursos tecnológicos adquiridos pelo **WORKMONITOR** devem ter imediatamente suas senhas padrões (default) alteradas.
- ✓ Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

**Sistemas internos e de terceiros**

O **WORKMONITOR** utiliza sistemas próprios e de terceiros para execução dos serviços, os dados lançados em tais sistemas são classificados com pessoais e pessoais sensíveis, assim, toda operação deve ser baseada nos termos desta política e princípios de segurança e integridade.

- O acesso deve ser feito exclusivamente por login precedido de senha pessoal e intransferível;
- A integridade dos dados deve ser mantida, sendo proibida a sobreposição ou exclusão de termos e documentos enviados anteriormente;
- A utilização de tais sistemas devem ser feita de forma obrigatória nos equipamentos da organização e não particulares, salvo autorização expressa;
- Em hipótese nenhuma é permitida a captura de tela, geração de relatório e qualquer outro meio de obtenção de dados para envio para terceiro não autorizado;

**Compartilhamento de informações:**

O **WORKMONITOR** exerce atividade estritamente ligada a dados pessoais e dados pessoais sensíveis, tais informações são protegidas pela presente política, além de disposições legais, assim, visando a integridade e segurança das informações, o compartilhamento e divulgação de resultados somente poderá ocorrer com quem de direito, salvo expressa autorização do responsável hierárquico.

- Funcionários: Os dados pessoais dos funcionários somente serão compartilhados ara cumprimento de obrigação legal, requisição judicial ou quando devidamente consentido pelos mesmos;
- Clientes: Os dados pessoais e pessoais sensíveis somente serão compartilhados com os titulares, salvo autorização expressa desse para terceiro;

- Terceiros: Dados pessoais de terceiros somente serão compartilhados para cumprimento de obrigação legal ou requisição judicial.
- Internamente: a circulação de dados internamente deverá obedecer aos princípios da necessidade e interesse.
- Contratual: Dados pessoais poderão ser compartilhados para cumprimento de obrigações contratuais, nos termos dos contratos vigentes.

O compartilhamento indevido ou fora dos padrões da organização ocasionará a responsabilidade civil e penal daquele que descumprir as regras, além de eventuais sanções trabalhistas.

**Dispositivos móveis**

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo setor de Tecnologia da Informação, como: notebooks, smartphones, Hds Externos e pendrives.

O **WORKMONITOR** não permite a utilização de dispositivos móveis pessoais em ambiente de trabalho, salvo os funcionários devidamente autorizados pela alta direção.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

- Todos os dados relacionados ao **WORKMONITOR** possuem caráter sigiloso e mesmo que discutidos em aparelho pessoal, devem ser mantidos em sigilo, sendo vedado seu compartilhamento de qualquer forma;
- Todos os aparelhos que vierem a ser utilizados para o trabalho, mesmo os pessoais, devem obedecer a critérios de segurança, tais como senha para desbloqueio, conta cadastrada e possibilidade de "reset" remoto, dupla verificação de acesso em aplicativos que envolvam a organização.

- Os aparelhos da organização e utilizados externamente também devem seguir os mesmos critérios acima, sendo vedado ainda a instalação de qualquer outro aplicativo diferente dos utilizados para o trabalho, além de serem devolvidos todo final de expediente para o superior hierárquico.
- Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.
- O suporte técnico aos dispositivos móveis de propriedade do **WORKMONITOR** e aos seus usuários deverá seguir o mesmo fluxo de suporte da instituição.
- É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo **WORKMONITOR**, notificar imediatamente seu gestor direto, para que este seja bloqueado e inutilizado. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).
- O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao **WORKMONITOR** e/ou a terceiros.
- Equipamentos portáteis, como smart phones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

**Proteção de dados pessoais e pessoais sensíveis**

O **WORKMONITOR** possui e aplica as disposições da Lei Geral de Proteção de Dados, assim como as disposições correlatas relativas a segurança da informação, realizando treinamentos, palestras e divulgando informações pertinente sobre o tema.

Todas as ações aplicadas tem por base as legislações citadas, bem como as orientações emitidas pela Associação Brasileira de Normas Técnicas, além dos órgãos de classe, visando sempre o sigilo e segurança das informações confiadas.

**Desenvolvimento de software**

O WORKMONITOR possui como uma de suas atividades o desenvolvimento de software, aplicativos e funcionalidades, seguindo padrões legais, em especial a proteção a privacidade, mais especificamente privacy by desing, princípio transcrito no artigo 46 da Lei Geral de Proteção de Dados.

Ao desenvolver sistemas, os colaboradores mantêm a privacidade e proteção dos dados em primeiro plano, implementando códigos seguros e realizando testes antes de disponibilizar a ferramenta no mercado.

Neste sentido, sempre que há o desenvolvimento de um sistema, ao menos é garantido de plano a proteção aos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

**Backup físico dentro da organização**

O WORKMONITOR mantém como um de seus produtos a hospedagem de dados em suas dependências, em servidores próprios e dotados de segurança.

A transferência dos dados entre partes deve ocorrer preferencialmente via cabeamento direto, porém, sendo aceito a transmissão via VPN, onde há a aplicação de criptografia sobre os dados em trânsito, garantindo uma privacidade e segurança.

A responsabilidade pela integridade dos dados alocados nos servidores internos WORKMONITOR é do contratante, devendo este verificar a situação e sempre que possível, fazer a alocação via dados criptografados, em criptografia sob sua responsabilidade.

Compete ao WORKMONITOR a responsabilidade pela disponibilidade dos dados, de modo que seja possível a restauração ou acesso em caso de solicitação. Também é responsabilidade a segurança dos servidores, com limitação de acesso e geração de logs daqueles que vierem a ter contato com os dados gravados.

Os termos específicos deste serviço deverão estar regulados em contrato próprio, com a delimitação das responsabilidades, prazos e demais disposições legais.

**Servidor de e-mail**

A disponibilização do serviço de servidor de e-mail será regulada por contrato próprio, dentro das características de cada contraentes.

O WORKMONITOR se responsabiliza pela configuração e disponibilização do serviço, porém, não é de sua responsabilidade a entrega e recebimento de mensagens, visto que a operação envolve a troca de pacotes dentre servidores e pode ocorrer a perda de mensagens, assim, conteúdos relevantes devem preceder de duplo fator de confirmação.

O gerenciamento das contas poderá ser feito tanto pelo WORKMONITOR quanto pelos contratantes, se dará através de um painel de controle, onde haverá a possibilidade de aumentar a capacidade de armazenamento, criação, suspensão e exclusão de contas, bem como, acesso completo pelo administrador.

A alocação das mensagens será realizada em servidores terceiros, contratados WORKMONITOR e será gerenciado pelo responsável pelo painel de controle, sendo recomendado o arquivamento em outros locais de mensagens e arquivos importantes, visto a temporalidade de armazenamento das mensagens, o que deverá fazer parte do contrato de prestação de serviço.

É responsabilidade do contratante o gerenciamento das senhas e logins de acesso, devendo utilizar padrões adequados e com alta segurança, ainda, regulando e monitorando o acesso em especial em ambientes fora das dependências da organização contratante.

**Dados em nuvem**

O WORKMONITOR utiliza os serviços em nuvem disponibilizados por Oracle Brasil – Aplicações e Plataforma em Nuvem e Amazon Web Services – Amazon AWS, servidores conhecidos e dotados de ampla segurança.

A utilização das plataformas descritas acima é amparada por contratos, onde há a delimitação das respectivas responsabilidades e funcionalidades.

A responsabilização das plataformas se dá apenas pela disponibilidade e segurança dos dados, ressaltando que compete ao contratante estabelecer padrões altos de segurança para conexão.

A utilização do serviço em nuvem deve levar em conta a banda larga utilizada, bem como a finalidade, considerando o tempo de resposta e acesso aos dados, não sendo garantida a conexão em caso de falha ou indisponibilidade de serviço de internet.

É de responsabilidade do contratante informar eventuais restrições geográficas de alocação de dados, sendo neste caso, após a informação, responsabilidade WORKMONITOR a adequação em região que atenda os limites de segurança estabelecidos pela legislação pátria.

É de responsabilidade do contratante o conteúdo dos arquivos alocados na nuvem, bem como, a integridade, livre de malware e ransomware que possam corromper os demais arquivos alocados. Ainda, recomenda-se a utilização de criptografia nos dados e gerenciamento dos arquivos.

Recomenda-se a utilização de criptografia para a guarda de backups em nuvem, sendo que tal responsabilidade pode ser do WORKMONITOR ou da contratante, dependendo da disposição contratual. Em sendo responsabilidade do WORKMONITOR, as chaves de acesso serão longe do acesso de terceiros e com a aplicação de padrões de segurança.

A utilização de nuvem para guarda de dados derivados de programas desenvolvidos WORKMONITOR se dará de forma criptografada, com a aplicação de fatores de segurança e não repúdio.

**Manutenção preventiva e corretiva**

O serviço de manutenção preventiva pode ser realizado nas dependências do contratante ou via acesso remoto, condições a serem estabelecidas contratualmente.

O WORKMONITOR preza pela segurança dos dados confiados, a realização de manutenção precede a abertura de chamado no site (https://www.workmonitor.com/) – onde são lançados o nome da contratante, endereço de e-mail de quem está abrindo o chamado, telefone, CPF do responsável, assunto e descrição do problema, podendo ser anexado arquivo com a descrição.

O atendimento poderá ser presencial ou remoto, no caso de atendimento presencial, além das disposições contratuais específicas, fica registrado:

- Entrada e saída de hardware deverão ser realizada mediante formulário fornecido pelo contratante, ou na sua falta, mediante ordem de serviço.
- Não deverá haver coleta de dados pessoais das bases dos contratantes
- Não deverá ser utilizado login e senha de usuário para reparo e manutenção em sistemas;

No caso de acesso remoto, além da previsão legal, deverão ser observados os seguintes pontos:

- A permissão de acesso deverá ser feita pela direção ou alguém por ela indicada;
- O acesso somente será permitido para resolução da questão descrita no chamado aberto;
- O acesso somente se dará via IP Fixo do WORKMONITOR ou VPN, a depender das disposições contratuais e características dos contratantes.
- Somente funcionários autorizados do WORKMONITOR deverão realizar tal opção.
- Não é autorizada a captura de tela de dados dos clientes.

## TREINAMENTO E VERIFICAÇÕES

O **WORKMONITOR** busca aprimorar e diminuir riscos operacionais, assim, há o pleno comprometimento com a qualificação e treinamento de seus funcionários, sejam eles técnicos ou relativos a temas relevantes e principalmente de segurança da informação.

As verificações devem ocorrer ao menos uma vez ao ano e ter por objetivo assegurar a integridade e segurança de dados, sendo responsabilidade da Encarregada de dados.

## RESPOSTA A INCIDENTES

Com o objetivo de assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil, eventual incidente deverá ser comunicado com urgência, buscando-se atender ao prazo de 48 horas indicado pela ANPD.

A constatação de incidente de segurança deverá ser feita internamente, de acordo com parâmetros definidos pela ABNT, ISO 22301.

Ocorrendo eventual evento de segurança, o qual deverá ser validado internamente, sendo obrigatório o registro, os terceiros interessados deverão ser comunicados, constando os eventos identificados, ações tomadas e eventuais prejuízos.

Os titulares de dados deverão ser comunicados, num prazo de até 15 dias úteis, constando na notificação os dados acima e se possível, quais dados foram violados.

Em caso de incidente de segurança de dados passível de comunicação para ANPD -Autoridade Nacional de Proteção de Dados, após deliberação com o terceiro contratualmente ligado, haverá a comunicação devida, observado o formulário anexo ao presente relatório.

## GESTÃO DE TERCEIROS

Todos os terceiros que se relacionem com **WORKMONITOR** deverão firmar contratos e termos de confidencialidade, com exceção de serviços esporádicos, tais como manutenção elétrica e/ou ar-condicionado, aferição de equipamentos e outros sem acesso a informações.

- Todos os contratos devem ser elaborados e assinados pela alta direção;
- Os contratos devem obedecer às regras civis, do direito contratual, proteção de dados e outras normas correlatas;
- Todos os contratos devem ser registrados, arquivados e monitorados;
- A presente política e normas de segurança devem de conhecimento de terceiros;
- É obrigação do Encarregado de Dados coletar ciência daqueles que prestarem serviços dentro das instalações da organização.

## PENALIDADES

O descumprimento da presente política poderá acarretar sanções cíveis e criminais para aqueles que manifestamente agirem em desconformidade com a legislação pátria, além de responsabilidade trabalhista.

## ENCARREGADO DE DADOS

Nos termos do artigo 41 da Lei Geral de Proteção de Dados, o **WORKMONITOR** nomeia como responsável, na data de 01 de abril de 2023, o funcionário GUSTAVO LARANJEIRA BARBOSA DA SILVA - ficando esta responsável pelas funções designadas em lei e pelas respostas através do e-mail contato@smartcomputadores.com.br.

A presente nomeação tem prazo indeterminado e poderá ser revogada ou alterada a critério da alta direção, porém, nunca ficando vago o cargo.

## ATUALIZAÇÕES

Esta política entra em vigor em 01 de maio de 2025, substituindo a versão 2.0, e possui prazo indeterminado, porém, podendo ser alterada sempre que houver necessidade ou ao menos validada anualmente, mediante simples aditivo.

Bauru, 01 de maio de 2025

gustavo.laranjeira@spa.tec.br
Assinado
GUSTAVO LARANJEIRA BARBOSA DA SILVA
D4Sign

**WORKMONITOR**

SMART- COMPUTADORES E SERVIÇOS LTDA, CNPJ – 03.959.325/0001-94

S.P.A TECNOLOGIA LTDA, CNPJ – 48.035.953/0001-11

25 páginas - Datas e horários baseados em Brasília, Brasil
**Sincronizado com o NTP.br e Observatório Nacional (ON)**
Certificado de assinaturas gerado em 09 de May de 2025, 15:41:54

# Politica Seguranca da Informação V 2 1 -WorkMonitor pdf

Código do documento 2e372668-1f38-4e50-9ce9-9d5464f973f7

## Assinaturas

Gustavo Laranjeira Barbosa Da Silva
gustavo.laranjeira@spa.tec.br
Assinou

GUSTAVO LARANJEIRA BARBOSA DA SILVA

## Eventos do documento

**09 May 2025, 15:37:54**
Documento 2e372668-1f38-4e50-9ce9-9d5464f973f7 **criado** por GUSTAVO LARANJEIRA BARBOSA DA SILVA (50b93576-41ec-4a14-945d-3f3c5fb81bb0). Email:gustavo.laranjeira@spa.tec.br. - DATE_ATOM: 2025-05-09T15:37:54-03:00

**09 May 2025, 15:41:15**
Assinaturas **iniciadas** por GUSTAVO LARANJEIRA BARBOSA DA SILVA (50b93576-41ec-4a14-945d-3f3c5fb81bb0). Email: gustavo.laranjeira@spa.tec.br. - DATE_ATOM: 2025-05-09T15:41:15-03:00

**09 May 2025, 15:41:37**
GUSTAVO LARANJEIRA BARBOSA DA SILVA **Assinou** (50b93576-41ec-4a14-945d-3f3c5fb81bb0) - Email: gustavo.laranjeira@spa.tec.br - IP: 201.13.0.135 (201-13-0-135.dsl.telesp.net.br porta: 30766) - Geolocalização: -22.3379456 -49.053696 - Documento de identificação informado: 253.939.258-08 - DATE_ATOM: 2025-05-09T15:41:37-03:00

Hash do documento original
(SHA256):ec2e9545ca2349b546ab4b85bfece11dfae96fbadad433b4d7598b533e4c3030
(SHA512):7fa4128901884ea509312b2ef0fa7fdb7705dc1a051e91d4f2f36c826f7f5d88d85ac9578bfee21c74f70fc0b62ce5df450e385775d10f7cf7173b70bc263785

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

**Esse documento está assinado e certificado pela D4Sign**
**Integridade certificada no padrão ICP-BRASIL**
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.