Política de Segurança da Informação

Inclui gestão de ativos, acessos, treinamento, fornecedores e incidentes

Empresa	Leiloeiro Judicial – Vanderlei Antonio Drabach Leiloes– CNPJ 70.169.624/0001-12 – leiloeirojudicial.com.br
Código / versão	PSI-01 – versão 2.0 (substitui a versão de 11/11/2026)
Aprovada por	Vanderlei Antônio Drabach, Diretor e Leiloeiro responsável
Data de vigência	16/11/2026
Próxima revisão	16/11/2027 (anual, ou antes se houver mudança relevante de lei, sistema ou contrato)
Classificação	Interna – disponível a todos os colaboradores na pasta compartilhada “Políticas”
Referências	ABNT NBR ISO/IEC 27001, 27002 e 27701; Lei nº 13.709/2018 (LGPD)

1. Objetivo e abrangência

Esta política define as regras da Leiloeiro Judicial para proteger a confidencialidade, a integridade e a disponibilidade das informações que trata, incluindo dados pessoais de licitantes, arrematantes, partes de processos e dados recebidos de comitentes e contratantes.

Aplica-se ao Diretor, a todos os colaboradores, estagiários, prepostos e prestadores de serviço que acessem informações, sistemas ou equipamentos da empresa. Todos devem ler este documento e assinar o Termo de Ciência antes de receber qualquer acesso.

2. Responsabilidades

Papel	Responsabilidades
Diretor	Aprova e revisa esta política; autoriza acessos; decide sobre incidentes e sua comunicação.
Encarregado de Dados (DPO)	Atende titulares e a ANPD; orienta a equipe; mantém os registros de treinamento, fornecedores e incidentes.
Colaboradores e prestadores	Cumprem esta política; protegem suas credenciais; comunicam imediatamente qualquer incidente ou suspeita.
Suporte de TI	Configura e mantém antivírus, criptografia, atualizações e backups dos equipamentos.

3. Gestão de ativos

- **Inventário:** a empresa mantém inventário atualizado de equipamentos (notebooks, computadores, celulares corporativos), sistemas, contas e bases de dados, com responsável por cada item. O inventário é revisado a cada 6 meses e sempre que um ativo entra ou sai.
- **Classificação da informação:** Pública (editais e lotes divulgados); Interna (rotinas e documentos de trabalho); Confidencial (dados pessoais, cadastros, documentos de arrematação, dados e credenciais recebidos de comitentes e contratantes).
- **Uso aceitável:** equipamentos e contas da empresa destinam-se ao trabalho. Informação confidencial só é tratada em equipamentos inventariados e protegidos conforme o item 5.
- **Dispositivos pessoais e mídias removíveis:** é proibido copiar ou armazenar cadastros e informações confidenciais em dispositivos pessoais, pen drives ou contas particulares sem autorização expressa do Diretor.

- **Dados de comitentes e contratantes:** são usados somente para a finalidade contratada e não são compartilhados com terceiros sem autorização.
- **Descarte e devolução:** papéis com dados pessoais são fragmentados; equipamentos e mídias são formatados com apagamento seguro antes de descarte, venda ou conserto externo. No desligamento, o colaborador devolve todos os ativos.

4. Gestão de acessos e autenticação segura

- **Privilégio mínimo:** cada pessoa recebe apenas os acessos necessários à sua função, autorizados pelo Diretor e registrados no controle de acessos.
- **Contas individuais:** usuário e senha são pessoais e intransferíveis. É proibido compartilhar credenciais ou usar contas genéricas.
- **Senhas:** mínimo de 12 caracteres, exclusivas para cada serviço, nunca anotadas em papel, planilhas ou mensagens.
- **Autenticação em dois fatores (MFA/2FA):** obrigatória em todas as contas Google, e-mails, plataforma de leilões, bancos e demais sistemas que ofereçam o recurso.
- **Cofre de senhas:** todas as senhas ficam no cofre de senhas adotado pela empresa. As credenciais fornecidas por contratantes (por exemplo, contas @cresolexterno da Cresol) são guardadas exclusivamente no cofre, usadas apenas pelo titular designado e nunca compartilhadas.
- **Contas de administrador:** restritas ao Diretor e a, no máximo, um substituto designado; protegidas por MFA; usadas apenas para tarefas administrativas.
- **Revisão e revogação:** os acessos são revisados a cada 6 meses. No desligamento ou mudança de função, os acessos são revogados ou ajustados em até 24 horas.

5. Proteção dos equipamentos

- **Antimalware:** todo computador e notebook tem antivírus ativo, com proteção em tempo real e atualização automática. É proibido desativá-lo.
- **Criptografia:** o disco de todos os notebooks e computadores Windows é criptografado com BitLocker. A chave de recuperação fica guardada no cofre de senhas.
- **Atualizações:** sistema operacional, navegadores e aplicativos permanecem com atualização automática ativada.
- **Bloqueio de tela:** automático após 5 minutos de inatividade, com senha; o usuário bloqueia a tela ao se ausentar.
- **Backup:** arquivos de trabalho ficam no armazenamento em nuvem corporativo, e não apenas no disco local.
- **Redes:** o Wi-Fi do escritório é protegido por senha forte. Em redes públicas, não se acessam sistemas com dados confidenciais.

6. Treinamento e conscientização em segurança e privacidade

- **Quando:** na admissão, antes da liberação de acessos, e ao menos uma vez por ano para todos, inclusive o Diretor.
- **Conteúdo mínimo:** esta política; LGPD e cuidados com dados pessoais; senhas, MFA e cofre de senhas; identificação de phishing e golpes; como comunicar incidentes.
- **Comprovação:** cada treinamento gera lista de presença assinada e/ou certificado individual, arquivados pelo encarregado por no mínimo 5 anos.

7. Gestão de fornecedores

- **Registro:** a empresa mantém lista dos fornecedores que acessam ou armazenam seus dados (plataforma de leilões, hospedagem, e-mail e nuvem, contabilidade, suporte de TI), com o tipo de dado tratado e o local de armazenamento.
- **Avaliação prévia:** antes da contratação, verifica-se se o fornecedor possui política de privacidade, medidas de segurança adequadas e MFA.
- **Contrato:** os contratos incluem cláusulas de confidencialidade, conformidade com a LGPD, comunicação de incidentes em até 24 horas e devolução ou eliminação dos dados ao término.
- **Revisão:** a lista e a avaliação dos fornecedores são revisadas anualmente.

8. Gestão de incidentes de segurança da informação e privacidade

Incidente é qualquer evento que comprometa ou possa comprometer informações da empresa, tais como: perda ou roubo de equipamento, acesso indevido, vazamento ou envio de dados a destinatário errado, infecção por malware, golpe de phishing bem-sucedido ou indisponibilidade de sistema.

1. **Comunicar:** quem identificar um incidente ou suspeita avisa imediatamente o Diretor e o Encarregado pelo e-mail contato@leiloeirojudicial.com.br ou pelo telefone (49) 9 8827-8663.
2. **Conter:** isolar o equipamento da rede, trocar senhas, encerrar sessões e bloquear contas afetadas, preservando registros e evidências.
3. **Avaliar:** o Encarregado e o Diretor apuram o que ocorreu, quais dados e quantas pessoas foram afetadas e se há risco ou dano relevante aos titulares.
4. **Notificar:** havendo risco ou dano relevante, a ANPD e os titulares afetados são comunicados em até 3 dias úteis do conhecimento do incidente (art. 48 da LGPD e Resolução CD/ANPD nº 15/2024). Se o incidente envolver dados ou credenciais de comitente ou contratante, este é avisado em até 24 horas.
5. **Corrigir e registrar:** elimina-se a causa, restauram-se os sistemas e registra-se o incidente (data, descrição, dados afetados, medidas adotadas, comunicações e lições aprendidas). O registro é mantido por no mínimo 5 anos, mesmo quando o incidente não for comunicado à ANPD.

9. Descumprimento

O descumprimento desta política sujeita o responsável a advertência, suspensão de acessos e rescisão do contrato de trabalho ou de prestação de serviços, conforme a gravidade, sem prejuízo da responsabilização civil e criminal cabível.

10. Aprovação e histórico de versões

Esta política foi aprovada pelo Diretor da Leiloeiro Judicial e entra em vigor em 16/11/2026.

Versão	Data	Alteração	Aprovação
1.0	11/11/2026	Versão inicial (documento integrado de segurança e privacidade).	Diretor
2.0	16/11/2026	Separação em Política de Segurança da Informação (interna) e Política de Privacidade (site); texto simplificado; inclusão de MFA, cofre de senhas, criptografia e antimalware.	Diretor

Chapecó/SC, 18 de novembro de 2026.

Vanderlei Antonio Drabach
Diretor – Leiloeiro Judicial