FORMAÇÃO PRÁTICA EM GESTÃO CONDOMINIAL

Módulo 11
Cibersegurança e proteção de dados

Apostila de estudo e aplicação prática

Síndico Transparente

Conteúdo para síndicos, conselheiros, subsíndicos, equipes e moradores

Apresentação

Condomínios guardam dados pessoais em cadastros, contratos, câmeras, biometria, controles de acesso, aplicativos, e-mails e mensagens. Uma conta invadida, um boleto adulterado ou uma imagem divulgada sem critério pode causar prejuízo financeiro, expor moradores e funcionários e comprometer a confiança na gestão.

Esta apostila reúne uma rotina prática para conhecer os dados tratados, limitar acessos, proteger contas, orientar fornecedores e responder a incidentes. A Lei Geral de Proteção de Dados (LGPD) e a regulamentação da ANPD são consideradas na versão vigente consultada em 2 de novembro de 2026. A aplicação depende do papel de cada agente e dos fatos; dúvidas sobre bases legais, comunicação de incidentes ou direitos dos titulares devem ser encaminhadas à assessoria competente.

O material integra a Formação Prática em Gestão Condominial do Síndico Transparente, apresentada por Josué Leite, administrador de empresas, pós-graduado em Gestão de Recursos Humanos e síndico profissional há mais de 20 anos.

Objetivos de aprendizagem

- Identificar dados pessoais em sistemas e rotinas condominiais.
- Aplicar princípios de finalidade, necessidade, transparência, segurança e prevenção.
- Organizar o uso de CFTV, biometria, aplicativos, grupos de mensagens e registros de acesso.
- Reduzir riscos de golpes digitais e fraudes com boletos e pagamentos.
- Definir controles de acesso a contas, equipamentos, arquivos e fornecedores.
- Reconhecer e encaminhar incidentes com dados pessoais dentro dos prazos aplicáveis.

Como usar esta apostila

O texto serve como material de formação e lista de verificação inicial. Não substitui avaliação jurídica, encarregado de dados, auditoria de segurança, plano de resposta a incidentes ou orientação técnica para sistemas específicos. Não publique imagens, listas ou documentos para “resolver” uma ocorrência sem validar a finalidade e o canal adequado.

1. Dados pessoais na rotina do condomínio

Dado pessoal é informação relacionada a uma pessoa natural identificada ou identificável. Nome, telefone, unidade vinculada a um morador, placa de veículo, registro de entrada e imagem identificável podem ser dados pessoais. Dado biométrico vinculado a uma pessoa é dado pessoal sensível, com proteção reforçada na LGPD.

Rotina ou sistema	Exemplos de dados	Riscos que precisam ser controlados
Cadastro e portaria	Nome, unidade, telefone, visitante, prestador, horário e autorização.	Acesso excessivo, retenção sem finalidade e divulgação indevida.
CFTV	Imagens de moradores, funcionários, visitantes e veículos.	Visualização sem autorização, cópia informal ou publicação em grupos.
Biometria e reconhecimento facial	Características biométricas, identidade e histórico de entrada.	Tratamento de dado sensível, falha de segurança e ausência de alternativa ou transparência.

Rotina ou sistema	Exemplos de dados	Riscos que precisam ser controlados
Aplicativos e nuvem	Chamados, boletos, documentos, comunicados e dados de contato.	Senha compartilhada, conta exposta, acesso de ex-funcionário ou fornecedor sem controle.
Departamento pessoal e contratos	Dados de empregados, terceirizados, prestadores, pagamentos e documentos.	Fraude, exposição de dados financeiros e guarda excessiva.

Consulte a Lei Geral de Proteção de Dados — Lei nº 13.709/2018

2. Princípios para decidir como tratar dados

A LGPD não se resume a obter consentimento ou inserir uma cláusula em contrato. Para cada atividade, a administração deve identificar a finalidade, avaliar uma base legal adequada, limitar os dados ao necessário, informar o tratamento e adotar medidas de segurança compatíveis com os riscos.

Princípio	Pergunta de gestão
Finalidade	Para que o dado é coletado e usado?
Adequação	O uso tem relação com a finalidade informada?
Necessidade	É possível cumprir o objetivo com menos dados ou menos tempo de guarda?
Transparência	A pessoa consegue saber quem trata os dados, por quê e por qual canal perguntar?
Segurança e prevenção	Que medidas reduzem acesso indevido, perda, alteração ou divulgação?
Responsabilização	Há registro de decisões, responsáveis, controles e providências?

A base legal deve ser identificada para cada finalidade. Consentimento não é a única base prevista na lei e nem sempre é a adequada. A administração deve evitar textos genéricos como “coletamos para segurança” sem definir dados, finalidades, acesso e retenção.

3. Governança: controlador, operador e fornecedores

Controlador é quem toma as decisões referentes ao tratamento; operador trata dados em nome do controlador. O nome do contrato não resolve sozinho o papel de cada organização: é necessário observar quem decide as finalidades e os meios essenciais em cada atividade. Um condomínio, uma administradora, uma empresa de portaria e um fornecedor de aplicativo podem assumir papéis diferentes conforme o serviço e as decisões que realmente tomam.

Ator	Pontos de governança
Condomínio e síndico	Definir quem aprova finalidades, acessos e retenção; manter documentos, canal de atendimento e decisões registradas.
Administradora	Esclarecer quais dados trata por instrução, quais decisões toma e como apoia solicitações e incidentes.
Portaria e segurança	Acessar apenas dados necessários ao serviço; receber instruções e comunicar incidentes rapidamente.

Ator	Pontos de governança
Fornecedor de software ou nuvem	Definir segurança, local e prazo de armazenamento, subcontratados, exportação, eliminação e apoio a incidentes.
Encarregado ou canal designado	Receber solicitações e coordenar comunicação entre titulares, agentes de tratamento e ANPD, conforme as regras aplicáveis.

Revise contratos e termos de serviço para incluir escopo, instruções, confidencialidade, controles de acesso, comunicação de incidentes, apoio a solicitações, devolução ou eliminação de dados e procedimento de encerramento. A contratação de terceiro não elimina a necessidade de o condomínio entender o fluxo de dados e verificar responsabilidades.

4. Câmeras, imagens e reconhecimento facial

Câmeras devem ter finalidade definida, posicionamento proporcional e acesso restrito. Instale equipamentos para atender a um objetivo legítimo de segurança, observando privacidade de unidades e áreas em que as pessoas esperam maior intimidade. Não grave ou divulgue imagens como forma de constranger, punir informalmente ou identificar alguém em grupo de mensagens.

4.1 Procedimento para gravações de CFTV

1. Definir por escrito quem pode visualizar, exportar e entregar imagens, e em quais situações.
2. Orientar o solicitante a informar data, faixa de horário, local e motivo, sem exigir dados desnecessários.
3. Preservar o trecho relevante por canal seguro quando houver finalidade legítima e necessidade documentada.
4. Registrar consulta, extração, destinatário, data e justificativa, limitando a cópia ao trecho pertinente.
5. Encaminhar pedidos de autoridades, titulares, advogados ou seguradoras à administração e à assessoria, verificando requisitos legais.
6. Eliminar gravações pelo ciclo definido, salvo retenção justificada por ocorrência, obrigação ou processo.

O acesso por funcionário deve ser individual e rastreável. Contas compartilhadas impedem identificar quem consultou uma gravação. Imagens podem revelar dados de pessoas que não têm relação com o fato; restrinja a visualização e evite encaminhar arquivos por grupos abertos ou celulares pessoais.

4.2 Biometria e reconhecimento facial

Biometria vinculada a uma pessoa é dado pessoal sensível. Antes de contratar reconhecimento facial, avalie finalidade, necessidade, base legal aplicável, segurança, retenção, fornecedor, riscos, transparência e meios alternativos de acesso. O condomínio deve evitar coletar biometria por conveniência se outra solução menos invasiva atender ao objetivo. Analise também os impactos para visitantes, funcionários, crianças, idosos e pessoas com deficiência.

Leia o artigo do blog sobre reconhecimento facial em condomínios e LGPD

5. Aplicativos, e-mail, nuvem e grupos de mensagens

Aplicativos e grupos de mensagens ajudam a comunicação, mas não são repositórios universais para documentos, imagens e dados de acesso. Escolha o canal conforme a sensibilidade da informação, o público que precisa recebê-la e a possibilidade de controlar quem visualiza, encaminha ou guarda o conteúdo.

Canal	Orientação de uso
E-mail institucional	Use para registros administrativos; confirme destinatário e anexos antes de enviar; proteja a conta com autenticação em dois fatores quando disponível.
Aplicativo do condomínio	Revise perfis, permissões, usuários inativos, exportação de dados, suporte e encerramento do contrato.
Grupo de mensagens	Compartilhe avisos gerais; evite listas de visitantes, documentos, dados de funcionários, imagens de CFTV e boletos individualizados.
Armazenamento em nuvem	Use pastas com permissões por função, autenticação forte, histórico de acesso e cópias de segurança testadas.
Celular de funcionário	Evite guardar dados condominiais em aparelhos pessoais; se houver uso autorizado, defina bloqueio, atualização, acesso e remoção remota.

Veja o guia do blog sobre grupos de WhatsApp em condomínios: regras, riscos e limites

6. Controles básicos de cibersegurança

A segurança depende de rotinas consistentes e adequadas ao porte do condomínio. Comece pelas contas que permitem movimentar dinheiro, administrar usuários, acessar câmeras e emitir boletos. Aplique acesso mínimo necessário e retire permissões quando as funções ou contratos terminarem.

- Use uma conta individual para cada funcionário e fornecedor; evite senhas compartilhadas.
- Ative autenticação em dois fatores para e-mail, bancos, aplicativos administrativos, nuvem e redes sociais.
- Use senhas longas e exclusivas; guarde-as em gerenciador confiável, sem planilhas abertas ou papéis expostos.
- Revise usuários e permissões periodicamente e imediatamente após desligamentos ou troca de fornecedor.
- Mantenha computadores, celulares, roteadores, aplicativos e sistemas atualizados.
- Faça cópias de segurança periódicas, protegidas e testadas; mantenha ao menos uma cópia separada do ambiente principal.
- Proteja roteador e Wi-Fi administrativo com senha forte; separe a rede de convidados e dispositivos de automação quando tecnicamente possível.
- Registre quem aprova pagamentos, altera dados bancários de fornecedores e emite segunda via de boletos.

A ANPD disponibiliza um guia de segurança da informação para agentes de tratamento de pequeno porte

7. Golpes digitais e fraude com boletos

Golpistas se aproveitam de urgência, mudanças de gestão e confiança em fornecedores. Podem enviar boleto adulterado, pedir troca de conta bancária, assumir um e-mail ou perfil de WhatsApp e solicitar pagamento “fora do procedimento”. A proteção mais eficaz combina confirmação por canal independente, dupla aprovação e treinamento da equipe.

7.1 Sinais de alerta

- Pedido inesperado para pagar hoje ou ignorar a aprovação habitual.
- Mudança de dados bancários enviada apenas por e-mail ou mensagem.
- Boleto com beneficiário, CNPJ, valor ou vencimento diferente do cadastro esperado.
- Link para atualizar senha ou liberar conta enviado por mensagem não solicitada.
- Mensagem de fornecedor ou síndico com estilo incomum, erros ou pedido de segredo.
- Arquivo compactado, documento inesperado ou código QR recebido de origem não confirmada.

7.2 Rotina de confirmação de pagamento

1. Conferir beneficiário, CNPJ, valor, vencimento e origem do boleto em fonte confiável.
2. Em qualquer alteração de conta, ligar para contato já cadastrado, não para o número fornecido na própria mensagem.
3. Separar preparação e autorização do pagamento; definir limites e aprovadores por escrito.
4. Não abrir links ou anexos inesperados; acessar o portal digitando o endereço conhecido.
5. Registrar a conferência e guardar comprovantes no repositório administrativo.
6. Se houver suspeita de pagamento fraudulento, avisar o banco e a administração imediatamente e preservar mensagens e comprovantes.

8. Direitos dos titulares e atendimento de solicitações

Moradores, visitantes, empregados e prestadores podem exercer direitos previstos na LGPD. O condomínio precisa saber quem recebe os pedidos, como verifica a identidade sem coletar dados em excesso e como encaminha a solicitação aos agentes responsáveis. Alguns direitos dependem da base legal, da finalidade, da existência de obrigação de guarda e de outras hipóteses legais; não prometa exclusão imediata de todo registro.

Pedido recebido	Encaminhamento inicial
Confirmação ou acesso	Registrar o pedido, confirmar a identidade de forma proporcional e localizar o tratamento pertinente.
Correção de cadastro	Verificar a informação com segurança e atualizar sistemas e fornecedores que receberam o dado quando aplicável.
Informação sobre compartilhamento	Identificar prestadores e sistemas envolvidos, respeitando limites legais e segredos protegidos.
Eliminação ou oposição	Verificar base legal, obrigação de guarda, necessidade e eventual retenção legítima; responder com fundamento.
Pedido de imagens de CFTV	Encaminhar à administração e assessoria; verificar terceiros identificáveis, finalidade, segurança e forma de atendimento.

Consulte as orientações da ANPD sobre direitos dos titulares de dados

9. Resposta a incidentes de segurança

Incidente pode incluir acesso indevido, perda, alteração, destruição ou divulgação de dados pessoais. Uma vulnerabilidade ainda não explorada não é necessariamente um incidente. Confirme os fatos, contenha o problema e avalie quais dados e pessoas foram afetados. Não apague evidências nem tente esconder o ocorrido.

9.1 Primeiras providências

1. Receber e registrar o alerta, horário, sistema, pessoa que percebeu e sinais observados.
2. Conter o acesso indevido com apoio técnico: bloquear conta comprometida, revogar sessões ou isolar equipamento quando apropriado.
3. Preservar evidências e registros, sem alterar arquivos ou encaminhar dados por canais abertos.
4. Identificar dados, titulares, volume, período, sistemas e fornecedores envolvidos.
5. Acionar síndico, administradora, fornecedor, assessoria jurídica e encarregado ou canal designado.
6. Avaliar riscos e danos potenciais, medidas de mitigação e necessidade de comunicação.
7. Registrar decisões, prazos, responsáveis, avisos e lições para corrigir o processo.

A ANPD informa que a comunicação regulatória cabe ao controlador quando o incidente confirmado envolve dados pessoais e pode acarretar risco ou dano relevante aos titulares. Pela Resolução CD/ANPD nº 15/2024, a comunicação à ANPD e aos titulares deve ser feita em até três dias úteis, contados do conhecimento de que o incidente afetou dados pessoais, ressalvada regra específica. Se faltarem informações, a comunicação pode ocorrer em etapas, com justificativa e complementação conforme o regulamento. A classificação do incidente, o responsável e o conteúdo do aviso devem ser definidos com apoio jurídico e técnico.

Consulte a página oficial da ANPD sobre comunicação de incidentes de segurança

9.2 O que a comunicação deve esclarecer

- Qual categoria de dados foi afetada e quais impactos são possíveis.
- Quando o controlador tomou conhecimento e o que já foi confirmado.
- Quais medidas foram adotadas ou serão adotadas para conter e reduzir os efeitos.
- Qual canal os titulares podem usar para obter informações.
- Quais dados ou hipóteses continuam em apuração e quando haverá atualização.

10. Estudos de caso

Caso 1 — Imagem de câmera enviada a grupo

Um funcionário compartilha no grupo de moradores um vídeo de uma pessoa retirando objeto da garagem. A administração solicita que o conteúdo não seja replicado, preserva o arquivo original por canal restrito, registra quem acessou e encaminha o caso para análise e providências legais, sem expor a pessoa publicamente.

Caso 2 — Boleto com nova conta bancária

Chega mensagem de fornecedor informando mudança urgente de conta. O financeiro liga para o telefone cadastrado anteriormente e confirma que a solicitação é falsa. O condomínio não paga o documento, guarda a mensagem e avisa administradora e banco se houver credenciais ou dados expostos.

Caso 3 — Ex-funcionário ainda acessa as câmeras

Na troca de empresa, a equipe descobre que uma senha antiga permanece ativa. O condomínio pede bloqueio imediato, revisa todas as contas e sessões, exige nova lista de usuários e registra a ação. O contrato passa a prever revogação e devolução de acessos na saída.

Caso 4 — Morador pede cópia das imagens

A administração recebe pedido de gravação de horário em que houve avaria. Registra o objetivo e a faixa temporal, preserva o trecho relevante e encaminha a análise. A resposta considera as imagens de terceiros, a finalidade e os procedimentos jurídicos para disponibilização.

11. Exercícios e modelos práticos

11.1 Exercício: mapa de dados

Escolha três rotinas do condomínio e anote: qual dado é coletado, finalidade, base legal a validar, sistema, pessoas com acesso, fornecedor, prazo de guarda e procedimento de eliminação.

11.2 Checklist de segurança mensal

- ☐ Contas bancárias, e-mail, nuvem e câmeras têm usuários individuais.
- ☐ Autenticação em dois fatores está ativa nos serviços que a oferecem.
- ☐ Acessos de ex-funcionários e prestadores foram removidos.
- ☐ Cópias de segurança foram concluídas e um teste de restauração foi feito.
- ☐ Sistemas e equipamentos recebem atualizações de segurança.
- ☐ Dados e imagens estão sendo compartilhados somente com pessoas autorizadas.
- ☐ Contatos de resposta a incidentes e fornecedores estão atualizados.
- ☐ A equipe conhece o procedimento para confirmar boletos e pedidos urgentes.

11.3 Ficha de registro de incidente

Campo	Preencher
Data e hora do alerta / conhecimento	_____
Pessoa e canal que reportaram	_____
Sistema, conta ou equipamento afetado	_____
Dados e titulares potencialmente envolvidos	_____
Ações de contenção e evidências preservadas	_____
Fornecedores e responsáveis acionados	_____
Avaliação de risco e decisão de comunicar	_____
Prazo, responsável e próxima atualização	_____

11.4 Modelo de aviso interno à equipe

“Foi identificado um possível incidente envolvendo [sistema ou rotina]. Não encaminhe mensagens, arquivos ou imagens relacionados e não apague registros. Informe imediatamente à administração pelo canal [canal], incluindo horário, tela ou mensagem recebida e ações já realizadas. A equipe técnica e a administração coordenarão as providências. Não responda a solicitações externas sobre o caso sem orientação.”

11.5 Perguntas para revisar um fornecedor

- Quais dados o serviço recebe, armazena, compartilha ou exporta?
- Quem administra usuários e como são revogados os acessos?
- Qual é o canal e o prazo de aviso ao condomínio em caso de incidente?
- Há cópias de segurança, criptografia, registros de acesso e plano de continuidade?
- Como os dados são devolvidos ou eliminados no encerramento do contrato?

12. Plano de ação para os primeiros 30 dias

Período	Ação	Entrega
Dias 1 a 7	Inventariar sistemas, dados, câmeras, biometria, contratos e canais de comunicação.	Mapa inicial de dados e acessos.
Dias 8 a 14	Revisar contas, usuários, autenticação, permissões e rotina de pagamentos.	Lista de correções imediatas e responsáveis.
Dias 15 a 21	Revisar contratos, avisos de privacidade, retenção de gravações e canais de titulares.	Plano de governança e lacunas documentais.
Dias 22 a 30	Treinar equipe e simular golpe de boleto ou incidente de acesso a imagens.	Registro de treinamento e roteiro de resposta.

Revisão do módulo

- Câmeras, biometria, placas e registros de acesso podem conter dados pessoais.
- Biometria vinculada a uma pessoa é dado pessoal sensível e exige cuidado reforçado.
- Consentimento não é a única base legal; a finalidade e a base precisam ser avaliadas para cada atividade.
- Imagens de CFTV devem ser acessadas e compartilhadas por procedimento restrito e registrado.
- Confirme mudanças bancárias por um canal independente e não compartilhe senhas.
- Incidentes com risco relevante podem exigir comunicação pelo controlador; registre, contenha e avalie rapidamente.

Glossário essencial

Termo	Significado neste módulo
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.

Termo	Significado neste módulo
Dado pessoal sensível	Categoria especial prevista na LGPD, incluindo dado biométrico vinculado a pessoa natural.
Controlador	Agente que toma decisões referentes ao tratamento de dados pessoais.
Operador	Agente que trata dados pessoais em nome do controlador.
Encarregado	Canal de comunicação entre agentes de tratamento, titulares e ANPD conforme a LGPD.
Incidente de segurança	Evento que compromete confidencialidade, integridade ou disponibilidade de dados ou sistemas.
Autenticação em dois fatores	Verificação de identidade por dois elementos diferentes, além ou em complemento à senha.

Referências e leituras complementares

BRASIL. Lei nº 13.709/2018 — LGPD: texto oficial no Planalto

ANPD. Resolução CD/ANPD nº 15/2024 e comunicação de incidentes: orientações e prazos oficiais

ANPD. Guia de segurança da informação para agentes de pequeno porte: guia oficial

ANPD. Direitos dos titulares: orientação oficial

Leituras do Síndico Transparente: Reconhecimento facial em condomínios: segurança e LGPD; Grupos de WhatsApp em condomínios: regras, riscos e limites

Nota de atualização: normas e orientações podem mudar. A comunicação de incidentes deve ser decidida pelo controlador após avaliação dos fatos, dos dados afetados e do risco aos titulares. Esta apostila é educativa e não substitui orientação jurídica, análise técnica de segurança, política de privacidade ou resposta especializada a incidentes.

Encerramento

Proteção de dados exige rotina: conhecer o que se guarda, limitar acessos, proteger contas, confirmar pagamentos e agir com rapidez diante de incidentes.