POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E TI

Diretrizes administrativas, lógicas e operacionais do ambiente local

Documento	**Políticas de Segurança da Informação e TI**
Unidade	**CARTÓRIO PALMINÓPOLIS - OFÍCIO ÚNICO**
CNPJ	57239152000169
Endereço	Rua Elpidio De Paula Ribeiro, 28-A, Centro - Palminópolis/GO
Responsável (Controladora)	**Renata Santiago Strassburger**
E-mail institucional	cartorio@palminopolis.com
Encarregado de Dados (DPO)	**LARYSSA ANDREL ALVES NUNES – cartoriopalminopolis@gmail.com**
Versão	1.0
Data de aprovação	06/07/2026
Próxima revisão	06/07/2027 – NO MÁXIMO 12 MESES

Sumário

Após abrir o documento no Word, clique com o botão direito no sumário abaixo e selecione "Atualizar campo" para refletir números de página corretos.

Objetivo e abrangência

Este documento consolida as políticas de segurança da informação e de uso dos recursos de TI aplicáveis ao CARTÓRIO PALMINÓPOLIS - OFÍCIO ÚNICO, em atendimento ao Provimento CNJ nº 213/2026, à Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e às boas práticas de segurança da informação.

As diretrizes aqui descritas se aplicam a colaboradores, prepostos, substitutos, escreventes, prestadores de serviço autorizados e quaisquer terceiros que utilizem recursos tecnológicos da serventia.

Princípios gerais

- **Privilégio mínimo**: cada usuário deve ter somente os acessos necessários para sua função.
- **Responsabilização**: toda ação executada com credenciais individuais é atribuída ao respectivo usuário.
- **Segurança por camadas**: proteção de borda, antivírus, backup, autenticação centralizada e segregação de funções.
- **Revisão contínua**: políticas e acessos devem ser revistos periodicamente e sempre que houver mudança relevante.
- **Conformidade legal**: aderência ao **Provimento CNJ nº 213/2026**, à LGPD e às demais normas aplicáveis aos serviços notariais e de registro.

1. Política de contas e acessos

- Contas de rede devem ser individuais e vinculadas ao colaborador autorizado; é vedado o uso de contas genéricas ou compartilhadas.
- Criação, alteração e desligamento de acessos devem ocorrer mediante solicitação formal do responsável do setor.
- Contas administrativas devem ser restritas à equipe de TI e usadas somente para atividades técnicas.
- O desligamento ou mudança de função de usuários deve gerar revisão imediata dos acessos e grupos.
- Acessos privilegiados devem ser revistos no mínimo **a cada 3 meses**.

2. Política de senhas e bloqueio de sessão

- Senhas devem possuir no mínimo 8 caracteres, com combinação de letras maiúsculas, minúsculas, números e, sempre que possível, caracteres especiais.
- É proibido compartilhar senhas, anotá-las em local visível ou enviá-las por e-mail/mensagens sem proteção adequada.
- As estações devem ser bloqueadas automaticamente por inatividade, conforme GPO aplicada no domínio (sugestão: 10 minutos).

- Tentativas excessivas de autenticação sem sucesso devem gerar bloqueio conforme política vigente do domínio.
- Credenciais privilegiadas devem ser distintas das credenciais de uso comum do usuário.
- Sempre que disponível, deve ser adotada autenticação multifator (MFA), em especial para acessos administrativos e remotos.

3. Política de estações de trabalho e software

- A instalação ou remoção de softwares somente pode ser realizada pela equipe de TI ou mediante autorização formal.
- Não é permitido instalar programas sem licença, utilitários de origem duvidosa ou aplicações sem relação com a atividade do cartório.
- A solução de antivírus/EDR – Bitdefender – Data de Vencimento: 17/06/2028 deve permanecer ativa e gerenciada em todos os ativos compatíveis.
- Dispositivos devem receber atualizações e correções conforme janela operacional definida pela TI.
- A elevação de privilégios locais deve seguir controle técnico e administrativo.
- Estações sem uso prolongado devem ser desligadas ou colocadas em espera, salvo quando houver rotina técnica que exija o equipamento ligado.

4. Política de arquivos, servidor de arquivos e mídia removível

- Documentos de trabalho do cartório devem ser armazenados preferencialmente no servidor de arquivos – ou em locais homologados pela TI.
- As permissões de acesso aos compartilhamentos devem seguir grupos e ACLs integrados ao AD.
- O uso de dispositivos USB é controlado por política de domínio; exceções devem ser formalmente autorizadas e registradas.
- É vedada a cópia não autorizada de dados institucionais para mídias pessoais ou serviços externos não homologados (ex.: Google Drive pessoal, OneDrive pessoal, WhatsApp pessoal).
- Mídias removíveis utilizadas para tarefas autorizadas devem ser higienizadas/criptografadas conforme orientação da TI.

5. Política de Internet, e-mail e navegação

- O acesso à Internet deve ser utilizado prioritariamente para atividades relacionadas ao serviço.
- O firewall Pfsense – Realiza a proteção de borda e o NXFILTER completa o controle de navegação.

- É proibido abrir anexos ou links suspeitos, principalmente de remetentes desconhecidos.
- O e-mail institucional não deve ser utilizado para cadastros pessoais, redes sociais não autorizadas ou campanhas em massa sem aprovação.
- Sempre que houver dúvida sobre mensagem suspeita, o usuário deve interromper a ação e acionar a TI.

6. Política de acesso remoto

- Acessos remotos devem ser autorizados e realizados por meio seguro (VPN ou solução homologada), com registro e controle pela equipe de TI.
- Equipamentos externos que se conectem ao ambiente do cartório devem manter padrão mínimo de segurança (antivírus ativo, sistema operacional atualizado e tela bloqueável).
- Credenciais de acesso remoto não podem ser compartilhadas com familiares, colegas ou terceiros não autorizados.
- Sessões remotas inativas devem encerrar-se automaticamente conforme política técnica.

7. Política de backup, réplica e retenção operacional

Ativo	Proteção vigente	Destino	Finalidade
Chevette Backup	A Cada 24h	\\192.168.0.230\BackupVMs	Proteção de arquivos operacionais
Chevette Backup Cloud	A Cada 24	1ri-palminopolis	Proteção de arquivos operacionais
Chevette Réplica	A Cada 24h	Porsche	Proteção de arquivos operacionais
Corcel (Sistema) Backup	A Cada 30 min	\\192.168.0.230\BackupVMs	Proteção de arquivos operacionais

Ativo	Proteção vigente	Destino	Finalidade
Corcel (Sistema) Backup Cloud	Diário 03:20	1ri-palminopolis	Proteção de arquivos operacionais
Corcel (Sistema) Réplica	A Cada 30 min	Porsche	Proteção de arquivos operacionais
Corsa Backup	A Cada 24h	\ \192.168.0.230\BackupVMs	Proteção de arquivos operacionais
Corsa Réplica	A Cada 24h	Ferrari	Proteção de arquivos operacionais
Escort Backup	Diário 20:00	\ \192.168.0.230\BackupVMs	Proteção de arquivos operacionais
Escort Backup Cloud	A Cada 24h	1ri-palminopolis	Proteção de arquivos operacionais
Escort Réplica	Diário 21:00	Porsche	Proteção de arquivos operacionais
Fusca Backup	A Cada 24h	\	Proteção de

Ativo	Proteção vigente	Destino	Finalidade
		\192.168.0.230\BackupVMs	arquivos operacionais
Fusca Backup Cloud	A Cada 24h	1ri-palminopolis	Proteção de arquivos operacionais
Fusca Réplica	A Cada 24h	Ferrari	Proteção de arquivos operacionais
Uno (CheckMK) Backup	A Cada 24h	\ \192.168.0.230\BackupVMs	Proteção de arquivos operacionais
Uno (CheckMK) Réplica	A Cada 24h	Ferrari	Proteção de arquivos operacionais

As rotinas devem ser monitoradas e testadas periodicamente. Falhas de execução devem gerar análise, correção e novo teste de restauração.

Testes formais de restauração devem ocorrer no mínimo **a cada 6 meses** com registro do resultado.

8. Política de segurança física e energia

- A sala/rack de equipamentos deve permanecer com acesso controlado.
- Os nobreaks – 1 nobreak SMS 1500VA – devem receber manutenção preventiva e validação periódica de autonomia.
- Intervenções físicas em servidores, storage, switches, firewall ou cabeamento devem ser executadas por pessoal autorizado.

- Câmeras, controle de acesso e demais sistemas de segurança física devem ser mantidos em funcionamento e revisados periodicamente.

9. Política de monitoramento, incidentes e auditoria

- Incidentes de segurança ou indisponibilidade devem ser registrados, classificados e tratados formalmente.
- Alertas provenientes do antivírus/EDR, do backup ou da infraestrutura devem ser avaliados pela TI.
- Evidências de incidentes relevantes devem ser preservadas para análise posterior e eventual auditoria.
- Incidentes de segurança que envolvam dados pessoais devem ser comunicados à Corregedoria competente e à ANPD nos prazos legais, observado o Provimento CNJ nº 213/2026 e a LGPD.
- Este documento deve ser revisado ao menos uma vez por ano ou quando houver mudança material na infraestrutura.

10. Política de mesa limpa e tela limpa

Esta política tem por objetivo reduzir o risco de exposição não autorizada de informações sensíveis em ambientes de trabalho do cartório, considerando o trânsito constante de usuários, partes interessadas e prestadores de serviço.

10.1. Mesa limpa

- Documentos contendo dados pessoais, informações sigilosas ou minutas de atos não devem permanecer expostos sobre mesas, balcões ou bancadas quando o colaborador estiver ausente.
- Ao final do expediente, todo material físico sensível deve ser guardado em gavetas, armários ou arquivos com fechadura.
- Chaves de gavetas, armários, cofres e malotes devem ser mantidas sob responsabilidade do usuário designado, sendo vedado deixá-las à vista.
- Documentos descartados que contenham dados pessoais ou sigilosos devem ser fragmentados (picotados) antes do descarte; é vedado descarte direto em lixo comum.
- Carimbos, selos, livros e mídias com informações institucionais devem ser guardados em local seguro quando não estiverem em uso.
- Senhas e credenciais não podem ser anotadas em papéis, post-its, agendas ou qualquer suporte visível.

10.2. Tela limpa

- Estações de trabalho e notebooks devem ser bloqueados (Windows + L ou equivalente) sempre que o usuário se afastar, mesmo por curto período.
- O bloqueio automático por inatividade deve permanecer habilitado conforme GPO do domínio.

- Sistemas com dados sensíveis (sistema notarial/registral, e-mail, sistemas do tribunal, ONR, e-Notariado etc.) não devem ser exibidos em telas voltadas para o público.
- Em videoconferências e compartilhamentos de tela, deve-se evitar exibir áreas de trabalho, e-mails ou documentos não relacionados ao assunto tratado.
- Ao final do expediente, os equipamentos devem ser bloqueados ou desligados, conforme orientação da TI.

10.3. Impressão e digitalização

- Documentos enviados para impressão devem ser retirados imediatamente da impressora.
- Impressões esquecidas que contenham dados pessoais devem ser fragmentadas; nunca reaproveitadas como rascunho fora do cartório.
- Scanners e copiadoras compartilhados devem ter sua memória interna limpa periodicamente, conforme orientação da TI.

10.4. Reuniões e atendimento

- Quadros, *flipcharts* e anotações utilizados em reuniões devem ser apagados/recolhidos ao término.
- Em atendimentos presenciais, os documentos do cliente devem ser conferidos e devolvidos ou arquivados imediatamente, evitando seu acúmulo no balcão.

11. Política de cookies

Esta seção integra as políticas de privacidade do cartório e disciplina o uso de cookies e tecnologias similares no(s) site(s) e aplicação(ões) institucional(is) operados por CARTÓRIO PALMINÓPOLIS - OFÍCIO ÚNICO, inscrito no CNPJ 57239152000169, doravante denominado CONTROLADORA.

Em sites diversos, redes sociais e afins, recomenda-se ao usuário consultar também a política de *cookies* dos respectivos proprietários. Caso sejam utilizados *cookies* de terceiros (comuns em publicidade), o usuário será avisado e deverá conceder anuência.

O usuário pode controlar os *cookies* pelo pop-up (janela) que abre ao acessar o site/aplicação e, além de autorizar o uso, pode escolher quais utilizar durante a navegação (ressalvando que, dependendo do *cookie*, a navegação pode tornar-se menos prática).

11.1. Dos cookies

Cookies são pequenos arquivos – fragmentos ou textos – contendo informação que são baixados em seu computador, smartphone ou qualquer outro dispositivo com acesso à internet quando o usuário utilizar nosso site/aplicação.

Nesses arquivos são contidas informações sobre a navegação em nossas páginas, retendo apenas dados relacionados às suas preferências, melhorando e tornando prática a sua navegação. A maioria das informações é apagada logo ao encerrar a sessão.

11.2. Tipos de cookies e motivos

Quanto a seus proprietários

- *Cookies* proprietários: definidos por nós ou por terceiros em nosso nome.
- *Cookies* de terceiros: definidos por terceiros confiáveis em nossa aplicação (por exemplo, quando se utiliza o site para demonstrar publicidade).

Quanto ao seu tempo de vida

- *Cookies* de sessão ou temporários: expiram assim que o usuário fecha o navegador, encerrando a sessão.
- *Cookies* persistentes ou permanentes: permanecem no dispositivo durante um período determinado ou até que sejam excluídos.

Quanto à sua finalidade

- *Cookies* necessários: essenciais à navegação e ao acesso a todos os recursos; sem estes os serviços podem apresentar desempenho não satisfatório ou não funcionar.
- *Cookies* de desempenho: otimizam o funcionamento das aplicações coletando informações anônimas sobre as páginas acessadas.
- *Cookies* de funcionalidade: memorizam preferências e escolhas (como nome de usuário) e usos de APIs para otimização.
- *Cookies* de publicidade: direcionam anúncios em função dos interesses e limitam a quantidade de vezes que o anúncio aparece (podem ser *cookies* de terceiros).

Motivação dos cookies

A instituição utiliza *cookies* para fornecer a melhor experiência de uso, tornando as aplicações mais fáceis e personalizadas, com base nas escolhas e no comportamento de navegação. As categorias acima, conforme forem utilizadas, serão listadas e, sempre que possível, com escolha de aceitação pelo usuário.

11.3. Cookies utilizados pela instituição

Dentre os possíveis *cookies* destacados, e enumerados em documento próprio pela ANPD (Autoridade Nacional de Proteção de Dados), o usuário pode verificar quais são utilizados na pop-up de *cookies* presente em nossas aplicações, podendo, além de decidir se aceitará o uso, autorizar especificamente aqueles aos quais consentir.

11.4. Gerenciamento dos cookies

A instalação dos *cookies* está sujeita ao seu consentimento. Apesar de a maioria dos navegadores estar inicialmente configurada para aceitar *cookies* de forma automática, o usuário pode rever suas permissões a qualquer tempo, de forma a bloqueá-los, aceitá-los ou ativar notificações para quando alguns *cookies* forem enviados ao dispositivo.

Na primeira vez que o usuário acessa nossas aplicações, será requerida a sua concordância com a instalação destes; apenas após a aceitação serão ativados.

Para tanto, utilizamos um sistema de banner (em duas camadas – duas janelas) de informações ou outro mecanismo que alerta e solicita o consentimento na página inicial da instituição. A navegação continuada nos sites será entendida como consentimento.

O usuário pode, a qualquer tempo e sem nenhum custo, alterar as permissões, bloquear ou recusar os *cookies*, ou ainda configurá-los caso a caso. Todavia, a revogação do consentimento de determinados *cookies* pode inviabilizar o funcionamento correto de alguns recursos da plataforma.

Para gerenciar os *cookies* do navegador, basta fazê-lo diretamente nas configurações do navegador, na área de gestão de cookies. Tutoriais oficiais podem ser consultados nos sites dos respectivos navegadores (Internet Explorer, Firefox, Safari, Google Chrome, Microsoft Edge e Opera).

11.5. Formas de identificação adicionais

Web beacons

Web beacons (também conhecidos como tags de internet, pixels e GIFs invisíveis ou minúsculos) são imagens gráficas transparentes colocadas em um site ou e-mail. São usados em combinação com cookies para aprender sobre as interações e capturar a jornada do usuário, criar categorias de segmento e padrões de comportamento ou veicular anúncios direcionados. A instituição (ou terceiros contratados) pode utilizar beacons para obter informações como endereço IP, URL da página, horário de visualização e tipo de navegador usado.

Endereços IP e URLs

Um endereço IP é o identificador do dispositivo na rede. Quando o usuário visita o site, podemos visualizar o endereço IP utilizado para conectar-se à internet. A instituição utiliza apenas a parte editada do endereço IP para determinar a localização física mais ampla (por exemplo, cidade e país), sem identificar localização precisa. Caso fôssemos coletar dados de localização precisos para fins publicitários, disponibilizaríamos opção para obter consentimento.

IDs do dispositivo

IDs do dispositivo são identificadores numéricos atribuídos a um smartphone ou dispositivo portátil semelhante a partir do qual a internet pode ser acessada. Esses IDs podem ser utilizados para os mesmos fins buscados com os cookies, conforme descrito nesta política.

Impressão digital do dispositivo

A impressão digital do dispositivo é uma combinação de identificadores atribuídos a um dispositivo (sistema operacional, tipo e versão do navegador, configurações de idioma, endereços IP, entre outros), usados para identificá-lo e singularizá-lo. A finalidade dessa identificação é equivalente à dos cookies.

11.6. Controle de cookies de modo detalhado

- **Modelo opt-in**: consentimento por meio do banner de cookies exibido ao usar o site. Algumas funcionalidades podem exigir cookies de terceiros, ativados apenas mediante interação específica.
- **Modelo opt-out**: desativação dos cookies a qualquer momento no Portal de Preferências de Cookies ou nas configurações do navegador.
- **Portal de preferências**: pop-up em duas camadas que permite alterar preferências (exceto cookies obrigatórios) a qualquer momento.
- **Navegador**: é possível alterar a aceitação de cookies diretamente nas configurações do navegador utilizado.
- **Dispositivos móveis**: as operações também podem ser realizadas em dispositivos portáteis (iOS: Configurações → Privacidade → Publicidade → Limitar Rastreamento de Anúncios; Android: Configurações → Google → Anúncios → Desativar anúncios baseados em interesses).

11.7. Duração dos cookies

Os cookies utilizados duram o necessário para melhor navegação e uso das aplicações. Os cookies de sessão expiram imediatamente após o término da navegação no site.

11.8. Alterações na política de cookies

Quaisquer alterações no uso de cookies serão publicadas na pop-up ou portal de preferências de cookies. Caso as alterações sejam significativas, tomaremos medidas para que o usuário tenha ciência. Mantenha-se informado quanto à versão mais recente desta política, disponível no site institucional.

11.9. Contato sobre a política de cookies

Em caso de dúvidas sobre esta política ou sobre o uso de cookies, o usuário pode entrar em contato pelo e-mail cartoriopalminopolis@gmail.com ou direcionar questionamentos aos cuidados do encarregado pelo tratamento de dados pessoais.

12. Disposições finais

- O descumprimento das diretrizes deste documento sujeita o infrator às medidas administrativas, contratuais e legais cabíveis.
- Casos omissos serão decididos pelo responsável pela serventia, ouvido o encarregado pelo tratamento de dados pessoais e a TI.
- Esta política entra em vigor na data de sua aprovação e será revisada conforme periodicidade definida na ficha de identificação.

Palminópolis, 06/07/2026.

RENATA SANTIAGO STRASSBURGER:00841538069

Assinado de forma digital por RENATA SANTIAGO STRASSBURGER:00841538069
Dados: 2026.07.06 14:57:21 -03'00'

Responsável pela Serventia (Controladora)
Renata Santiago Strassburger