Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

Política de Segurança da Informação

Código:	PSI 01
Versão:	1.2
Data da versão:	10/01/2025
Criado por:	LP Consultoria jurídica
Aprovado por:	Giovana Manfron da Fonseca Maniglia
Nível de confidencialidade:	Pública

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
04/09/2022	1.0	LP Cons.	Criação da Política de Privacidade e Proteção de Dados
09/02/2023	1.1	LP Cons.	Revisão Titular – GMFM e Encarregado EJT
16/01/2025	1.2	LP Cons.	Revisão Titular – GMFM e Encarregado EJT

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

Sumário

1. INTRODUÇÃO

1.1. A informação é um recurso fundamental para o desenvolvimento das atividades do Serviço Distrital da Barreirinha e, como tal, necessita ser protegida. A Política de

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

Segurança da Informação visa preservar a confidencialidade, a integridade e a disponibilidade da informação.

1.2. Este documento estabelece os princípios e diretrizes que norteiam a segurança da informação no Serviço Distrital da Barreirinha Curitiba. É aprovado e divulgado por decisão do Delgatário da Serventia, que apoia e fomenta as iniciativas necessárias ao alcance dos objetivos de segurança estabelecidos.

2. OBJETIVO

2.1. Estabelecer princípios e orientar a definição de mecanismos de segurança que garantam o cuidado, a legalidade, e excelência na prestação dos serviços extrajudiciais desta serventia. Assim como, preservando a continuidade dos seus negócios.

2.2. Definir o escopo da segurança da informação no Serviço Distrital da Barreirinha e suas diretrizes para manuseio seguro dos seus ativos.

2.3. Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3. NORMAS RELACIONADAS

3.1 LGPD - LEI Nº 13.709/ 2018.
3.2 PROVIMENTO CNJ Nº 74/2018
3.3 ABNT ISO/IEC 27701:2019
3.4 PROVIMENTO CGJ-CG Nº 302/2021
3.5 PROVIMENTO CNJ Nº 134/2022
3.6 PROVIMENTO CNJ Nº 149/2023
3.7 PROVIMENTO CNJ Nº 161/2024

4. ABRANGÊNCIA

4.1. Esta política aplica-se ao Delegatário, funcionários, contratados, temporários, fornecedores ou qualquer parte envolvidas com os serviços prestados pelo Serviço Distrital da Barreirinha. Deve ser lida e conhecida por todos os usuários da informação.

4.2. A política é aplicável ao ambiente do Serviço Distrital da Barreirinha, assim como o informatizado de armazenamento da informação. Abrange todos os equipamentos e sistemas possuídos ou utilizados pelo Serviço Distrital da Barreirinha para estes fins.

5. GLOSSÁRIO

5.1. Ativos: Qualquer coisa que tenha valor para a organização.

5.2. Ativos de informação: Qualquer informação que tenha valor para a organização.

5.3. Colaboradores: funcionários, estagiários, fornecedores, terceirizados ou quaisquer outras pessoas que sejam usuários de informações.

5.4. Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

5.5. Integridade: salvaguarda da exatidão, completeza da informação e dos métodos de processamento.

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

5.6. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes.
5.7. Custodiante: pessoa ou órgão com atribuição fornecida pelo proprietário da informação de proteger adequadamente esta informação.
5.8. Responsável pela informação: Gestor da área onde a informação é gerada. Define o nível de classificação da informação. (recebe o nome de proprietário dos ativos ou proprietário da informação na NBR ISO/IEC 27002:2005).
5.9. Usuário: pessoa que acessa ou utiliza de forma legítima e autorizada as informações.
5.10. Terceiros: pessoas que prestam serviço e podem possuir acesso às instalações e recursos de informação do Serviço Distrital da Barreirinha.
5.11. Incidente de segurança: evento não planejado que pode acarretar prejuízos a empresa ou mesmo violar as regras de segurança.
5.12. Áreas sensíveis: são áreas ou setores que concentram uma quantidade considerável de informações.

6. CONFORMIDADE

6.1. Ao usuário de informações não é dado o direito de desconhecimento da Política de Segurança da Informação, devendo seguir rigorosamente o disposto nas regras.
6.2. Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada, garantindo que todos a conheçam e a pratiquem.
6.3. A inobservância das políticas e normas de segurança sujeita o usuário a sanções internas e, nos casos cabíveis, às leis vigentes.
6.4 Verificações para assegurar o nível e elaborar projetos para melhoria dos índices de conformidade ou correções de não conformidade.

7. DEVERES E RESPONSABILIDADES

7.1. Dos Colaboradores

7.1.1 Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os equipamentos de informática disponibilizados para a realização do seu trabalho.
7.1.2 Cumprir as determinações desta Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis.
7.1.3 Utilizar recursos e sistemas de informações do Serviço Distrital da Barreirinha somente para finalidades profissionais.
7.1.4 Todas as informações que forem transitadas internamente e externamente devem ser feitas através de mecanismos corporativos (e-mail da serventia).
7.1.5 Comunicar por escrito ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

7.2 Do Delegatário e Ecarregado

7.2.1. Gerenciar o cumprimento desta Política, por parte de seus supervisionados.
7.2.2. Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

7.2.3. Impedir o acesso de funcionários demitidos aos ativos, utilizando- se dos mecanismos de desligamento do empregado.
7.2.4. Zelar, em nível físico e lógico, pelos ativos de informação e de processamento do Serviço Distrital da Barreirinha, relacionados com atuação.
7.2.5. Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações.
7.2.6. Documentar formalmente a concessão de privilégios a usuários de TI (Tecnologia da Informação), que acessos e permissões devem ter os colaboradores, sob sua supervisão, à informações e sistemas.
7.2.7. Comunicar formalmente a concessão de privilégios aos usuários de TI (Tecnologia da Informação), quais os colaboradores demitidos ou transferidos, para exclusão de permissões no cadastro dos usuários.

7.3 Dos Prestadores de Serviço

7.3.1. Devem estar previstas nos contratos, cláusulas que contemplem a responsabilidade dos funcionários e prestadores de serviços no cumprimento desta Política de Segurança da Informação, suas normas e procedimentos.

8. DIRETRIZES

8.1. Toda informação gerada pelos usuários, utilizando integralmente ou parcialmente recursos do Serviço Distrital da Barreirinha é de propriedade exclusiva do Serviço Distrital da Barreirinha.
8.2. O Serviço Distrital da Barreirinha, como custodiante de dados e informações de seus usuários, os considera sigilosos, logo, devem ser tratados assim pelos seus colaboradores.
8.3. No que se refere às informações em custódia do Serviço Distrital da Barreirinha, considera-se proibido tudo aquilo que não esteja previamente autorizado por esta política e demais documentos normativos.
8.4. Devem ser prevenidas, através de controles, todas as possibilidades de vazamento de informações do Serviço Distrital da Barreirinha.
8.5. A divulgação de informações classificadas do Serviço Distrital da Barreirinha, deverá ser feita por meio do Delegatário, ou encarregado de dados, segundo suas atribuições e com autorização do Delegatário.
8.6. Os colaboradores devem utilizar os recursos da serventia seguindo os princípios de segurança sem afetar ou causar prejuízo a outrem.
8.7. Eventual descumprimento desta Política de Segurança de Informação deve ser imediatamente comunicado ao Encarregado ou Delegatário.
8.8. Todas as espécies de pressões e chantagens devem ser denunciadas.
8.9. O Gerenciamento de Riscos deve identificar por tipo de exposição, avaliar quanto à probabilidade de incidência e quanto ao impacto, todos os riscos que possam comprometer a realização dos serviços do Serviço Distrital da Barreirinha.

8.10. Os sistemas de controles internos devem ser continuamente reavaliados e aprimorados, principalmente quanto ao risco de segurança das informações, com procedimentos apropriados nos processos de cada setor

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

8.11. Todos os processos internos devem estar mapeados e documentados. Além de serem revisados periodicamente visando elevar o nível de maturidade na sua segurança.
8.12. As informações devem ser classificadas quanto a confidencialidade e identificadas de forma a serem adequadamente armazenadas, copiadas, transmitidas, manuseadas, descartadas ou destruídas. Esta classificação deve estar coerente.
8.13. As medidas de proteção aos recursos devem ser aplicadas de forma compatível com o risco e com o valor da informação para os serviços do Serviço Distrital da Barreirinha.
8.14. Todos os ativos de informação devem ser identificados, classificados, permanentemente atualizados pelo Encarregado e Responsável pelo TI.
8.15. Deve haver um processo que visa conscientizar os usuários da necessidade da segurança das informações e aspectos previstos na Política de Segurança da Informação.
8.16. Os empregados devem estar devidamente capacitados quanto à correta e eficiente utilização dos recursos, de acordo com as normas em vigor.
8.17. A Gestão de Segurança da Informação do Serviço Distrital da Barreirinha deve ser feita por empregados da Entidade, devidamente capacitados para a função.
8.18. Um Plano de Continuidade do Negócio, cujo objetivo é manter em funcionamento os processos e serviços críticos, na ocorrência de desastres, atentados, falhas e intempéries, deve ser mantido atualizado, testado e documentado.
8.19. Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.
8.20. Os procedimentos de cópia de segurança (backup) e de recuperação (restore) devem ser documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações, seguindo entendimento do Provimento 74 do CNJ.
8.21. Na concessão de quaisquer acessos aos recursos, físicos ou lógicos, deve ser observado o princípio do menor privilégio, que consiste em conceder somente os acessos e recursos estritamente necessários ao desempenho das atividades autorizadas.
8.22. Os colaboradores devem ter acesso físico e lógico liberado, somente aos recursos e informações necessários e indispensáveis ao desempenho de suas atividades e em conformidade com os interesses do Serviço Distrital da Barreirinha.
8.23. As autorizações devem ser concedidas de acordo com as necessidades de desempenho das funções e considerando o princípio do menor privilégio.
8.24. Mecanismos de segurança baseados em sistemas de proteção de acesso devem ser utilizados para proteger as transações entre redes externas e a rede interna.
8.25. Os serviços de rede e acessos devem ser controlados.
8.26. As senhas, certificações digitais e outras formas de autenticação são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada.
8.27. O acesso às áreas sensíveis deve ser resguardado, por meio do uso de dispositivos de controle de acesso e utilização de câmeras de monitoração.
8.28. As câmeras de segurança devem gravar as imagens captadas para posterior análise do pessoal responsável ou através de solicitação formal, sem o uso de inteligência artificial de reconhecimento do titular.
8.29. As imagens devem ser armazenadas de forma protegida.
8.30. Devem ser guardados os registros de segurança (logs), de modo a auxiliar na identificação de desvios, falhas ou usos indevidos, além de serem periodicamente analisados para os propósitos de caráter corretivo, legal e de auditoria. O período de análise dever ser sempre o menor possível.

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

8.31. Os registros (informações, arquivos, documentos, imagens) devem ser protegidos e armazenados com segurança, o período de armazenamento é definido pelo responsável pelo TI, através de comunicação formal.
8.32. Os computadores, servidores, seus sistemas, switches e No-Breaks devem ser monitorados, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.
8.33. Os controles e administração de Servidores e Serviços que forem aplicados fora das dependências do Serviço Distrital da Barreirinha (Nuvem), devem ser feitos por profissionais devidamente responsabilizados contratualmente.
8.34. Os horários das máquinas devem estar sincronizados para permitir o rastreamento de eventos.
8.35. As mídias e informações serão eliminadas de forma segura.
8.36. Uma política de mesa e tela limpa deve ser implementada para reduzir o risco de acessos não autorizados ou danos a documentos/papeis, mídias e recursos de processamento de informações.
8.37. As cláusulas contratuais devem ser avaliadas criteriosamente para que haja definição clara dos papéis e responsabilidades entre as partes envolvidas, níveis de processamento necessário, segurança, monitoração e requisitos de contingência.
8.38. Acordos de confidencialidade devem ser firmados para garantir a confidencialidade das informações do Serviço Distrital da Barreirinha.
8.39 Aos colaboradores não é permitida a utilização do whatsapp pessoal para comunicação com usuários da serventia, assim como, o recebimento de documentos ou dados pessoais destes. Aos colaboradores é vedado o uso de celular pessoal quando estiverem em horário de trabalho, os aparelhos pessoais devem ser guardados nos locais apropriados.
8.40. O celular corporativo deve ser manuseado com a cautela devida e sua guarda é de responsabilidade do usuário/setor responsável, que deve mantê-lo em local seguro, fora do alcance de usuários de nossos serviços. O celular corporativo não deve ser retirado das dependências do cartório. Somente em situações excepcionais, mediante autorização da titular ou do substituto, pode ser levado aos locais em que são feitas atas notariais de constatação de fato.

9. BACKUPS

Os backups são executados diariamente e de acordo com o Provimento nº 74 do CNJ.

O banco de dados do sistema é replicado em tempo real para um servidor secundário na serventia e para nuvem segura da empresa desenvolvedora.

Os diretórios da rede do servidor principal são replicados a cada 30 (trinta) minutos para o servidor secundário na serventia.

Cópias de segurança do banco de dados, do acervo digital e dos diretórios de dados da rede dos dados são realizadas diariamente para 02(dois) HDD’s externos intercalados (mantida sempre uma unidade em local seguro, fora das dependências da serventia), para um storage local e nuvem segura remota.

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

Os horários definidos seguem o fluxo:

Objeto do backup	Horário	Destino
Banco de dados do sistema	11 Hrs	Diretório de dados na rede
Banco de dados do sistema	18 Hrs	Diretório de dados na rede
Diretório de dados da rede	19:00 Hrs	Storage
Diretório de dados na rede	18:30 Hrs	HDD externo
Diretório de dados da rede	20:00 Hrs	Nuvem segura remota

Diretivas adicionais de segurança incluem a realização de backup apenas em HDD's externos previamente registrados (BLKID);

Tanto os HDD's externos quanto o Storage são conectados, montados, apenas nos horários programados para o backup, desconectados ao final, impedindo a corrupção das informações salvas.

10. PROTEÇÕES

Antivírus

A proteção antivírus e anti sequestro adotada em todas as estações de trabalho é a premiada solução Bitdefender Gravityzone Advanced Security, com seu banco de dados atualizado diariamente com as últimas definições.

As verificações ocorrem em tempo real sem comprometer o desempenho das estações de trabalho.

Adicionalmente, políticas de segurança impedem a conexão, acesso e cópia de dados para pendrives, HDD's externos, celulares e etc.

Relatórios detalhados por estação de trabalho sobre infecções neutralizadas, dispositivos bloqueados são gerados e comunicados para tomada de ação,

Firewall e Proxy de rede

A rede do cartório está protegida pelo firewall PFSense, que impede acesso externo e violação da integridade das informações mantidas nos servidores e estações de trabalho da serventia.

Av. Anita Garibaldi, 1142 - Cabral CEP 80.540-400 Curitiba/PR Fone (41) 3077-3008
www.cartoriodabarreirinha.com.br - atendimento@cartoriodabarreirinha.com.br

Regras de acesso à internet são impostas aos colaboradores através de listas de sites bloqueados, definidos por categoria, no componente de proxy transparente (toda conexão à rede externa, transita pelo filtro do proxy).

Para supervisão, os históricos de acesso a sites e proteção a invasão são guardados pelo período de 03 (três) meses.

Licença e software

Todas as estações de trabalho possuem sistema operacional profissional devidamente licenciado para o meio corporativo e empresarial.

Atualizações de segurança são realizadas semanalmente.

Softwares de edição, planilhas e e-mail do pacote Microsoft Office, são licenciados anualmente.

As instalações de outros softwares e aplicações, mesmo as do tipo gratuitas, requerem senha de usuário com privilégios administrativos, reservado apenas para colaboradores pré definidos.

11. VALIDADE

A data deste documento inicia-se após a aprovação e divulgação, considerando 12 (doze) meses de validade ou quando surgir tecnologia relevante aos processos em andamento.

12. APROVAÇÃO

Esta Política foi aprovada pelo Delegatário “Giovana Manfron da Fonseca Maniglia”, Encarregado Elton Jorge Targa e Responsável pelo TI Carlos, em 16/01/2025.