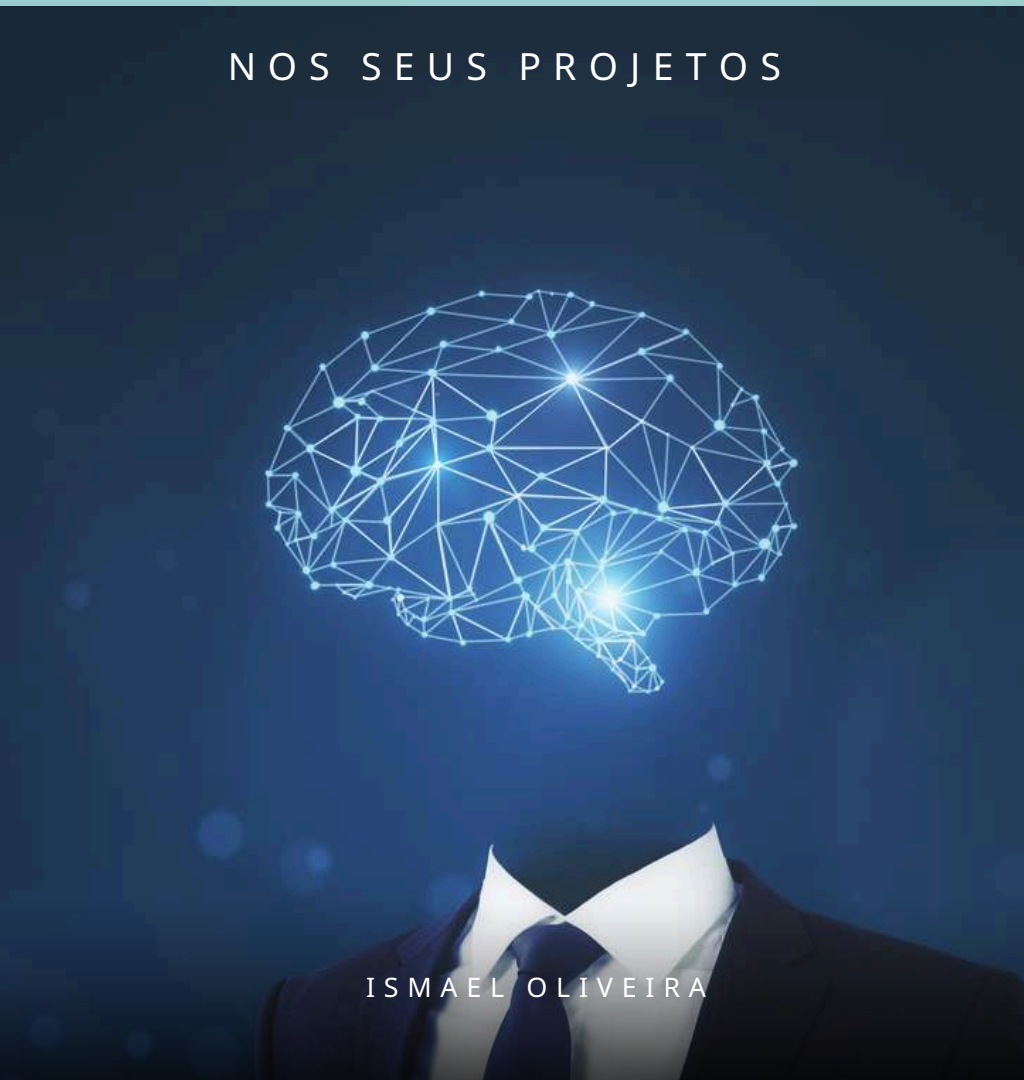
SUPORTE

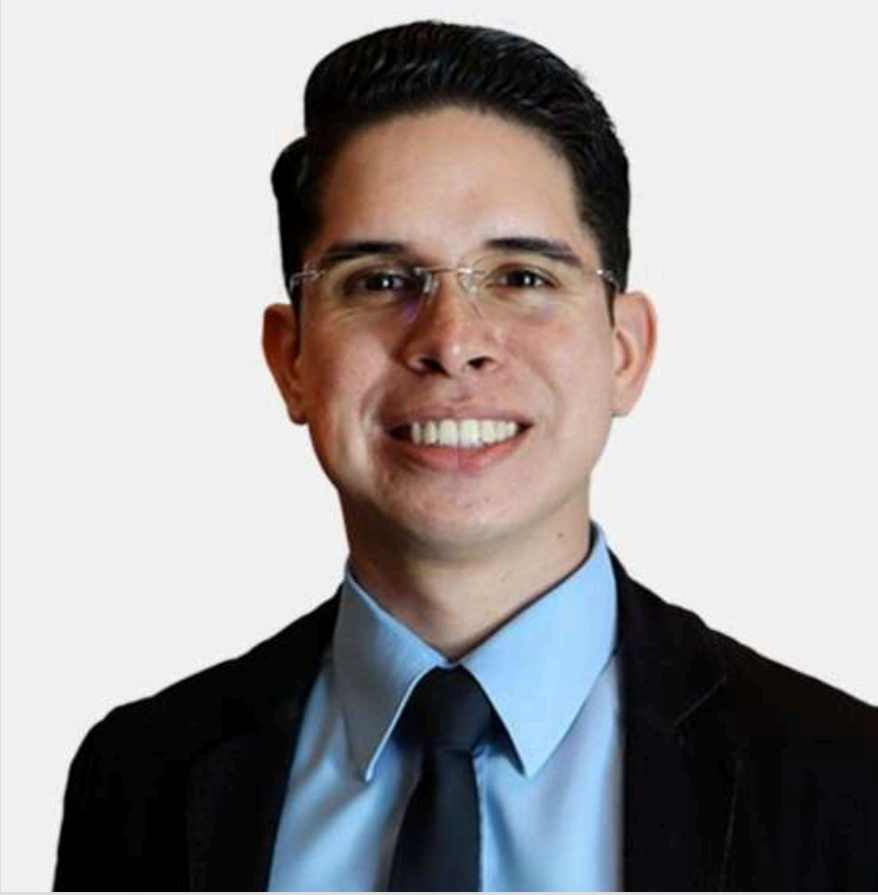
TÉCNICO-JURÍDICO

SUPORTE DE INFORMÁTICA, LGPD E SEGURANÇA DA INFORMAÇÃO

NOS SEUS PROJETOS



ISMAEL OLIVEIRA



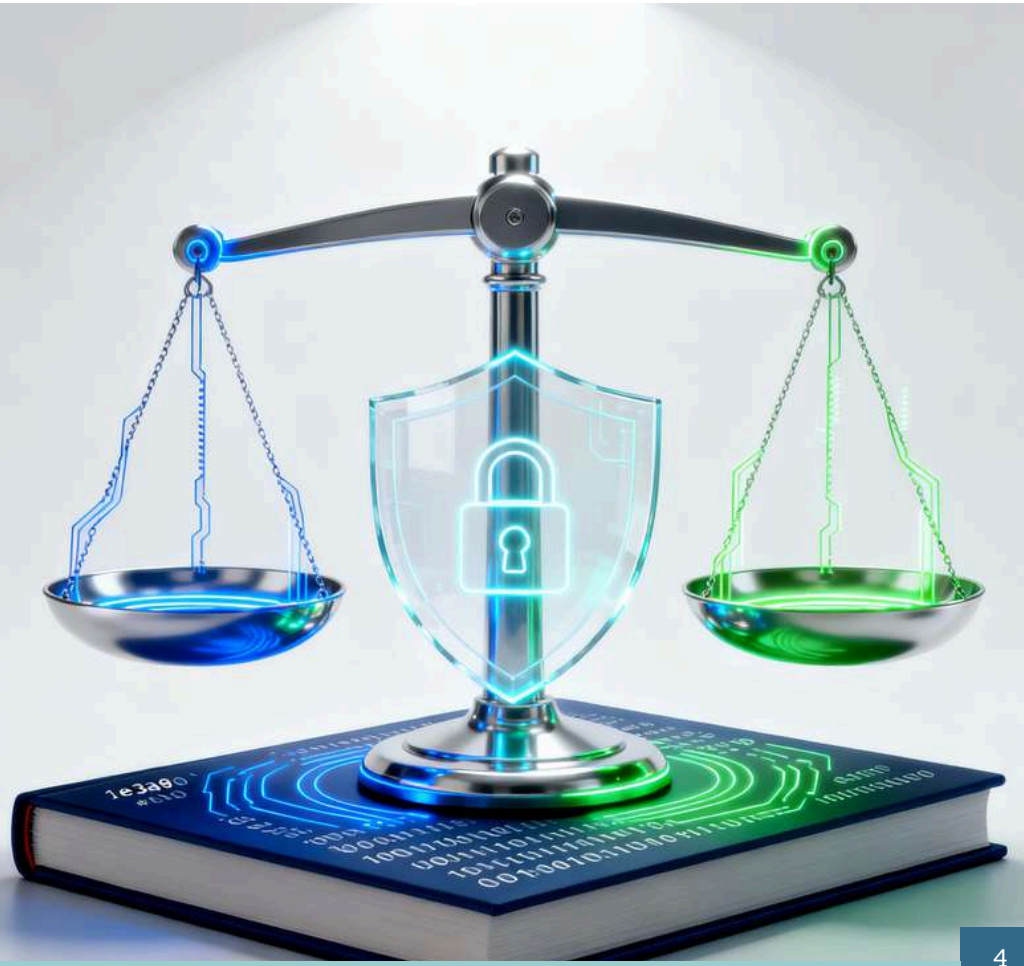
ISMAEL OLIVEIRA

Ismael Oliveira é um profissional com experiência especializada na interseção entre Tecnologia da Informação e o Setor Jurídico. Atuando como Suporte Técnico na R. Amaral Advogados, ele é essencial para garantir a eficiência operacional, a continuidade dos serviços de TI e a segurança no ambiente de advocacia. Com forte domínio em Suporte Técnico e Redes de Computadores, Ismael consolidou sua experiência prática para oferecer soluções rápidas e eficazes, sendo um recurso valioso para a gestão tecnológica no contexto jurídico.

ÍNDICE

Capítulo I – Introdução

O avanço da digitalização no meio jurídico exige uma estrutura de suporte técnico altamente capacitada e consciente das normas legais que regem o tratamento da informação. Este eBook foi desenvolvido com foco técnico-jurídico, abordando as práticas essenciais de suporte de informática em escritórios de advocacia, departamentos jurídicos e órgãos públicos, com ênfase em segurança da informação, LGPD (Lei Geral de Proteção de Dados) e governança digital.



Capítulo II – O Papel do Suporte Técnico-Jurídico

O suporte técnico-jurídico não se limita à manutenção de sistemas. Ele é responsável por garantir a confidencialidade, integridade e disponibilidade das informações jurídicas, além de apoiar o cumprimento das obrigações legais de proteção de dados.

As **principais** atribuições incluem:

- Garantir o acesso seguro às plataformas judiciais e administrativas;
- Monitorar e mitigar riscos cibernéticos;
- Orientar usuários sobre conformidade com a LGPD;
- Assegurar a continuidade operacional de sistemas jurídicos;
- Integrar TI e departamento jurídico para decisões estratégicas.

Capítulo III –
Acesso e Gestão das Plataformas Jurídicas

PJe (Processo Judicial Eletrônico)

O suporte deve assegurar que os advogados e servidores utilizem o PJe em conformidade com as normas de segurança. É fundamental o uso de certificados digitais válidos, autenticação segura e manutenção do módulo PJeOffice.

Boas práticas:

- Habilitar autenticação de múltiplos fatores (quando disponível);
- Garantir atualização do Java e do navegador;
- Realizar limpezas regulares de cache e cookies para evitar falhas de assinatura.

eProc, e-SAJ e Projudi

Cada sistema possui requisitos técnicos específicos, mas todos demandam atenção à segurança e à integridade das assinaturas digitais. O suporte deve manter documentação atualizada e registrar incidentes recorrentes para aprimorar o atendimento.

e-CAC, gov.br e Serpro

Essas plataformas concentram grande volume de dados sensíveis. O acesso deve ser protegido por autenticação forte e uso exclusivo de máquinas seguras.
É recomendável implementar políticas internas que impeçam o compartilhamento indevido de credenciais e definir logs de auditoria para cada acesso realizado.

#1e3a88 e-CAC gov.Br. Serpro

Capítulo IV –
Certificados Digitais e Assinaturas Eletrônicas

O suporte técnico deve compreender os tipos e aplicações de certificados digitais (A1, A3, e-CPF, e-CNPJ).

Deve também garantir que o processo de instalação, renovação e uso siga os princípios da LGPD: finalidade, necessidade e segurança.

Práticas recomendadas:

- Utilizar senhas fortes nos tokens A3;
- Manter os certificados sob guarda do titular;
- Evitar cópias indevidas de certificados A1;
- Registrar toda instalação e renovação em sistema interno.

Capítulo V – Microsoft 365: Administração e Governança Tecnológica

Portal Microsoft 365

O suporte deve assegurar o uso corporativo seguro, promovendo boas práticas de armazenamento no OneDrive e compartilhamento restrito de dados jurídicos no SharePoint.

Admin Center

Como administrador, é essencial gerenciar usuários, políticas e dispositivos de forma integrada com a LGPD e a política de segurança institucional.
Funções essenciais incluem:

- Implementar autenticação multifator (MFA);
- Configurar políticas de retenção e exclusão de dados;
- Monitorar logs e alertas de segurança;
- Administrar permissões por função (RBAC – Role-Based Access Control).

Ferramentas Colaborativas

- Outlook: aplicar políticas de criptografia e assinatura digital de e-mails.
- Teams: configurar canais privados para comunicações sensíveis.
- OneDrive/SharePoint: definir políticas de acesso granular e auditoria de downloads.

Licenciamento, Políticas e Segurança

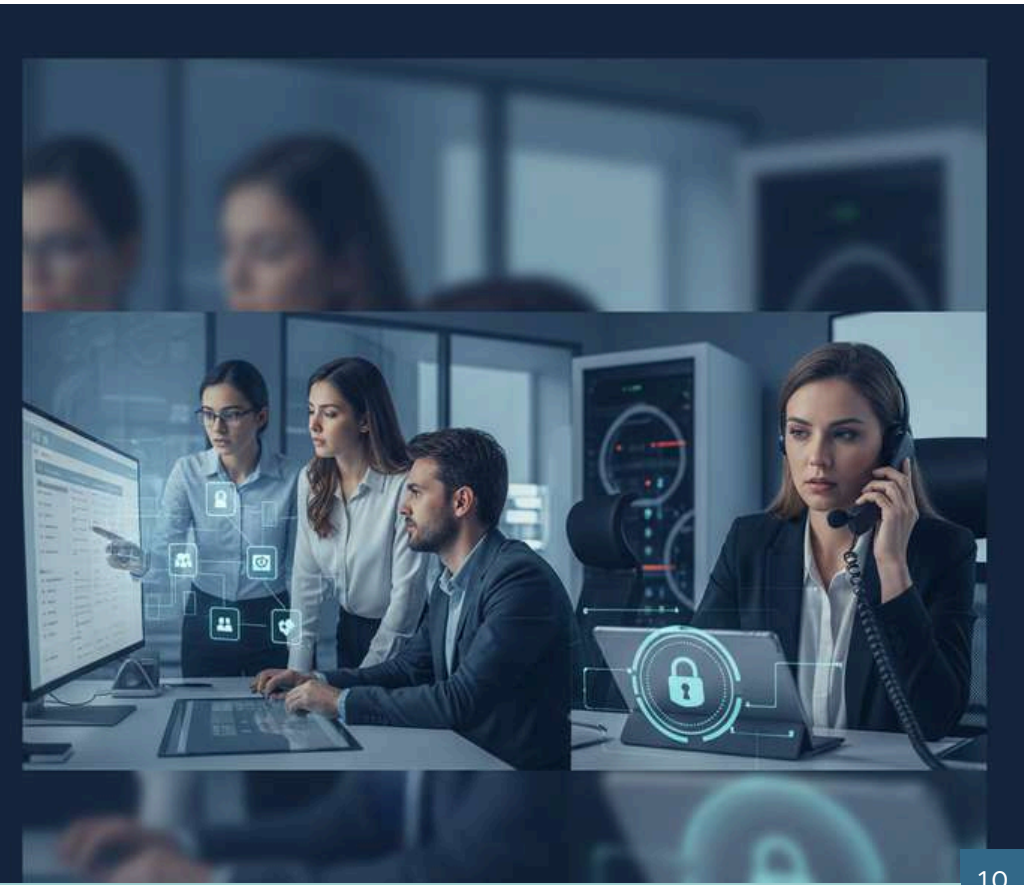
- O controle de licenças deve seguir critérios de conformidade e transparência. Além disso, o suporte deve integrar o Microsoft Defender for Cloud Apps e o Compliance Manager para garantir o cumprimento dos requisitos da LGPD.

Capítulo VI –
Atendimento ao Usuário e Gestão de Chamados

Um suporte eficiente requer processos documentados. Cada solicitação deve conter descrição, prioridade, responsável e prazo de resolução.

A equipe deve adotar metodologia ITIL (Information Technology Infrastructure Library), assegurando rastreabilidade e histórico de incidentes.

Além disso, os chamados que envolvam dados pessoais devem ser tratados sob protocolo sigiloso, respeitando o princípio da confidencialidade jurídica.



Capítulo VII –
Manutenção de Hardware e Infraestrutura Crítica

A confiabilidade do ambiente jurídico depende de equipamentos em perfeito estado.

As práticas recomendadas incluem:

- Verificação de integridade de discos e memórias;
- Testes de redundância elétrica (no-breaks e geradores);
- Políticas de descarte seguro de mídias e discos rígidos;
- Aplicação de patches de segurança em BIOS e firmware.

Capítulo VIII –
LGPD e Conformidade Digital no Setor Jurídico

A LGPD estabelece dez princípios que devem orientar o tratamento de dados. Os mais relevantes para o suporte técnico-jurídico são:

- Segurança: proteção contra acessos não autorizados;
- Prevenção: adoção de medidas antecipadas contra incidentes;
- Responsabilização: documentação de todas as ações técnicas;
- Adequação: tratamento de dados compatível com a finalidade jurídica.

Funções do Controlador, Operador e DPO

- Controlador: define as finalidades do tratamento (geralmente o órgão ou escritório).
- Operador: executa o tratamento sob instrução do controlador (setor de TI).
- DPO (Encarregado de Dados): atua como elo entre a instituição e a ANPD (Autoridade Nacional de Proteção de Dados).

Boas Práticas de Proteção de Dados

- Implementar backup criptografado;
- Utilizar VPN em acessos remotos;
- Evitar armazenamento local de petições e documentos sensíveis;
- Aplicar controle de versão em sistemas jurídicos.

Gestão de Incidentes e Vazamento de Dados

O suporte deve possuir um **plano de resposta a incidentes** que inclua:

- Identificação e contenção imediata;
- Notificação interna e ao DPO;
- Registro detalhado do incidente;
- Adoção de medidas corretivas e preventivas.

LGPD Principles

Security

Prevention

Accountability

Adequacac

Roles & Responsibilities

Best Practices & Incident Management

up

VPN Remote Access

No Local Storage

Identifcacion

Au

Notification

Detailed Record

Corre

Capítulo IX –
Segurança da Informação: Políticas, Controles e Monitoramento

Classificação da Informação

Todo documento jurídico deve ser classificado conforme seu nível de confidencialidade: público, restrito ou sigiloso. O suporte técnico deve configurar permissões adequadas em cada nível.

Controles de Acesso e Autenticação

Adotar autenticação multifator, senhas complexas e controle de dispositivos confiáveis. O acesso a sistemas jurídicos deve ser limitado a usuários previamente autorizados.

Criptografia e Proteção de Dados em Trânsito

Todo tráfego de dados deve ocorrer via HTTPS/TLS e, preferencialmente, com uso de VPN. Documentos sensíveis devem ser armazenados com criptografia AES-256.

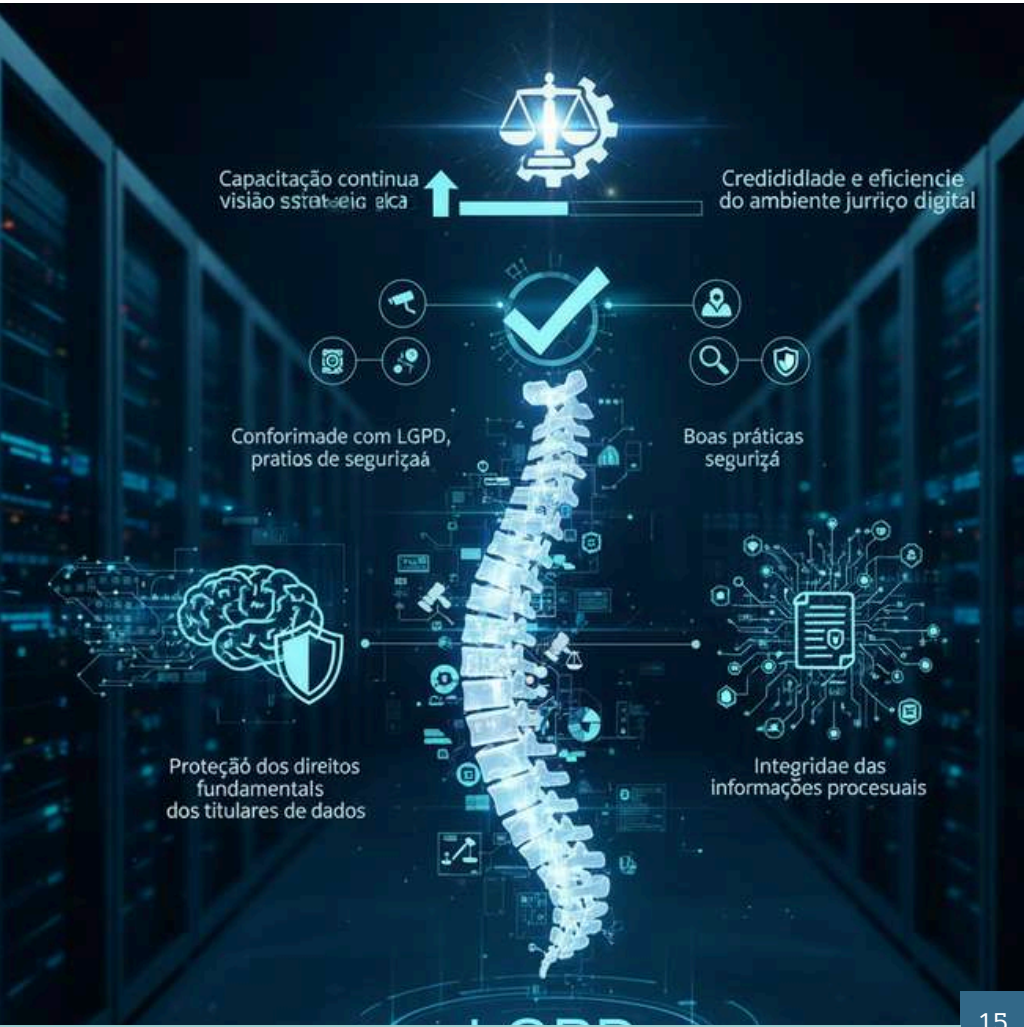
Auditorias e Conformidade

Realizar auditorias periódicas em logs de acesso, políticas de backup e permissões de usuários. Relatórios de conformidade devem ser enviados à diretoria jurídica e ao DPO.

Conclusão

O suporte técnico-jurídico é a **espinha dorsal da governança** digital no setor jurídico. Seu papel vai além da resolução de problemas técnicos; envolve a **proteção dos direitos fundamentais** dos titulares de dados, a integridade das informações processuais e a conformidade com a LGPD.

Com capacitação contínua, boas práticas de segurança e visão estratégica, **o suporte** torna-se parte essencial da credibilidade e eficiência do ambiente jurídico digital.



(85) 9.9826.1414

nexusinnova.com.br

contato@nexusinnova.com.br