POLÍTICA DE USO RESPONSÁVEL DOS RECURSOS DE TI E SEGURANÇA DE DOCUMENTOS SIGILOSOS

LIBERAÇÃO DO DOCUMENTO

	Emissão: 26/03/2025	Validade: 26/03/2027
Revisado: Rafael Victor Tavares Pinheiro Assinatura:	Data:	Rubrica:
Aprovado: Marcos Leal Assinatura:	Data:	Rubrica:
Implementado: Ricardo Tiago Sá Assinatura:	Data:	Rubrica:

1. OBJETIVO

Estabelecer as diretrizes e responsabilidades relacionadas ao uso responsável dos recursos de TI, à segurança da informação e à proteção de documentos sigilosos. Abrange todos os equipamentos corporativos, práticas de segurança e o comportamento esperado de colaboradores, prestadores de serviços, contratados e parceiros que interagem com nossos sistemas e dados. O compromisso é garantir a integridade, confidencialidade e disponibilidade das informações, alinhando nossas práticas às normas internacionais de segurança e privacidade, como as séries ISO 27001, 27002, 27003, 27004, 27005, 27007 e a ISO/IEC 27701, que estabelece um SGPI. Além disso, estamos em conformidade com legislações como a LGPD no Brasil, o GDPR da União Europeia, o Código Civil Brasileiro, o Marco Civil da Internet e as Leis de Proteção à Propriedade Intelectual - Leis nº 9.610/98 e 9.609/98. Esta política reflete nosso empenho em promover uma cultura de segurança e responsabilidade no uso de recursos de TI.

2. RESPONSABILIDADES

- **Alta administração**: Aprovar políticas, alocar recursos e fomentar a cultura de segurança;
- **Gestor**: Informar suas equipes, implementar diretrizes e reportar incidentes;
- **Equipe de TI e Segurança:** Implantar medidas técnicas, monitorar sistemas e oferecer treinamentos regulares (ISO 27001, Anexo A.7.2.2);
- **Colaboradores**: Seguir as políticas, proteger dados e notificar incidentes imediatamente;
- **Contratados e parceiros**: Manter a confidencialidade e aderir às regras de segurança e privacidade da GreyLogix.

3. DOCUMENTOS RELACIONADOS

Referências normativas e legais estão listadas no final da política, em “Referências”.

4. GLOSSÁRIO

BYOD - Bring Your Own Device: Traga seu próprio dispositivo.

Compliance: Programa de implementação de códigos de ética ou de conduta internos.

GDPR: Regulamento Geral sobre a Proteção de Dados.

Helpdesk: Sistema que fornece suporte técnico e assistência aos usuários para resolver problemas, responder perguntas e fornecer informações.

LGPD: Lei Geral de Proteção de Dados.

SGPI: Sistema de Gestão de Privacidade da Informação.

TI - Tecnologia da Informação: Setor responsável por hardware, software, dados, rede de comunicação e serviços.

5. ÂMBITO

Esta política aplica-se a todos os indivíduos e entidades que utilizam os recursos de TI da GreyLogix, incluindo:

- **Colaboradores:** Em regime presencial, remoto ou híbrido, independentemente de sua localização;
- **Prestadores de serviços, contratados e parceiros:** Ao acessar sistemas, redes ou dados da empresa, seja em escritórios, instalações de clientes ou ambientes externos;
- **Dispositivos abrangidos:** Equipamentos corporativos, dispositivos pessoais (no contexto *BYOD*) e dispositivos sem fio ou portáteis, estejam eles no Brasil ou no exterior.

E assim assegurar que todos os envolvidos sigam padrões consistentes de segurança e privacidade, independentemente do contexto ou tipo de dispositivo utilizado.

6. CONFORMIDADE LEGAL - LGPD e GDPR

A GreyLogix exige o cumprimento rigoroso das leis de proteção de dados aplicáveis, com destaque para a LGPD e o GDPR, que orientam o tratamento de dados pessoais. As principais diretrizes incluem:

- **Consentimento**: Sempre que necessário, o tratamento de dados pessoais deve ser precedido de consentimento explícito e informado dos titulares, conforme Artigo 9 da LGPD e Artigo 13 do GDPR;
- **Direitos dos titulares**: Deve ser garantido o respeito aos direitos de acesso, retificação, exclusão, portabilidade e oposição ao processamento, conforme Artigos 17-22 da LGPD e Artigos 12-23 do GDPR;
- **Transferência internacional**: Qualquer envio de dados pessoais entre países deve atender aos requisitos legais, como os Artigos 33-36 da LGPD e Artigos 44-50 do GDPR, com medidas de segurança adicionais previstas na ISO/IEC 27701;
- **Privacidade por padrão**: Adotar práticas que priorizam a proteção de dados desde a concepção dos processos, alinhadas à ISO/IEC 27701 e ao Artigo 5 do GDPR.

Todos os usuários dos recursos de TI devem agir de forma proativa para assegurar essa conformidade.

7. USO DE EQUIPAMENTOS CORPORATIVOS

Os equipamentos fornecidos pela GreyLogix são ferramentas essenciais para desempenhar as atividades profissionais e os usuários devem seguir regras específicas de uso:

- **Propriedade e devolução**: Todos os dispositivos cedidos (computadores, tablets, smartphones, etc) são de propriedade exclusiva da GreyLogix e devem ser utilizados unicamente para fins profissionais durante a vigência do contrato. Ao término da relação contratual, os equipamentos devem ser devolvidos em perfeitas condições, considerando o desgaste natural, sob pena de responsabilização civil por danos ou perdas, conforme o Código Civil Brasileiro;

- **Logística de envio**: A GreyLogix deve cobrir os custos de envio ao endereço informado pelo colaborador, ou em caso de mudança de endereço solicitada pela organização. Em caso de mudança subsequente de endereço por necessidade do próprio colaborador, seja nacional ou internacional, implicam que os custos logísticos passam ao colaborador, que também deve assumir a responsabilidade por eventuais danos durante o transporte; da mesma forma deve ocorrer a devolução do equipamento em finalização de contrato.
- **Manutenção e reparos**: Danos causados por negligência, mau uso ou transporte não autorizado devem ser custeados pelo colaborador, incluindo reparos ou substituição, conforme ISO 27001, Anexo A.8.2.3;
- **Equipamentos fora do país**: Em casos de manutenção ou upgrades necessários no exterior, o colaborador deve utilizar dispositivos próprios temporariamente até a GreyLogix providenciar uma solução, garantindo a continuidade das operações sem comprometer a segurança.

8. SEGURANÇA E USO ADEQUADO DOS EQUIPAMENTOS

A segurança dos equipamentos corporativos é uma responsabilidade compartilhada:

- **Proteção física e lógica**: Os usuários devem adotar medidas para evitar acessos não autorizados, perda ou roubo, como o uso de senhas fortes e bloqueio imediato ao se ausentar (ISO 27001, Anexo A.9.2);
- **Proteção de dados**: Dados armazenados nos dispositivos devem ser protegidos contra vazamentos ou uso indevido, em conformidade com a LGPD (Artigos 46-49) e o GDPR (Artigo 32), utilizando criptografia e outras tecnologias recomendadas pela ISO/IEC 27701;
- **Monitoramento e auditoria**: A GreyLogix reserva-se o direito de monitorar o uso dos equipamentos e realizar auditorias periódicas para assegurar a conformidade com esta política (ISO 27001, Anexo A.13.1.1);
- **Responsabilidade por danos**: Negligência ou violação das políticas que resultar em danos, extravio ou comprometimento dos equipamentos, e implicar em custos de reparo ou substituição, podem ser cobrados ao colaborador, além de possíveis sanções disciplinares.

9. *BRING YOUR OWN DEVICE BYOD* - TRAGA SEU PRÓPRIO DISPOSITIVO

A GreyLogix permite o uso de dispositivos pessoais e dispositivos sem fio/portáteis, corporativos ou não, para acessar sistemas e dados da empresa, desde que sejam cumpridos requisitos rigorosos de segurança:

- **Requisitos de segurança para dispositivos sem fio e portáteis**:
    - Todos os dispositivos (smartphones, tablets, laptops, etc) devem ter sistemas operacionais atualizados, antivírus ativo e firewalls configurados;
    - Conexões Wi-Fi devem utilizar criptografia WPA3 ou superior, evitando redes públicas não seguras;
    - Dados corporativos acessados ou armazenados nesses dispositivos devem ser criptografados e protegidos por autenticação multifator (ISO/IEC 27701);
    - Dispositivos não corporativos devem ser registrados junto à equipe de TI e submetidos a verificações regulares de conformidade;

- **Uso adequado**: Parceiros e colaboradores que utilizam dispositivos próprios devem seguir as mesmas políticas aplicáveis aos equipamentos corporativos, incluindo proteção contra malware e conformidade com LGPD e GDPR;
- **Responsabilidade**: Qualquer violação das diretrizes, como uso indevido ou falhas de segurança em dispositivos *BYOD*, pode levar à revogação de acesso, sanções contratuais ou responsabilização por perdas, conforme ISO 27002, Seção 15.1.

10. POLÍTICA DE MESA E TELA LIMPA

Para proteger informações sigilosas, adotamos as seguintes práticas:

- **Mesa limpa**:
  - Documentos confidenciais em papel devem ser armazenados em gavetas trancadas ou armários ao final do expediente ou durante ausências prolongadas;
  - Senhas, logins ou dados sensíveis não devem ser anotados em locais visíveis;
  - Dispositivos de armazenamento removíveis, pertencentes à empresa, como: *pendrives* e HDs externos; devem ser guardados em segurança quando não utilizados;
  - Materiais impressos obsoletos devem ser destruídos em fragmentadoras adequadas (ISO 27001, Anexo A.8.3.3);
- **Tela limpa**:
  - Computadores e dispositivos devem ser bloqueados manualmente, utilizando os atalhos Ctrl+Alt+Del ou Windows+L, ao se afastar da estação de trabalho;
  - Configuração de bloqueio automático após 5 minutos de inatividade é obrigatória;
  - Sistemas com dados sensíveis devem ser “deslogados” ao final do uso;
  - Informações confidenciais não devem ser exibidas em locais acessíveis a pessoas não autorizadas.

11. RESPONSABILIZAÇÃO

- **Monitoramento e auditoria**: Auditorias e análise de logs podem ser realizadas para verificar a conformidade (ISO 27002, Seção 18.1);
- **Relatórios**: Incidentes devem ser comunicados à equipe de TI em até 24 horas através do *helpdesk*, disponível na intranet, com relatórios periódicos à alta direção contendo detalhes do incidente e plano de ação adotado.
- **Consequências**: Violações podem resultar em advertências, suspensão, demissão ou ações legais, dependendo da gravidade.

12. SANÇÕES

O descumprimento desta política sujeita o infrator a sanções disciplinares como: advertência, suspensão ou desligamento e, em casos de violação de dados, a penalidades previstas na LGPD e GDPR, além de responsabilização civil ou criminal conforme o Código Civil e o Marco Civil da Internet.

13. COMPLIANCE COM REGULAMENTAÇÕES

Esta política deve estar alinhada às seguintes normas e legislações:

- ISO 27001 e séries relacionadas (27002, 27003, 27004, 27005, 27007: Boas práticas para gestão da segurança da informação);
- ISO/IEC 27701: Sistema de Gestão de Privacidade da Informação, com controles para proteção de dados pessoais;
- LGPD: Conformidade com o tratamento de dados pessoais no Brasil;
- GDPR: Padrões europeus de proteção de dados;
- Código Civil Brasileiro e Marco Civil da Internet: Responsabilidade civil e proteção online;
- Lei nº 9.610/98 (Direitos Autorais) e Lei nº 9.609/98 (Proteção de Software): Proíbem o uso de softwares piratas ou não licenciados, com regras específicas:
    - Proibição de softwares não licenciados: É vedada a instalação ou uso de programas sem licença em qualquer dispositivo conectado aos sistemas da GreyLogix;
    - Autorização de instalação: Somente a equipe de TI pode instalar softwares licenciados e aprovados;
    - Respeito a licenças: Usuários devem seguir os termos de uso das licenças, evitando cópias ou distribuições ilegais;
    - Sanções por violação: Uso indevido pode levar a ações disciplinares e responsabilização legal.

14. APROVAÇÃO E VIGÊNCIA

Aprovada pela alta administração, esta política entra em vigor na data de publicação e será revisada anualmente ou conforme necessário, garantindo sua atualização frente às normas aplicáveis.

15. REFERÊNCIAS

ISO 27001: Anexo A.8.1 - Responsabilidades de ativos, A.8.1.3 - Uso aceitável de ativos.
ISO 27001: Anexo A.11.2.6 - Controle de acesso a áreas seguras.
ISO 27001: Anexo A.11.2.4 - Proteção contra ameaças externas e ambientais.
ISO 27001: Anexo A.12.1.3 - Planejamento e aceitação do sistema.
ISO 27001: Anexo A.9.2.3 - Gestão de senhas de usuário.

ISO 27001: Anexo A.12.4 - Registro e monitoramento de eventos.

ISO 27001: Anexo A.18.2.2 - Revisões de conformidade com a segurança da informação.

ISO 27001: Anexo A.13.2.3 - Mensagens eletrônicas.

ISO 27001: Anexo A.6.2 - Dispositivos móveis e teletrabalho.

ISO 27002: Seção 12.6.2 - Controles contra software malicioso.

ISO 27001: Anexo A.13.2.1 - Política e procedimentos para a transferência de informações.

ISO 27001: Anexo A.11.2.9 - Política de mesa limpa e tela limpa.

ISO 27001: Anexo A.18.2.3 - Revisão independente de segurança da informação.

ISO 27001: Anexo A.7.2.2 - Educação, treinamento e conscientização em segurança da informação.

ISO 27001: Anexo A.18.2.1 - Conformidade com os requisitos legais e contratuais.

ISO 27001: Anexo A.9.4.2 - Controle de acesso do usuário.

ISO 27001: Anexo A.11.2.8 - Futuro desenvolvimento e procedimentos de instalação.

ISO 27001: Anexo A.11.2.7 - Descarte de equipamentos.

ISO 27001: Anexo A.8.3 - Descarte de ativos.

ISO 27001: Anexo A.9.4.3 - Uso de informações de autenticação.

ISO 27001: Anexo A.6.1.1 - Responsabilidades e papéis na segurança da informação.

ISO 27001: Anexo A.11.2 - Segurança em áreas e equipamentos.

ISO 27001: Anexo A.5.1.1 - Política para segurança da informação.

ISO 27001: Anexo A.16.1.2 - Relato de eventos de segurança da informação.

ISO 27001: Anexo A.12 - Operações de segurança.

ISO 27001: Anexo A.8.2.3 - Tratamento de ativos.

ISO 27001: Anexo A.15 - Relações com fornecedores.

ISO 27001: Anexo A.15.1.1 - Política de segurança da informação para fornecedores.

ISO 27001: Anexo A.18.2 - Revisão de conformidade.

ISO 27001: Anexo A.12.4.1 - Registros de eventos.

ISO 27001: Anexo A.7.2.3 - Consequências da falta de conformidade.

ISO 27701: Sistema de Gestão de Privacidade da Informação, com controles para proteção de dados pessoais.

LGPD: Artigo 38 - Responsabilidade do controlador e do operador.

LGPD: Artigo 45 - Responsabilidade.

LGPD: Artigo 46 - Segurança e sigilo.

LGPD: Artigo 6 - Princípios.

LGPD: Artigo 7 - Bases legais.

LGPD: Artigo 8 - Consentimento.

LGPD: Artigos 17 a 22 - Direitos dos titulares.

LGPD: Artigos 33 a 36 - Transferência internacional de dados.

LGPD: Artigos 52 a 54 - Sanções administrativas.

GDPR: Artigo 24 - Responsabilidade do responsável pelo tratamento.

GDPR: Artigo 83 - Condições gerais para imposição de coimas administrativas.

GDPR: Artigo 28 - Encarregado do tratamento.

GDPR: Artigo 82 - Direito a indemnização e responsabilidade.

GDPR: Artigo 6 - Licitude do tratamento.

GDPR: Artigo 5 - Princípios relativos ao tratamento de dados pessoais.

GDPR: Artigo 6 - Licitude do tratamento, Artigo 30 - Registos das atividades de tratamento.

GDPR: Artigo 7 - Condições para o consentimento.

GDPR: Artigos 15 a 20 - Direitos do titular dos dados.

GDPR: Artigos 44 a 50 - Transferências de dados pessoais para países terceiros ou organizações internacionais.

GDPR: Artigo 32 - Segurança do tratamento.

GDPR: Artigo 13 - Informações a facultar quando os dados pessoais são recolhidos junto do titular dos dados.

Código Civil Brasileiro: Artigos 927 - Responsabilidade por ato ilícito, 944 - Indenização, 1.196 e 1.198.

Lei de Direitos Autorais - Lei n. 9.610/98

Art. 7º, inciso XII: Define os programas de computador como obras intelectuais protegidas pela lei.

Art. 29: Estabelece que a utilização de obras protegidas - incluindo programas de computador depende de autorização expressa do titular dos direitos.

Art. 102: Protege o software contra qualquer alteração, reprodução ou modificação sem o consentimento do autor.

Art. 24: Define o direito moral do autor, que protege a integridade da obra.

Art. 101: Estabelece que a violação dos direitos do autor sobre programas de computador é sujeita a penalidades civis e criminais.

Art. 104: Especifica que o usuário deve respeitar os limites e as condições de uso definidas pelo autor ou licenciante.

Art. 87: Protege a integridade do software, proibindo a modificação, adaptação ou alteração sem autorização.

Lei de Proteção à Propriedade Intelectual de Programa de Computador - Lei n. 9.609/98:

Art. 9º: Estabelece que a reprodução, comercialização ou distribuição de programas de computador sem autorização do titular dos direitos autorais constitui crime, com penas de detenção e multa.

Art. 2º: Determina que os programas de computador são protegidos como obras literárias, abrangendo sua proteção por direitos autorais.

Art. 4º: Define que o usuário final só pode utilizar o programa de computador conforme os termos do contrato de licença, sendo vedado o uso sem a devida autorização.

Art. 6º: Determina que o titular dos direitos pode licenciar o uso do software em termos e condições específicos, e que o descumprimento dessas condições constitui violação.

Art. 6º, §1º: Proíbe a alteração, modificação ou a realização de engenharia reversa de programas de computador, exceto nas situações expressamente permitidas pelo contrato de licença ou pela lei.

Art. 9º, inciso I: Define como crime a reprodução ou modificação de programas de computador sem autorização, sujeitando o infrator às penalidades previstas.

Art. 7º: Proíbe a reprodução, distribuição ou utilização de programas de computador para fins comerciais ou não comerciais sem a devida autorização, assegurando o direito exclusivo de cópia ao titular dos direitos.

Art. 8º: Estabelece que o uso irregular de software que não atenda às condições da licença contratual é considerado infração dos direitos autorais.

HISTÓRICO DE REVISÕES

Revisão:	Executado por:	Descrição:
01	Rafael Victor Tavares Pinheiro	Adequações em todos os parágrafos.
00	Rafael Victor Tavares Pinheiro	Emissão inicial.

Ciente:

_____

Nome (letra de forma)

_____

Assinatura

_____/_____/_____

Data