

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Proteção das informações da firma e das informações sob sua custódia.

AUDIMEC AUDITORES INDEPENDENTES

Versão 1.0
Aprovado pelos sócios da AUDIMEC

AUDIMEC
AUDITORES INDEPENDENTES

Política de Segurança da Informação

Esta Política estabelece os requisitos de proteção das informações e dos recursos utilizados pela AUDIMEC. Aplica-se ao ambiente físico e digital, aos trabalhos de auditoria e aos demais serviços, independentemente do local de execução.

01 Objetivo e aplicação 3

02 Governança e responsabilidades 4

03 Classificação e ciclo de vida 5

04 Identidades e controle de acesso 6

05 Equipamentos e trabalho remoto 7

06 Compartilhamento e serviços digitais 8

07 Privacidade e documentação de auditoria 9

08 Backups e continuidade 10

09 Gestão de riscos e incidentes 11

10 Aplicação revisão e ciência 12

Aprovação institucional

Esta é a versão 1.0 aprovada pelos sócios da AUDIMEC. O registro formal da aprovação, a data de aplicação e as designações de responsáveis devem ser mantidos pela administração. Os contatos operacionais devem ser divulgados e atualizados nos meios institucionais.

Objetivo e aplicação

1.1 Objetivo

Proteger a confidencialidade, a integridade e a disponibilidade das informações: restringir o acesso a pessoas autorizadas, preservar exatidão e rastreabilidade e assegurar acesso adequado quando necessário. A Política também orienta a prevenção de incidentes, a continuidade das atividades e o cumprimento das obrigações legais, profissionais e contratuais.

1.2 Abrangência

São abrangidos sócios, empregados, estagiários, prestadores, fornecedores e parceiros com acesso às informações ou aos ambientes da firma. As regras alcançam documentos impressos, papéis de trabalho, relatórios, dados pessoais, comunicações, sistemas, equipamentos, serviços em nuvem e mídias. Terceiros devem assumir compromissos compatíveis com o acesso concedido.

1.3 Relação com outros requisitos

A Política deve ser aplicada em conjunto com o Código de Ética e Compliance, as normas profissionais e os contratos. Procedimentos complementares devem detalhar acessos, classificação, backups, retenção e incidentes. Sua aprovação não comprova, por si só, que todos os controles estejam implementados. Nenhuma exceção interna autoriza violar a legislação ou obrigações profissionais.

1.4 Sigilo e titularidade

O acesso depende de compromisso de confidencialidade, por termo ou cláusula contratual. Informações de clientes permanecem sujeitas aos direitos e obrigações pertinentes; sua custódia não transfere automaticamente a propriedade à AUDIMEC. Documentação produzida pela firma deve observar os requisitos profissionais e contratuais específicos. O sigilo persiste após o término do vínculo.

1.5 Comportamento esperado

Todos devem proteger credenciais, bloquear a estação ao se afastar, guardar documentos, confirmar destinatários e relatar suspeitas prontamente. É vedado explorar informação para benefício pessoal, contornar controles ou retirar arquivos para uso particular. A classificação pública de um dado não autoriza qualquer tratamento de dados pessoais.

Governança e responsabilidades

Sócios e administração	Aprovar a Política e suas revisões; designar responsáveis e substitutos; assegurar recursos e acompanhar riscos e correções.
Responsável por segurança	Coordenar controles, riscos, incidentes, conscientização e testes; reportar questões relevantes à administração.
Suporte de tecnologia	Executar configurações, atualizações, gestão técnica de acessos, backups e resposta técnica, com autorizações e registros.
Gestores da informação	Classificar ativos, autorizar acessos e compartilhamentos, definir necessidades de conservação e validar revisões.
Responsável pelo trabalho	Proteger arquivos do cliente e a documentação técnica; assegurar supervisão, revisão e rastreabilidade.
Função de privacidade	Orientar tratamento de dados pessoais, avaliar direitos e comunicações legais e apoiar a resposta a incidentes.
Usuários e terceiros	Cumprir regras, utilizar recursos autorizados e comunicar riscos, perdas, falhas e acessos indevidos.

2.1 Designações e independência funcional

As funções podem ser exercidas por pessoas internas ou apoio externo, mediante designação formal e gestão de conflitos. Não se presume a existência de departamento ou comitê específico. O responsável por segurança deve ter acesso à administração e poder escalar incidentes sem bloqueio pelo gestor envolvido.

2.2 Cadastro operacional

A administração deve manter cadastro acessível de responsáveis, substitutos, suporte e meios de comunicação de incidentes, incluindo alternativa para indisponibilidade do canal principal. Novos usuários devem receber essas informações antes do acesso. Cada ativo relevante deve ter gestor e custodiante identificados.

Classificação e ciclo de vida

Pública	Divulgação expressamente autorizada. Exemplos: materiais institucionais publicados. Preservar integridade e direitos de terceiros.
Interna	Uso por profissionais autorizados. Exemplos: rotinas e comunicados internos. Não divulgar externamente sem autorização.
Confidencial	Acesso por necessidade de trabalho. Exemplos: propostas, contratos, relatórios não públicos e papéis de auditoria. Compartilhar apenas por meios controlados.
Restrita	Proteção reforçada. Exemplos: credenciais, chaves, investigações, dados de saúde e documentos de alto impacto. Limitar nominalmente acessos e registrar autorizações.

3.1 Classificação e inventário

O gestor deve classificar a informação conforme sigilo, impacto e obrigações aplicáveis, identificando-a por rótulo, metadado ou localização controlada. Dados pessoais não são todos sensíveis na acepção legal, mas todos exigem proteção apropriada. Na dúvida, documentos de clientes devem ser tratados como confidenciais até avaliação. O inventário deve incluir sistemas, equipamentos, repositórios, dados críticos e dependências.

3.2 Criação armazenamento e transporte

A proteção deve acompanhar a informação durante coleta, uso, cópia, armazenamento, transferência e descarte. Arquivos devem permanecer em repositórios corporativos autorizados, com organização por cliente e trabalho e controle de versões. Cópias locais devem ser limitadas e protegidas. Documentos físicos devem ficar em locais controlados; impressão e transporte exigem guarda e destinatário definido.

3.3 Retenção e descarte

Prazos devem constar de tabela aprovada que considere leis, normas profissionais, contratos e necessidades justificadas. Deve haver bloqueio de descarte em investigações, litígios e determinações de conservação. O descarte autorizado requer fragmentação de papel ou eliminação segura de mídias e arquivos, inclusive avaliação das cópias e do ciclo de retenção dos backups.

Identidades e controle de acesso

4.1 Menor privilégio

O acesso deve ser individual, limitado à função e aprovado pelo gestor da informação. A solicitação deve identificar usuário, finalidade, escopo e duração. Equipes devem acessar apenas os clientes e trabalhos necessários. Privilégios administrativos precisam de justificativa e conta separada do uso cotidiano, quando tecnicamente possível.

4.2 Credenciais e autenticação

Senhas devem ser robustas, exclusivas e armazenadas somente em solução autorizada. É vedado compartilhar contas, códigos de autenticação, tokens, certificados ou chaves privadas. Deve ser exigida autenticação multifator para e-mail corporativo, acessos remotos, contas privilegiadas e repositórios confidenciais quando suportada; limitações técnicas exigem controle compensatório e exceção registrada.

4.3 Entrada movimentação e desligamento

A criação de contas depende da autorização e da ciência das regras. Mudanças de função devem ajustar permissões. No desligamento, revogar acessos no momento apropriado ao encerramento, recolher ativos e preservar arquivos e evidências. Contas temporárias e de terceiros devem ter prazo e responsável. A preservação dos trabalhos não autoriza manter ativa a credencial de quem saiu.

4.4 Revisões e registros

Permissões devem ser revisadas pelo menos semestralmente e sempre que houver mudança relevante ou suspeita de comprometimento. A revisão deve abranger contas inativas, convidados, grupos, links e privilégios. Sistemas críticos devem registrar eventos relevantes de acesso e administração; registros devem ser protegidos contra alteração e conservados por prazo definido com base no risco e nas obrigações.

4.5 Acessos de emergência

Acessos excepcionais devem ser limitados no tempo, aprovados por responsável competente e revogados após uso. Se a urgência impedir a autorização prévia, a justificativa e as ações devem ser registradas e submetidas à revisão assim que possível. É vedado usar a emergência como autorização geral para copiar dados ou desabilitar controles.

Equipamentos e trabalho remoto

5.1 Configuração e manutenção

Equipamentos devem constar de inventário, receber atualizações de segurança, proteção contra malware, bloqueio de tela e configurações aprovadas. Dispositivos com informação confidencial devem utilizar criptografia de armazenamento, quando suportada. Instalação de software, extensões e conexão de mídias removíveis dependem de autorização. Falhas críticas devem ter prioridade de correção conforme o risco.

5.2 Trabalho remoto e viagens

Trabalhe em ambiente que evite exposição de tela, documentos e conversas. Use conexões seguras e mecanismos aprovados para acesso remoto; redes públicas exigem proteção adicional. Não deixe equipamentos e documentos sem vigilância. Evite computadores compartilhados ou de terceiros para acessar informações confidenciais. Perda ou furto deve ser reportado imediatamente, com indicação dos dados e acessos potencialmente expostos.

5.3 Dispositivos pessoais

O uso de dispositivo pessoal para atividades da AUDIMEC exige autorização e avaliação de segurança, separação de dados e regras claras de suporte e retirada das informações corporativas. Não deve haver acesso irrestrito a dados particulares. Se não for possível assegurar proteção adequada, o dispositivo não deve armazenar ou processar informações confidenciais da firma ou dos clientes.

5.4 Segurança física

Visitantes devem ter acesso limitado e acompanhamento quando necessário. Áreas de arquivo e infraestrutura devem ter acesso controlado. Documentos devem ser retirados prontamente de impressoras e guardados ao final do uso. Reuniões com informações confidenciais exigem verificação de participantes e gravação apenas quando autorizada e justificada.

5.5 Uso aceitável

Recursos devem atender a finalidades profissionais autorizadas. São vedados softwares sem licença, mecanismos de evasão de controles e atividades ilícitas. Uso pessoal eventual, se admitido, não pode gerar risco, consumo inadequado ou prejuízo ao trabalho. O monitoramento deve ser informado, proporcional e compatível com direitos e obrigações legais.

Compartilhamento e serviços digitais

6.1 Envio e recebimento seguro

Antes de compartilhar, verifique identidade, necessidade e autorização do destinatário. Prefira links com acesso nominal, prazo e permissões limitadas; evite links públicos. Documentos restritos exigem proteção reforçada e, quando pertinente, senha enviada por meio separado. Arquivos recebidos devem ser verificados antes da abertura; instruções de pagamento ou mudanças de conta devem ser confirmadas por canal independente.

6.2 E-mail e mensagens

Não encaminhe documentos de clientes a contas particulares nem use aplicativos não autorizados como arquivo permanente dos trabalhos. Mensagens suspeitas não devem ser respondidas, e links e anexos duvidosos não devem ser abertos. Se ocorrer envio incorreto, comunique o incidente; pedidos de exclusão ao destinatário não substituem análise e registro da exposição.

6.3 Nuvem e fornecedores

Serviços digitais devem ser avaliados antes da contratação: acesso, criptografia, localização dos dados, subcontratação, recuperação, registros e saída do serviço. Contratos devem prever confidencialidade, responsabilidades, comunicação de incidentes, devolução ou descarte e requisitos de segurança. Ferramentas corporativas, inclusive plataformas de colaboração, exigem configuração adequada; sua marca ou contratação não garante segurança por si só.

6.4 Inteligência artificial

O uso de IA depende de aprovação da ferramenta e do caso de uso, considerando sigilo, tratamento de dados, retenção e utilização para treinamento. É vedado inserir informação confidencial, pessoal ou documentação de auditoria em soluções não aprovadas. Resultados precisam de revisão humana, validação de fontes e registro quando relevantes ao trabalho. Nenhuma ferramenta substitui julgamento profissional.

6.5 Desenvolvimento e mudanças

Novos sistemas, integrações e automações devem incorporar segurança desde o desenho, testes e controle de alterações. Ambientes de teste devem usar dados fictícios ou adequadamente protegidos. Mudanças relevantes precisam de aprovação, possibilidade de reversão e avaliação de permissões, segredos e exposição de dados.

Privacidade e documentação de auditoria

7.1 Dados pessoais

O tratamento exige finalidade, base legal e limitação ao necessário, com proteção proporcional ao risco. Dados de saúde, biometria e outras categorias legalmente sensíveis exigem análise específica. A equipe deve restringir solicitações de documentos ao escopo do trabalho e evitar coleta excessiva. Dados de crianças e adolescentes demandam cautelas próprias e avaliação do melhor interesse, quando aplicável.

7.2 Registros e papéis de tratamento

A função de privacidade deve manter registros das operações relevantes e avaliar se a AUDIMEC atua como controladora ou operadora em cada atividade. A natureza do contrato, isoladamente, não resolve essa classificação. Solicitações de titulares, compartilhamentos e transferências internacionais devem ser encaminhados para avaliação e execução conforme as regras aplicáveis.

7.3 Papéis de trabalho

Documentação deve permitir identificar quem executou e revisou os procedimentos e quando, com preservação de versões e conclusões. É vedado alterar evidências para ocultar erro ou modificar indevidamente a data de execução. Acesso de revisores, profissionais de qualidade e fiscalizadores deve ser autorizado e controlado conforme normas e deveres profissionais. Não se devem misturar arquivos de diferentes clientes sem proteção adequada.

7.4 Conservação e pedidos de exclusão

Solicitações de eliminação devem ser avaliadas em conjunto com obrigações de conservação e bases legais. Não se deve excluir documentação de auditoria automaticamente nem conservar dados indefinidamente por conveniência. A tabela de retenção deve distinguir documentos técnicos, dados administrativos, registros de segurança e backups e contemplar os requisitos próprios de cada categoria.

7.5 Divulgação autorizada

Relatórios, casos, nomes, imagens e marcas de clientes somente podem ser publicados com autorização apropriada e respeito às obrigações profissionais. Informações exigidas por autoridades devem ser encaminhadas por pessoas autorizadas, com registro e limitação ao necessário. O dever de confidencialidade não impede cumprimento de comunicação legal obrigatória.

Backups e continuidade

8.1 Plano de cópias de segurança

Ativos críticos devem ter backup definido por responsável, frequência, retenção e objetivo de recuperação. Deve existir cópia separada do ambiente principal e protegida contra exclusão indevida, com acesso restrito e criptografia conforme o risco. Sincronização de pastas e histórico de versões não devem ser presumidos como backup suficiente.

8.2 Verificação e restauração

A execução das cópias deve ser acompanhada, com tratamento das falhas. Testes de restauração devem ocorrer ao menos semestralmente e após mudanças relevantes, registrando resultados, integridade dos dados e pendências. Não basta verificar que o arquivo de backup foi criado: deve-se demonstrar a capacidade de recuperar informações utilizáveis.

8.3 Continuidade das atividades

A administração deve identificar serviços críticos, dependências e prioridades, definindo o tempo máximo de interrupção tolerável e a perda de dados aceitável. O plano deve indicar responsáveis, fornecedores, comunicação e alternativas para falha de sistemas, indisponibilidade de nuvem, ataque, perda de equipamento e interrupção física. A continuidade deve preservar sigilo e qualidade técnica.

8.4 Recuperação controlada

O retorno deve ocorrer em ambiente verificado, com análise da causa, validação das configurações e acompanhamento de sinais de comprometimento. Não restaure dados potencialmente infectados sem avaliação técnica. A equipe do trabalho deve ser informada de perdas, alterações ou lacunas que possam afetar evidências e relatórios.

8.5 Exercícios e aprendizado

O plano de continuidade deve ser testado ao menos anualmente, mediante exercício compatível com os riscos. Pendências devem ter responsável e prazo. Alterações em contratos, repositórios ou fornecedores devem atualizar as dependências e os procedimentos de recuperação. Os intervalos previstos nesta Política são requisitos internos e não uma declaração de controles já executados.

Gestão de riscos e incidentes

9.1 Avaliação de riscos

Devem ser identificadas ameaças, vulnerabilidades, probabilidade, impactos e controles, com responsáveis e ações. A avaliação deve ocorrer ao menos anualmente e diante de novos sistemas, fornecedores, serviços ou incidentes relevantes. Correções devem ser priorizadas por risco, sem limitar a análise a dados pessoais.

9.2 Comunicação imediata

Qualquer suspeita de vazamento, acesso indevido, malware, perda, envio incorreto ou indisponibilidade relevante deve ser comunicada imediatamente ao responsável por segurança e ao gestor do trabalho ou ativo. Se não houver contato disponível, deve-se acionar um sócio, sem aguardar certeza. Utilize os canais divulgados; se comprometidos, empregue meio alternativo confiável. Não apague evidências nem investigue por conta própria.

9.3 Resposta e preservação

O responsável deve registrar horário de ciência, fatos, ativos, dados, pessoas potencialmente afetadas e medidas tomadas; avaliar criticidade; conter a exposição; e mobilizar apoio técnico, privacidade e jurídico. O isolamento de equipamentos e o bloqueio de contas devem preservar evidências na medida possível. Decisões, comunicações, recuperação e medidas corretivas precisam de rastreabilidade.

9.4 Comunicações externas

A função de privacidade deve avaliar se o incidente com dados pessoais pode gerar risco ou dano relevante e quais comunicações são exigidas pelo art. 48 da LGPD e pela regulamentação vigente da ANPD. Quando operadora, a AUDIMEC deve informar o controlador sem demora injustificada e cooperar com a resposta. Prazos legais e contratuais devem ser identificados desde a triagem; a apuração interna não autoriza adiar comunicação obrigatória. Somente pessoas autorizadas podem se manifestar pela firma.

9.5 Encerramento

Incidentes devem ter avaliação de causa, conclusão documentada, decisão sobre notificações e plano de correção. Registre também a justificativa para não notificar quando cabível. Pessoas que reportem de boa-fé não podem sofrer retaliação. O cadastro operacional deve definir substitutos e escalonamento, inclusive quando responsáveis estiverem envolvidos.

Aplicação revisão e ciência

10.1 Capacitação e exceções

Usuários devem receber orientação antes do acesso e capacitação anual sobre riscos de sua função. Exceções exigem justificativa, análise de risco, aprovação competente, controle compensatório, prazo e revisão. Não podem dispensar obrigação legal ou profissional. A administração deve acompanhar acessos revisados, falhas de backup, testes de recuperação, correções e cobertura de treinamento.

10.2 Consequências e revisão

Descumprimentos devem ser apurados com imparcialidade e resposta proporcional, observadas a legislação e as relações contratuais. Podem resultar em orientação, restrição de acesso e medidas disciplinares ou contratuais cabíveis. Não se presume culpa pela ocorrência de incidente. Esta Política deve ser revista anualmente e quando houver mudança relevante, com aprovação dos sócios e comunicação aos públicos afetados.

10.3 Referência normativa

Lei nº 13.709/2018 — LGPD: princípios e bases do tratamento, registros e proteção de dados, especialmente arts. 6º, 7º, 11, 16, 18, 33, 37 e 46 a 50. Texto vigente: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Aplicam-se também as normas profissionais do CFC relativas a sigilo, documentação e gestão da qualidade, os contratos e a regulamentação vigente da ANPD. Os controles e periodicidades internos desta Política não devem ser atribuídos à LGPD como exigências literais.

Termo de ciência e compromisso

Declaro que recebi acesso à Política de Segurança da Informação da AUDIMEC, versão 1.0, aprovada pelos sócios. Comprometo-me a observar suas regras, proteger as informações e comunicar incidentes e suspeitas prontamente. Reconheço que o dever de confidencialidade permanece após o término do vínculo. Este termo não implica renúncia a direitos legais.

Nome: _____
Função ou vínculo: _____
Local e data: _____
Assinatura: _____