CONTROL 361 TECNOLOGIA E SERVIÇOS LTDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2025 / 2026

CONTROL 361°

Índice

01

INTRODUÇÃO

A Política de Segurança da Informação (PSI) da CONTROL 361 define regras, princípios, controles e diretrizes para garantir a confidencialidade, integridade e disponibilidade das informações, bem como conformidade com a LGPD e demais normas aplicáveis.

Todos os colaboradores, prestadores de serviço, parceiros, fornecedores e qualquer pessoa que trate dados ou acesse recursos da empresa devem cumprir esta Política obrigatoriamente.

02

OBJETIVOS

1.Garantir a Confidencialidade, Integridade e Disponibilidade (CID) dos ativos de informação, por meio da implementação e manutenção de controles de acesso, criptografia e redundância, visando zero violações de dados críticos.

2. Estruturar e Oficializar as diretrizes de Segurança Física e Lógica (incluindo gestão de identidade e acesso), assegurando que 100% dos ambientes e sistemas críticos estejam cobertos por procedimentos operacionais formais.

3. Manter a Conformidade Plena (100%) com todas as leis, regulamentos e padrões de segurança aplicáveis, evitando multas e sanções regulatórias e comprovando esta conformidade em auditorias.

4. Elevar o Nível de Conscientização e Engajamento dos colaboradores, alcançando 95% de conclusão e aprovação nos programas de treinamento obrigatórios e contribuindo para a redução de 10% em incidentes causados por erro humano.

5. Facilitar e Suportar processos de auditoria (internas e externas) com alta eficiência, garantindo que todos os requisitos de evidência sejam atendidos no prazo e que o tempo de resolução de não-conformidades seja reduzido pela metade.

03

ABRANGÊNCIA

Esta Política aplica-se a todas as pessoas, físicas ou jurídicas, que, de qualquer forma, utilizem, tratem, armazenem, transmitam, manipulem ou acessem informações, recursos ou ativos da empresa, incluindo:

• Dados pessoais e dados pessoais sensíveis, em qualquer formato, conforme definição da LGPD.

• Informações corporativas, administrativas, operacionais, financeiras, estratégicas, comerciais, contratuais, tecnológicas e de propriedade intelectual.

• Sistemas, plataformas, servidores, redes, bancos de dados, aplicativos, e-mails corporativos e demais ferramentas tecnológicas disponibilizadas ou autorizadas pela empresa.

• Documentos e registros físicos ou digitais, independentemente do meio de armazenamento (papel, nuvem, dispositivos móveis, mídias externas etc.).

• Equipamentos, dispositivos e ativos corporativos, bem como dispositivos pessoais autorizados (BYOD), incluindo computadores, notebooks, celulares, tablets e quaisquer outros meios que permitam acesso às informações da empresa.

Esta Política também se estende a colaboradores, estagiários, aprendizes, diretores, prestadores de serviços, consultores, fornecedores, parceiros, terceirizados e quaisquer agentes de tratamento envolvidos nas operações da empresa.

04

CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação tem como objetivo garantir que cada dado seja tratado de acordo com seu nível de sensibilidade, impacto e requisitos legais, especialmente aqueles previstos na Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018).

Toda informação produzida, recebida, armazenada ou tratada pela empresa deve ser classificada em uma das categorias abaixo, independentemente do formato (digital, físico, audiovisual, verbal ou eletrônico):

4.1 Informação Pública

Informações cujo acesso é livre e não gera risco à empresa, aos titulares de dados ou às suas operações se divulgadas.

Exemplos:

• Conteúdo institucional já divulgado ao público

• Informações publicadas em site, redes sociais ou materiais oficiais

• Comunicados de utilidade pública

Regras:

• Não requerem autorização para divulgação

• Devem ser verificadas antes da publicação para garantir autenticidade e integridade

4.2 Informação Interna

Informações destinadas ao uso exclusivo de colaboradores e autorizados, cuja divulgação indevida pode gerar impactos administrativos, operacionais ou de imagem.

Exemplos:
• Procedimentos internos
• Manuais, fluxos de trabalho e relatórios não estratégicos
• Dados cadastrais corporativos não sensíveis

Regras:
• Acesso limitado a colaboradores e prestadores autorizados
• É proibida a divulgação externa sem permissão formal
• Necessário controle básico de acesso e armazenamento seguro

4.3 Informação Confidencial

Informações restritas a áreas, departamentos ou pessoas determinadas, cuja divulgação indevida pode causar impacto financeiro, estratégico, competitivo ou jurídico.

Exemplos:
• Dados pessoais não sensíveis (nome, documento, endereço etc.)
• Informações financeiras e contábeis
• Estratégias comerciais
• Contratos, negociações, propostas e documentos jurídicos
• Dados técnicos, códigos, metodologias, sistemas e propriedade intelectual

Regras:
• Acesso concedido somente conforme o princípio do menor privilégio
• Requer mecanismos de autenticação, controle de permissões e rastreabilidade
• Proibido copiar, transmitir ou armazenar fora dos sistemas autorizados

4.4 Informação Sigilosa (Crítica / Alta Sensibilidade)

Informações que exigem o mais alto nível de proteção, pois sua exposição pode gerar danos graves à empresa, aos titulares de dados ou provocar violação de normas legais, especialmente LGPD. Inclui dados pessoais sensíveis, dados estratégicos e informações regulamentadas.

Exemplos:
• Dados pessoais sensíveis (origem racial, saúde, biometria, religião, dados genéticos, vida sexual)
• Dados pessoais de alto risco (crianças, financeiros, localização em tempo real)
• Informações estratégicas, confidenciais de alto impacto, investigações internas
• Credenciais de acesso, chaves criptográficas, backups críticos
• Dados protegidos por sigilo legal, industrial, contratual ou regulatório

Regras:
• Acesso extremamente restrito, autorizado apenas a pessoal essencial
• Armazenamento com criptografia e controles reforçados

• Proibida a transferência sem mecanismos seguros
• Uso monitorado e auditável
• Requer plano de resposta em caso de incidente (data breach)

4.5 Regras Gerais de Classificação

• Toda informação deve possuir classificação definida pelo responsável pelo documento, sistema ou processo.
• Documentos e arquivos devem conter identificação visível da classificação.
• A classificação deve ser revisada periodicamente ou quando houver alteração no conteúdo.
• Em caso de dúvida, a informação deve ser tratada como Confidencial ou Sigilosa.
• A responsabilidade pela correta classificação e proteção é compartilhada entre todos os usuários.

05

CONTROLES DE ACESSO

Os controles de acesso têm como objetivo garantir que somente pessoas autorizadas acessem informações, sistemas, dispositivos, documentos e demais ativos da empresa, respeitando os princípios da necessidade, finalidade, proporcionalidade e segurança, previstos na LGPD e nas melhores práticas internacionais.
Os acessos devem ser concedidos, monitorados, revisados e revogados conforme as diretrizes abaixo:

5.1 Princípios Gerais

• Todos os acessos devem seguir o Princípio do Menor Privilégio, ou seja, concedidos exclusivamente conforme a necessidade de o usuário desempenhar suas funções.
• O acesso deve sempre estar vinculado a um responsável, um motivo e uma base legal, quando envolver dados pessoais.
• É proibido acessar qualquer informação que não estejam diretamente relacionadas às atribuições do usuário.
• A empresa mantém trilhas de auditoria para rastrear acessos, alterações e usos indevidos.

5.2 Identificação e Autenticação

• Cada usuário deve possuir credencial exclusiva, pessoal e intransferível.
• É proibido compartilhar logins, senhas ou dispositivos autenticados.
• Sistemas críticos devem utilizar autenticação multifator (MFA/2FA) obrigatória.
• Senhas devem seguir requisitos mínimos:
  ▪ Complexidade (maiúscula, minúscula, número e caractere especial)
  ▪ o Troca periódica conforme política interna
  ▪ o Armazenamento seguro (hashing e/ou mecanismos adequados)
• Senhas nunca devem ser anotadas em papel, post-its, cadernos ou ambientes desprotegidos.

5.3 Concessão de Acesso

• A concessão deve ser formalizada por meio de solicitação registrada (ticket, workflow ou documento específico).
• A aprovação deve ser realizada pelo gestor da área e/ou proprietário do ativo (data owner).
• O setor de TI e Segurança da Informação deve configurar o acesso conforme os níveis autorizados.
• A concessão deve considerar:
◦ Função do usuário
◦ Necessidade de acesso a dados pessoais
◦ Classificação da informação
◦ Riscos associados
◦ Controles exigidos por normativos de LGPD

5.4 Revisão, Atualização e Revogação de Acessos

• Revisões de acesso devem ocorrer periodicamente (mínimo trimestral ou conforme criticidade).
• Modificações de função, promoção, transferência ou mudança de atividade exigem atualização imediata dos acessos.
• A revogação deve ocorrer no mesmo dia do desligamento ou término da relação contratual.
• A empresa manterá registros das concessões, alterações e revogações para fins de auditoria e compliance.

5.5 Acesso a Dados Pessoais e Dados Sensíveis

• O acesso a dados pessoais depende de finalidade clara, base legal definida e aderência às normas internas da LGPD.

• Dados pessoais sensíveis só podem ser acessados por pessoas estritamente autorizadas, mediante:
◦ Controle rigoroso de permissões
◦ Registro de logs detalhados
◦ Mecanismos de criptografia e segregação de dados
• É proibido acessar, copiar, extrair ou compartilhar dados pessoais para finalidades não autorizadas.

5.6 Acesso Remoto

• Deve ocorrer apenas em dispositivos autorizados e protegidos por:
◦ VPN corporativa
◦ MFA
◦ Antivírus e firewall ativo
◦ Criptografia de disco quando necessária
• O uso de redes públicas sem proteção adequada é estritamente proibido.

5.7 Acesso de Terceiros e Fornecedores

• Acesso concedido a terceiros deve cumprir:
◦ Contratos com cláusulas de confidencialidade e LGPD
◦ Controle de acesso temporário e proporcional
◦ Monitoramento e auditoria durante todo o período de acesso
• A empresa pode exigir certificações de segurança, compromissos de sigilo e boas práticas como condição para concessão.

5.8 Monitoramento e Auditoria

• A empresa monitora atividades de acesso para:
◦ Identificação de uso indevido
◦ Prevenção de fraudes
◦ Detecção de incidentes de segurança
◦ Cumprimento de normas legais
• Logs são mantidos conforme política interna, garantindo integridade e sigilo.

5.9 Sanções

Descumprimentos, como compartilhamento de senhas, acessos indevidos ou tentativa de burlar controles, configuram falta grave, podendo resultar em:
• Advertência
• Suspensão
• Desligamento
• Responsabilização civil e penal
• Comunicação à ANPD em casos de violação de dados pessoais

USO ADEQUADO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO (TI)

06

Os recursos de Tecnologia da Informação (TI) da empresa devem ser utilizados de forma ética, responsável, segura e exclusivamente para fins profissionais autorizados. O uso adequado é essencial para garantir a proteção das informações, a continuidade das operações, o cumprimento das leis e a mitigação de riscos técnicos e jurídicos. Esta política se aplica a todos que utilizem equipamentos, sistemas ou serviços tecnológicos disponibilizados ou autorizados pela empresa.

6.1 Princípios Gerais

• Todo uso dos recursos de TI deve respeitar os princípios de segurança, confidencialidade, legalidade, finalidade e necessidade.
• Os recursos tecnológicos da empresa não são privados; portanto, podem ser monitorados conforme legislação e política interna.
• É proibido utilizar recursos tecnológicos para atividades ilegais, antiéticas, pessoais de alto risco ou não autorizadas.

6.2 Recursos Sob Gestão da Empresa

Consideram-se recursos de TI:
• Computadores, notebooks, tablets e smartphones corporativos
• Dispositivos móveis autorizados (BYOD)
• Redes cabeadas e Wi-Fi
• Servidores, storages, bancos de dados e nuvens corporativas
• Sistemas, plataformas e softwares corporativos
• E-mail institucional
• Ferramentas de comunicação, videoconferência e colaboração
• Impressoras, scanners, mídias externas e dispositivos periféricos

6.3 Uso Permitido

É permitido:
• Utilizar recursos exclusivamente para atividades profissionais e dentro das permissões autorizadas
• Acessar sistemas e informações conforme credenciais próprias
• Realizar comunicação profissional por meio de e-mail corporativo e ferramentas oficiais
• Utilizar serviços de nuvem apenas se forem homologados pela empresa
• Usar dispositivos pessoais para trabalho somente se autorizado e configurado com mecanismos de segurança

6.4 Uso Proibido

É estritamente proibido:

6.4.1 Instalação e Softwares
• Instalar softwares sem autorização
• Utilizar programas piratas, não licenciados ou não homologados
• Executar scripts, macros ou ferramentas suspeitas

6.4.2 Navegação e Conteúdos
• Acessar sites ilegais, pornográficos, discriminatórios ou que contrariem políticas internas
• Realizar downloads de origem duvidosa
• Acessar ambientes de alto risco (dark web, VPNs não autorizadas, proxy bypass)

6.4.3 Compartilhamento e Transmissão
• Compartilhar arquivos ou informações corporativas em e-mails pessoais
• Utilizar Google Drive, Dropbox, OneDrive ou outra nuvem pessoal para armazenar dados da empresa
• Enviar dados sem criptografia quando exigido

6.4.4 Dispositivos e Hardware
• Conectar pendrives ou mídias externas sem autorização
• Modificar, danificar ou desativar recursos de segurança dos dispositivos
• Usar gadgets que possam capturar áudio, vídeo ou dados sensíveis sem permissão

6.5 Uso de E-mail Corporativo

• Deve ser utilizado exclusivamente para fins profissionais.
• É proibido:
  ◦ Encaminhar dados pessoais ou sigilosos sem medida de segurança adequada
  ◦ Utilizar e-mail corporativo em cadastros pessoais
  ◦ Compartilhar credenciais de acesso
  ◦ Enviar correntes, spam, piadas, conteúdos ofensivos ou não profissionais
  ◦ Mensagens enviadas e recebidas podem ser registradas, arquivadas e auditadas conforme legislação.

6.6 Navegação na Internet

• Deve ocorrer exclusivamente para fins profissionais.
• A empresa pode bloquear sites que representem riscos.
• A navegação pode ser monitorada para garantir segurança e conformidade.

6.7 Dispositivos Móveis e BYOD

Dispositivos pessoais utilizados para fins profissionais devem:
• Ser autorizados formalmente
• Possuir bloqueio de tela, senha ou biometria
• Estar atualizados e com antivírus ativo
• Permitir instalação de ferramentas corporativas de segurança (MDM)
É proibido armazenar dados sensíveis ou confidenciais em dispositivos pessoais sem autorização expressa.

6.8 Armazenamento de Dados

• Documentos corporativos devem ser armazenados somente:
◦ Em sistemas oficiais da empresa
◦ Em nuvens corporativas homologadas
◦ Em servidores ou repositórios autorizados
• É proibido salvar dados corporativos em:
◦ Pendrives não autorizados
◦ E-mails pessoais
◦ Discos locais sem proteção
◦ Plataformas externas não autorizadas
◦ Backups pessoais são proibidos.

6.9 Comunicação e Ferramentas Corporativas

• Somente ferramentas aprovadas (Teams, Slack, Zoom, WhatsApp corporativo etc.) podem ser utilizadas.
• O uso de WhatsApp pessoal para dados corporativos deve seguir regras internas e não pode conter dados sensíveis.

6.10 Responsabilidade do Usuário

Todo usuário é responsável por:
• Zelar pelo equipamento sob sua guarda
• Bloquear a tela quando se ausentar
• Notificar imediatamente incidentes, perdas, roubos ou suspeitas
• Manter confidencialidade e proteção das informações acessadas

6.11 Monitoramento e Auditoria

Para garantir a segurança, a empresa poderá monitorar:
• Acessos
• Logs de sistemas
• Uso de e-mail
• Tráfego na rede
• Atividades realizadas no ambiente corporativo
O monitoramento será realizado conforme legislação (LGPD, Marco Civil e Código Civil), respeitando princípios de necessidade e proporcionalidade.

6.12 Penalidades

O uso inadequado de recursos de TI pode resultar em:
• Advertência
• Suspensão
• Desligamento
• Responsabilização civil e penal
• Comunicação à ANPD quando envolver dados pessoais

07 SEGURANÇA FÍSICA

A Segurança Física tem por objetivo proteger pessoas, ativos, instalações e informações contra acesso físico não autorizado, danos, interferências, furtos, vandalismo, desastres, violação de dados e quaisquer eventos que comprometam a confidencialidade, integridade e disponibilidade das informações e dos recursos corporativos.
Este conjunto de controles aplica-se a todos os ambientes físicos utilizados pela empresa, incluindo escritórios, salas técnicas, data centers, pontos de atendimento, unidades operacionais, depósitos, arquivos físicos, bem como áreas compartilhadas ou ocupadas por terceiros.

7.1 Controles de Acesso Físico

A empresa deve garantir mecanismos eficazes de controle de entrada, permanência e saída:
• Acesso permitido somente a pessoas autorizadas, mediante identificação prévia (crachá, biometria, cartão magnético ou outro controle formal).
• Visitantes, fornecedores e terceiros devem:
  ◦ ser devidamente registrados;
  ◦ portar credenciais identificáveis;
  ◦ ser acompanhados por colaborador responsável;
  ◦ ter acesso limitado apenas às áreas estritamente necessárias.
• Todo acesso a áreas críticas deve ser monitorado, registrado e auditável.
• É proibido o compartilhamento de crachás, senhas ou dispositivos de acesso.

7.2 Ambientes de Alta Criticidade (Salas Técnicas, CPDs, Racks, Infraestrutura de TI)

Ambientes críticos devem possuir:
• Controle de acesso segregado e altamente restrito.
• Monitoramento por CFTV 24h, com gravação de imagens conforme legislação aplicável.
• Alarmes de intrusão, sensores de movimento e registro automático de eventos.
• Portas reforçadas, fechaduras eletrônicas e mecanismos anti-arrombamento.
• Acesso apenas para equipe autorizada de TI ou manutenção.

Dados pessoais sensíveis e sistemas essenciais devem ser armazenados somente em áreas protegidas por controles estruturais e tecnológicos adequados.

7.3 Proteção de Documentos Físicos

Documentos físicos classificados como Confidenciais ou Sigilosos, especialmente contendo dados pessoais ou sensíveis, devem:
• Ser guardados em armários ou cofres trancados, com acesso limitado.
• Ter controle de empréstimo e devolução.
• Ser descartados somente por trituradores de segurança ou serviços certificados de descarte seguro (shredding).
• Nunca permanecerem expostos em mesas, impressoras ou áreas comuns (“clean desk policy”).

7.4 Monitoramento, Vigilância e Registro

A empresa pode utilizar monitoramento por CFTV, vigilância patrimonial e registro de entrada/saída, respeitando:
• a legislação de proteção de dados;
• o princípio da finalidade;
• o mínimo necessário;
• políticas de retenção e descarte seguro das imagens;
• sinalização adequada nos ambientes monitorados.
As imagens são utilizadas exclusivamente para finalidades de segurança, prevenção de incidentes e apuração de eventos.

7.5 Prevenção de Incidentes e Continuidade Operacional

A infraestrutura física deve prever:

• Sistemas de detecção e combate a incêndio (extintores, sprinklers, alarmes).
• Sinalização e rotas de evacuação.
• Fontes alternativas de energia (no-breaks, geradores) para sistemas críticos.
• Condições adequadas de climatização em salas técnicas.
• Controle de umidade e poeira para proteger equipamentos e documentos.
A empresa deve manter Plano de Continuidade de Negócios (PCN) e Plano de Resposta a Incidentes (PRI), incluindo procedimentos para desastres naturais ou emergências.

7.6 Equipamentos e Dispositivos Físicos

• Equipamentos corporativos não devem ser removidos das dependências sem autorização.
• Em caso de transporte ou deslocamento, devem ser utilizados mecanismos de proteção (malas travadas, selos de integridade, criptografia de disco).
• Dispositivos perdidos, danificados ou furtados devem ser comunicados imediatamente ao setor responsável e ao DPO, quando envolver dados pessoais.

7.7 Responsabilidade dos Colaboradores

Todos os usuários devem:
• Zelar pelos acessos físicos fornecidos.
• Não permitir o ingresso de pessoas não autorizadas (“tailgating”).
• Reportar situações suspeitas, portas abertas, visitantes não identificados ou qualquer incidente de segurança.
• Cumprir integralmente as medidas desta Política.

7.8 Penalidades

O descumprimento das regras de Segurança Física constitui falta grave, sujeita a:
• advertência;
• suspensão;
• rescisão por justa causa (quando aplicável);
• responsabilização civil e/ou criminal, nos casos previstos em lei.

08 SEGURANÇA LÓGICA / SEGURANÇA CIBERNÉTICA

A Segurança Lógica tem por objetivo proteger sistemas, redes, dispositivos, informações corporativas e dados pessoais contra acessos indevidos, ataques cibernéticos, perdas, vazamentos, destruição, interrupções e quaisquer riscos digitais que comprometam a confidencialidade, integridade, disponibilidade e autenticidade das informações.
Aplicam-se estes controles a todos os usuários, equipamentos, sistemas e ambientes, internos ou hospedados em provedores externos (nuvem, SaaS, PaaS, IaaS).

8.1 Controles de Acesso e Identidade (IAM – Identity and Access Management)

• Todos os usuários devem possuir credenciais individuais, sendo proibido o uso de contas compartilhadas.
• Adoção obrigatória de autenticação multifatorial (MFA) para acesso a sistemas sensíveis, dados pessoais e ambientes administrativos.
• Princípio do menor privilégio: permissões concedidas apenas no limite necessário às atividades.
• Revisão periódica de acessos (mínimo trimestral).
• Desativação imediata de acessos em caso de desligamento ou alteração de função.
• Contas privilegiadas (admin) devem possuir controles diferenciados, monitoramento e rastreabilidade.

8.2 Gestão de Senhas

• Senhas devem ser únicas, complexas, fortes e alteradas periodicamente.
• É proibido:
◦ compartilhar senhas;
◦ anotá-las em locais visíveis;
◦ usar senhas corporativas em serviços pessoais.
• Senhas sensíveis devem ser armazenadas apenas em cofres de senhas com criptografia forte.

8.3 Proteção de Rede e Infraestrutura

• Utilização de firewall corporativo, IPS/IDS, filtros de tráfego e segmentação de rede.

• Monitoramento contínuo de logs, comportamentos suspeitos e eventos de segurança.
• Bloqueio automático de acessos indevidos, tentativas de força bruta e padrões maliciosos.
• Acesso remoto permitido somente via VPN corporativa com autenticação forte.
• Proibição de redes Wi-Fi sem senha ou abertas; redes corporativas devem utilizar WPA2/WPA3.

8.4 Dispositivos e Endpoints

• Todos os dispositivos corporativos devem possuir:
◦ antivírus/antimalware atualizado;
◦ firewall ativo;
◦ criptografia de disco;
◦ bloqueio automático de tela.
• BYOD (uso de dispositivos pessoais) só é permitido mediante autorização formal e com instalação de MDM (Mobile Device Management).
• Conexão de dispositivos externos (pendrives, HDs, mídias) deve ser restrita e monitorada.

8.5 Segurança em Computação em Nuvem (Cloud Security)

Para sistemas hospedados em nuvem pública, privada ou híbrida:
• Obrigatória a adoção do modelo de responsabilidade compartilhada.
• Dados sensíveis devem estar criptografados em trânsito e em repouso.

• Avaliação prévia de segurança do fornecedor (due diligence, compliance, certificações).
• Controle de acesso segregado, logs de auditoria e políticas de retenção alinhadas à LGPD.
• Proibição de armazenamento de dados pessoais em plataformas não autorizadas (Google Drive pessoal, Dropbox, iCloud pessoal etc.).

8.6 Segurança Aplicada a Sistemas, Softwares e Aplicativos

• Sistemas devem ser desenvolvidos e mantidos seguindo o padrão Security by Design e Privacy by Design (LGPD).
• Aplicação obrigatória de patches e atualizações de segurança.
• Realização de testes de segurança:
◦ Análise de vulnerabilidades;
◦ Testes de intrusão (pentest);
◦ Testes de caixa cinza, branca ou preta, conforme criticidade.
• Integrações com APIs devem utilizar tokens seguros e criptografia.

8.7 Proteção contra Malware, Phishing e Engenharia Social

• Bloqueio automático de arquivos suspeitos e sandboxing para análise segura.
• Filtros de e-mail para detectar phishing, spam e anexos potencialmente maliciosos.
• Treinamentos periódicos obrigatórios sobre ameaças cibernéticas e LGPD.
• Qualquer recebimento de link, arquivo ou mensagem suspeita deve ser imediatamente reportado.

8.8 Criptografia e Segurança de Dados

• Dados pessoais, sensíveis e informações estratégicas devem ser criptografados em:
◦ armazenamento (at rest);
◦ transmissão (in transit).
• Chaves criptográficas devem ser armazenadas com segurança, utilizando HSM, quando aplicável.
• É proibida a criptografia “caseira” ou sem padrões reconhecidos.

8.9 Logs, Monitoramento e Auditoria

• Todos os sistemas críticos devem manter logs completos, com: registros de acesso;
◦ alterações;
◦ falhas;
◦ incidentes;
◦ tentativas de acesso indevido.
• Logs devem ser protegidos contra acesso e modificação, com retenção conforme legislação e políticas internas.
• Auditorias internas e externas devem ser realizadas periodicamente.

8.10 Transferência e Compartilhamento de Dados

• Transferência de informações só pode ocorrer por canais seguros (SSL/TLS, VPN).
• Proibido enviar dados pessoais:
◦ por e-mail não criptografado;

◦ via WhatsApp ou redes sociais;
◦ por ferramentas não autorizadas.
• Compartilhamento com terceiros exige contrato com cláusulas de segurança e LGPD.

8.11 Resposta a Incidentes de Segurança da Informação (CSIRT)

A empresa deve manter processo formal de gestão de incidentes, incluindo:
• identificação;
• contenção;
• erradicação;
• recuperação;
• comunicação;
• lições aprendidas.

Incidentes envolvendo dados pessoais devem seguir o protocolo LGPD, com:
• avaliação do risco;
• notificação à ANPD quando aplicável;
• comunicação ao titular, se necessário.

8.12 Penalidades

O descumprimento das regras de Segurança Lógica constitui falta grave e pode resultar em:
• medidas disciplinares internas;
• responsabilização civil;
• responsabilização administrativa;
• responsabilização criminal, conforme legislação aplicável.

09

GESTÃO DE ACESSOS

A Gestão de Acessos tem como finalidade garantir que colaboradores, terceiros e sistemas acessem apenas os recursos mínimos necessários para o desempenho de suas funções, prevenindo acessos indevidos, uso inadequado das informações e riscos de incidentes de segurança.
Esse processo abrange criação, modificação, revisão, monitoramento revogação de acessos a sistemas, redes, dispositivos, dados, ferramentas corporativas e ambientes físicos e lógicos.

9.1 Princípios Fundamentais

a) Princípio do Menor Privilégio (Least Privilege)
Cada usuário deve possuir somente as permissões estritamente necessárias às suas atividades.
A concessão excessiva de permissões é proibida.
b) Princípio da Necessidade (Need to Know)
O acesso é autorizado apenas quando houver justificativa operacional válida e aprovação da área responsável.
c) Segregação de Funções (SoD – Segregation of Duties)
Funções críticas não podem ser desempenhadas por um único usuário, evitando riscos de fraude ou manipulação indevida (ex.: mesmo usuário não pode criar e aprovar transações).
d) Identidade Individual e Intransferível
Cada usuário deve possuir credenciais únicas.
É proibido o compartilhamento de logins, senhas ou contas genéricas.

9.2 Criação de Acessos

Fluxo obrigatório:
1. Solicitação formal via sistema, e-mail corporativo ou ferramenta de gestão.
2. Aprovação pela liderança imediata ou área solicitante.
3. Criação do acesso pela área de TI ou responsável.
4. Registro documental/auditável da concessão.
5. Comunicação ao usuário sobre boas práticas de uso e responsabilidades.

Requisitos técnicos:
• Uso obrigatório de autenticação multifator (MFA) para sistemas críticos.
• Definição de perfis de acesso padronizados, por função ou departamento.
• Acesso inicial sempre restrito, ampliado apenas mediante justificativa.

9.3 Modificação de Acessos

Alterações de função, promoção, mudança de departamento ou responsabilidade exigem:
• revisão imediata dos privilégios;
• remoção de acessos incompatíveis;
• adequação ao novo perfil funcional;
• registro formal da modificação.
A permanência de acessos desnecessários é proibida.

9.4 Revogação de Acessos

Casos obrigatórios:
• desligamento do colaborador;
• término do contrato com fornecedores ou terceiros;
• mudança de função que torne o acesso desnecessário;
• violação de políticas internas;
• solicitação da liderança ou compliance.
Regras:
• Revogação deve ser imediata — preferencialmente no mesmo dia ou em até 24 horas.
• Contas e e-mails corporativos devem ser bloqueados e posteriormente excluídos conforme política de retenção.
• Equipamentos corporativos devem ser devolvidos antes ou durante o bloqueio.

9.5 Contas Privilegiadas (Administração – “Super Usuário”)

Credenciais privilegiadas (admin, root, master, superuser) devem possuir controles reforçados:

• uso estritamente limitado e monitorado;
• acesso mediante justificativa formal;
• bloqueio automático após tentativas suspeitas;
• registro completo de logs, incluindo comandos executados;
• revisão quinzenal ou mensal das permissões;
• armazenamento em cofre de senhas corporativo.
Essas contas representam risco elevado e devem seguir padrões internacionais de PAM (Privileged Access Management).

9.6 Acessos de Terceiros, Fornecedores e Prestadores de Serviços

• Devem possuir acesso apenas temporário, proporcional ao contrato.
• Acesso externo permitido somente via VPN + MFA.
• É obrigatória cláusula contratual impondo:
◦ confidencialidade;
◦ proteção de dados;
◦ responsabilidade por incidentes;
◦ regras de acesso e revogação.
• Acesso deve ser desativado imediatamente ao fim da relação contratual.

9.7 Monitoramento, Auditoria e Logs de Acesso

A empresa deve manter:
• registro completo de acessos bem-sucedidos e negados;
• auditorias periódicas de logs;
• identificação de acessos anômalos ou uso indevido;
• alertas automáticos para comportamentos suspeitos;
• ferramentas SIEM para correlação de eventos (quando aplicável).
Os logs devem ser protegidos contra alteração e armazenados conforme política de retenção e LGPD.

9.8 Revisão Periódica de Acessos

Revisões devem ocorrer:
• trimestralmente para usuários comuns;
• mensalmente para usuários com privilégios elevados;
• imediatamente após incidente ou suspeita de abuso.

A revisão deve confirmar:
• acessos compatíveis com a função;
• inexistência de acessos duplicados;
• ausência de contas inativas ou obsoletas;
• inexistência de acessos críticos indevidos.

9.9 Responsabilidades do Usuário

Todos os usuários são obrigados a:
• Utilizar suas credenciais de forma segura e sigilosa.
• Informar imediatamente qualquer uso indevido ou suspeita de invasão.
• Não tentar burlar mecanismos de segurança.
• Cumprir as políticas de segurança e LGPD.
• Respeitar o nível de classificação das informações acessadas.

9.10 Penalidades

A violação das regras de Gestão de Acessos configura falta grave, podendo resultar em:
• advertência;
• suspensão;
• demissão por justa causa;
• responsabilização civil;
• responsabilização criminal, quando aplicável.

10 BACKUP, RETENÇÃO E RECUPERAÇÃO DE DADOS

A política de Backup, Retenção e Recuperação de Dados tem como objetivo garantir a continuidade operacional, a proteção da informação e a mitigação de riscos relacionados à perda, corrupção, indisponibilidade, destruição ou modificação indevida de dados e sistemas corporativos.
Esta política abrange todos os dados, sistemas, bancos de dados, documentos, arquivos e ativos digitais mantidos pela empresa, inclusive aqueles armazenados em nuvem ou geridos por terceiros.

10.1 Princípios Gerais

• As operações de backup devem assegurar confidencialidade, integridade, disponibilidade e autenticidade (CIAA) das informações.
• Todos os procedimentos devem estar alinhados à legislação brasileira, incluindo a Lei Geral de Proteção de Dados (LGPD), principalmente no que tange à finalidade e retenção mínima necessária.
• Os backups devem contemplar dados operacionais, financeiros administrativos, estratégicos e dados pessoais.

10.2 Escopo do Backup

Devem ser incluídos nos backups:
• Bancos de dados e sistemas corporativos;

• Aplicações críticas e arquivos essenciais para o funcionamento da empresa;
• Documentos operacionais e administrativos;
• Registros relevantes à conformidade legal, fiscal, contratual e regulatória;
• Logs de auditoria e segurança, conforme períodos mínimos de retenção.
Dados classificados como Sigilosos ou Confidenciais, especialmente dados pessoais sensíveis, devem possuir camadas adicionais de criptografia e restrição de acesso.

10.3 Tipos de Backup

A empresa deve adotar uma estratégia híbrida com diferentes modalidades:
a) Backup Completo
Cópia integral de todos os dados definidos no escopo.
b) Backup Incremental
Copia apenas dados alterados desde o último backup.
c) Backup Diferencial
Copia dados alterados desde o último backup completo.
d) Backup Imutável (WORM)
Proteção avançada contra ransomware e manipulação indevida, evitando alteração ou exclusão por um período pré-definido.

10.4 Periodicidade dos Backups

A periodicidade deve considerar criticidade e necessidade de continuidade:
• Sistemas críticos: mínimo diário.

• Sistemas operacionais e administrativos: diário ou semanal.
• Arquivos gerais e documentos internos: conforme diretrizes da TI e compliance (geralmente diário ou semanal).
• Backups de retenção legal: conforme normas fiscais, contábeis e regulatórias.
A periodicidade deve ser formalizada em um Plano de Backup e Recuperação.

10.5 Localização e Armazenamento dos Backups

Backups devem ser armazenados de forma segura e segregada:
• Local primário: ambiente controlado, protegido e com acesso restrito.
• Local secundário (offsite): armazenamento em local geograficamente distinto para mitigação de desastres.
• Nuvem: provedores com padrões de segurança compatíveis com ISO 27001/27701 e LGPD.
• Utilização de criptografia forte durante armazenamento e transporte.
• Exigência de mecanismos de controle de acesso, MFA e monitoramento.
Mídias físicas (quando utilizadas) devem possuir rastreabilidade e inventário.

10.6 Testes de Recuperação (Restore)

A empresa deve realizar testes periódicos para garantir que os backups são recuperáveis:
• Testes trimestrais ou semestrais de restauração parcial e total.

• Registro formal dos resultados, com evidências e planos de ação.
• Correções imediatas caso sejam identificadas falhas de integridade ou inconsistências.
Sem testes regulares, o backup não é considerado válido.

10.7 Retenção de Dados e Prazos Mínimos

Os prazos de retenção devem observar:
• Necessidade operacional;
• Obrigações legais e regulatórias;
• Requisitos contratuais;
• LGPD (retenção mínima necessária e descarte seguro).

Exemplos (ajustáveis conforme área jurídica):
• Documentos fiscais: 5 anos (ou mais, conforme legislação específica).
• Documentos trabalhistas: 5 a 30 anos (dependendo da natureza).
• Logs de acesso e operações: mínimo de 6 meses a 5 anos, conforme criticidade.
• Dados pessoais devem ser eliminados após atingida a finalidade, salvo:

- obrigação legal;
- contrato;
- legítimo interesse válido;
- defesa judicial.

Todos os prazos devem constar na Política de Retenção e Descarte de Dados da empresa

10.8 Descarte Seguro de Backups

Quando um backup ultrapassar seu prazo de retenção:
• Deve ser destruído de modo irreversível, utilizando métodos seguros (wipe, destruição de mídia, sobrescrita).
• O processo deve gerar registro auditável.
• Dados pessoais devem respeitar as regras da LGPD e ANPD.
Descarte inadequado é considerado falha grave.

10.9 Continuidade de Negócios e Recuperação de Desastres (BCP/DRP)

A empresa deve possuir Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (DRP) contendo:
• procedimentos de restauração de sistemas;
• prioridades de recuperação (RPO e RTO definidos);
• ambientes alternativos de operação;
• responsáveis pela execução;
• comunicação interna e externa em caso de indisponibilidade;
• estratégias de mitigação contra ransomware e ataques severos.
A restauração deve ocorrer conforme criticidade do ativo e tolerância de indisponibilidade estabelecida.

10.10 Responsabilidades

Área de TI / Segurança:
• Executar, monitorar e validar backups.
• Garantir segurança, criptografia e integridade dos dados.
• Registrar e armazenar evidências das rotinas.
• Realizar testes e documentar resultados.

Gestores/Áreas Proprietárias da Informação:
• Definir criticidade dos dados.
• Validar prazos de retenção.
• Cumprir regras da LGPD e comunicar alterações na finalidade.
Usuários:
• Não armazenar dados pessoais ou informações críticas em locais não autorizados (HD pessoal, pendrive, nuvem pessoal).
• Respeitar as políticas de retenção, segurança e uso adequado.

10.11 Penalidades

O descumprimento das normas de backup e retenção configura falta grave, sujeitando o responsável a:
• advertência;
• suspensão;
• desligamento por justa causa;
• responsabilização civil e administrativa (inclusive perante LGPD);
• responsabilização criminal, quando aplicável.

SEGURANÇA EM E-MAIL, COMUNICAÇÃO E MENSAGERIA

Este item estabelece diretrizes para o uso seguro de e-mails corporativos, ferramentas de comunicação interna, aplicativos de mensagens e demais meios de troca de informações, visando proteger dados corporativos, prevenir incidentes e evitar vazamentos de informações, especialmente dados pessoais.

11

11.1 Diretrizes Gerais

• Todos os meios de comunicação corporativos devem ser utilizados exclusivamente para fins profissionais.
• Informações corporativas — especialmente dados pessoais e sensíveis — só podem ser enviadas por meios autorizados e seguros.
• é proibido utilizar e-mail ou mensageria pessoal (Gmail, Yahoo, WhatsApp pessoal etc.) para atividades corporativas.
• toda comunicação deve observar princípios da LGPD, especialmente finalidade, necessidade e segurança.

11.2 Segurança no Uso de E-mail Corporativo

• O envio de informações confidenciais, sigilosas ou contendo dados pessoais deve ser realizado com criptografia, proteção por senha e, quando possível, por canais corporativos específicos.
• É proibido encaminhar documentos da empresa para e-mails externos sem autorização formal.
• A caixa de e-mail é patrimônio da empresa e pode ser auditada conforme legislação e políticas internas.
• É proibido clicar em links suspeitos, abrir anexos desconhecidos ou responder mensagens que levantem suspeita de phishing.
• E-mails devem ser protegidos por MFA sempre que disponível.

11.3 Confidencialidade e Proteção de Dados

• Dados pessoais só podem ser transmitidos se houver base legal e necessidade comprovada.
• Dados pessoais sensíveis devem ter tratamento reforçado:
◦ criptografia;
◦ minimalização;
◦ envio apenas para destinatários autorizados;
◦ registro do compartilhamento quando necessário;
◦ avaliação de risco quando envolver terceiros.
• Blumenpecting statements devem acompanhar comunicações contendo dados protegidos.

11.4 Mensageria Corporativa (Teams, Slack, Workplace, etc.)

• Mensageria corporativa deve ser usada prioritariamente para comunicações internas.
• Grupos devem ser criados somente para fins corporativos e sob supervisão de gestor.
• Não é permitido compartilhar arquivos confidenciais em grupos abertos.
• Logs, conversas e arquivos enviados podem ser monitorados conforme políticas internas.

11.5 Aplicativos de Mensagens Instantâneas WhatsApp Business, Signal, Telegram – quando autorizados)

• O uso de aplicativos de mensagens pessoais para assuntos corporativos é proibido, exceto quando previamente autorizado.

• Para WhatsApp Business ou equivalente autorizado pela empresa:
◦ não enviar informações sensíveis sem proteção adequada;
◦ não encaminhar listas, bases de dados, documentos estratégicos ou dados pessoais sem criptografia;
◦ conversas comerciais devem ser mantidas nos canais oficiais e,
◦ quando necessário, registradas em sistemas internos;
◦ participar de grupos apenas se relacionados à atividade corporativa.
• Backup automático deve seguir regras de segurança da empresa.

11.6 Comunicação com Terceiros

• Envio de documentos e dados a fornecedores, clientes, parceiros ou órgãos públicos deve seguir protocolos de segurança definidos pela área jurídica e tecnológica.
• Sempre que envolver dados pessoais, o compartilhamento deve ser:
◦ registrado;
◦ limitado ao mínimo necessário;
◦ protegido por controle técnico;
◦ amparado por contrato com cláusulas de proteção de dados e confidencialidade.
• É proibido enviar documentos sem verificação prévia dos destinatários.

11.7 Prevenção a Fraudes e Phishing

• A empresa deve manter mecanismos contra spam, phishing, spoofing e engenharia social.
• Usuários devem:
◦ verificar endereços de remetentes;

11.8 Registro, Monitoramento e Auditoria

• Todas as comunicações corporativas podem ser registradas e monitoradas, respeitando legislação vigente e direitos do colaborador.
• Logs referentes à comunicação devem ser armazenados conforme Política de Retenção e Descarte de Dados.
• A empresa poderá utilizar ferramentas de DLP (Data Loss Prevention) para prevenir vazamento de informações.

11.9 Responsabilidades dos Usuários

• Manter sigilo e confidencialidade de todas as informações acessadas.
• utilizar apenas canais corporativos aprovados.
• reportar incidentes, mensagens suspeitas e acessos indevidos.
• proteger dispositivos utilizados para comunicação (senha, antivírus, atualização).
• cumprir integralmente esta Política e demais normativos.

FORNECEDORES E TERCEIROS

A relação com fornecedores, parceiros, prestadores de serviços e terceiros deve observar rigorosos padrões de segurança e privacidade, considerando que esses agentes podem ter acesso a dados corporativos e dados pessoais.

12

12.1 Avaliação Prévia (Due Diligence)

Antes da contratação, a empresa deve realizar avaliação estruturada que contemple:
• Requisitos técnicos de segurança da informação.
• Capacidade de proteção de dados pessoais conforme LGPD.
• Histórico de incidentes ou vulnerabilidades de segurança.
• Políticas internas de compliance, ética e governança do fornecedor.
• Necessidade real de acesso a dados e nível de criticidade.

12.2 Contratos, Cláusulas e Obrigações

Todo fornecedor deve firmar contrato contendo:
• Cláusulas de proteção de dados (LGPD), incluindo responsabilidades, obrigações, bases legais e regras de tratamento.
• Acordo de confidencialidade (NDA) com cláusulas reforçadas para dados sensíveis e informações estratégicas.
• Regras de segurança mínima: criptografia, controle de acesso, prevenção a vazamento, política de senhas, etc.
• Obrigação de notificar incidentes de segurança ou violações de dados em prazo razoável.
• Previsão de sanções contratuais pelo descumprimento das obrigações.

12.3 Gestão Contínua de Terceiros

Após a contratação, a empresa deve:
• acompanhar o cumprimento dos padrões de segurança.

• realizar auditorias, avaliações periódicas ou comprovações exigidas contratualmente.
• reavaliar o nível de acesso concedido e realizar ajustes quando necessário.
• revogar imediatamente acessos ao término da relação contratual.

TREINAMENTO E CONSCIENTIZAÇÃO

13

A empresa deve promover um programa contínuo de educação em segurança da informação e proteção de dados, visando criar cultura de segurança entre colaboradores, terceiros e parceiros.

13.1 Conteúdos Obrigatórios

Os treinamentos devem abordar, no mínimo:
• Segurança da Informação e controles internos.
• Boas práticas digitais e prevenção a ataques cibernéticos.
• Proteção de dados pessoais (LGPD), princípios e responsabilidades individuais.
• Prevenção a fraudes, phishing, engenharia social e golpes digitais.
• Segurança física e proteção patrimonial.

13.2 Abrangência

• Treinamentos são obrigatórios para todos os colaboradores, terceiros e prestadores com acesso às informações da empresa.
• Novos colaboradores devem ser treinados no momento da integração (onboarding).
• Reciclagens devem ocorrer de forma periódica ou sempre que houver alterações nas políticas internas.
13.3 Registro e Controle
• A empresa deve manter registros formais de participação e frequência.
• A ausência injustificada poderá gerar sanções internas.

MONITORAMENTO, REGISTROS E AUDITORIA

14

A empresa poderá monitorar, auditar e registrar acessos, operações e atividades relacionadas aos seus sistemas, dispositivos e informações, conforme legislação vigente e princípios da transparência e proporcionalidade.

14.1 Finalidades do Monitoramento

O monitoramento será realizado exclusivamente para:

• Garantia da segurança da informação.
• Prevenção e resposta a incidentes de segurança.
• Cumprimento de obrigações legais, regulatórias e contratuais.
• Investigações internas autorizadas.
• Preservação do patrimônio e reputação da empresa.

14.2 Tipos de Registros

Podem ser coletados e analisados:
• Logs de acesso e autenticação.
• Tráfego de rede corporativa.
• Utilização de sistemas, dispositivos e ferramentas.
• Downloads, uploads e compartilhamentos de arquivos.
• Eventos de segurança e alertas de ferramentas de proteção (DLP, firewall, antivírus, SIEM).

14.3 Conformidade Legal e Privacidade

• Todos os registros serão tratados conforme a LGPD, observando princípios de finalidade, necessidade e segurança.
• Logs e dados de monitoramento serão acessados apenas por profissionais autorizados.
• O período de retenção seguirá a Política de Gestão Documental e normas aplicáveis.

15 SANÇÕES E RESPONSABILIDADES

O descumprimento desta Política constitui falta grave e poderá resultar em responsabilização administrativa, civil e penal.

15.1 Sanções Internas

Conforme normas internas e legislação aplicável, o infrator poderá ser submetido a:

• Advertência verbal ou escrita.
• Suspensão disciplinar.
• Rescisão contratual por justa causa (empregados).
• Cancelamento de credenciamento (terceiros).

15.2 Responsabilidade Jurídica

O colaborador ou terceiro poderá responder:
• Civilmente, por danos praticados à empresa, a clientes ou a titulares de dados.
• Administrativamente, nos termos da LGPD e normas aplicáveis.
• Penalmente, quando a conduta configurar crime.

16

DISPOSIÇÕES FINAIS

• Esta Política poderá ser revista, ampliada ou atualizada a qualquer momento, conforme evolução tecnológica, normativa ou necessidade interna.
• Versões atualizadas serão divulgadas nos canais oficiais corporativos.
• Todos os colaboradores, terceiros, estagiários e prestadores devem aderir formalmente à Política no ato da contratação, vínculo ou credenciamento.
• Casos omissos serão analisados pela área Jurídica, Compliance e Segurança da Informação.

CONTROL 361°

2025/2026