



POLÍTICA DE TI

INGÁ Soluções Corporativas LTDA.

atendimento@inga.srv.br

Tel.: (11) 3390-3620

<http://inga.srv.br/>



POLÍTICA DE TI

A Política de Tecnologia da Informação é o documento que orienta e estabelece as diretrizes corporativas da **INGÁ Soluções Corporativas Ltda** para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

1. OBJETIVO

Estabelecer diretrizes que permitam aos colaboradores seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da **INGÁ Soluções Corporativas Ltda** quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. ABRANGÊNCIA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

3. DAS RESPONSABILIDADES

• DOS COLABORADORES EM GERAL

- I. Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.
- II. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **INGÁ Soluções Corporativas Ltda** e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.



INGÁ Soluções Corporativas Ltda
CNPJ 05.937.794/0001-38

- **DOS GESTORES DE PESSOAS E/OU PROCESSOS**

- I. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- II. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política.
- III. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **INGÁ Soluções Corporativas Ltda**. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

4. DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

- I. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- II. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- III. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política.
- IV. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- V. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a INGÁ Soluções Corporativas Ltda.
- VI. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
- VII. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custo diante.



- VIII. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- IX. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
 - os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.
- X. Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- XI. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- XII. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.
- XIII. Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- XIV. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- XV. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- XVI. Monitorar o ambiente de TI, gerando indicadores e históricos de:
- uso da capacidade instalada da rede e dos equipamentos;
 - tempo de resposta no acesso à internet e aos sistemas críticos;
 - períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
 - incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
 - atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);



5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta políticas a INGÁ Soluções Corporativas Ltda poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da diretoria;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

6. CORREIO ELETRÔNICO

É proibido aos colaboradores o uso do correio eletrônico da INGÁ Soluções Corporativas Ltda:

- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a INGÁ Soluções Corporativas Ltda vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a INGÁ Soluções Corporativas Ltda estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
 - Vise vigiar secretamente ou assediar outro usuário;
 - Vise acessar informações confidenciais sem explícita autorização do proprietário;
 - Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
 - Inclua imagens criptografadas ou de qualquer forma mascaradas;
 - Tenha conteúdo considerado impróprio, obsceno ou ilegal.

7. INTERNET

Todas as regras atuais da INGÁ Soluções Corporativas Ltda visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a



INGÁ Soluções Corporativas Ltda
CNPJ 05.937.794/0001-38

internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

8. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na INGÁ Soluções Corporativas Ltda, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.



INGÁ Soluções Corporativas Ltda
CNPJ 05.937.794/0001-38

9. DISPOSIÇÕES GERAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da INGÁ Soluções Corporativas Ltda. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

São Paulo, 15 de janeiro de 2016

CEO - Edmilson José Marchesotti
Ingá Soluções Corporativas Ltda.