

POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

Versão Atualizada: 1.0.0 - novembro/2023

POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

Objetivo

O objetivo da Política de Segurança da Informação e Confidencialidade é fortalecer a segurança da IAAS CONSULTORIA E SERVIÇOS LTDA (“IAAS”), garantindo a proteção, privacidade, integridade, disponibilidade e confidencialidade das informações sob sua propriedade e/ou guarda.

A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a IAAS (“Colaboradores”).

Responsabilidades

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de *Compliance*.

Informações Confidenciais

São consideradas “Informações Confidenciais” aquelas não disponíveis ao público, que:

- identifiquem dados pessoais ou patrimoniais (da IAAS ou de clientes);
- sejam objeto de acordo de confidencialidade celebrado com terceiros;
- identifiquem ações estratégicas – dos negócios da IAAS ou de seus clientes;
- todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da IAAS, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;
- sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória; e que o Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás), que são de uso pessoal e intransferível.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais: (i) mediante prévia autorização do Diretor de *Compliance*, (ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, bem como (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de *Compliance* acerca da possibilidade de compartilhamento da Informação Confidencial.

Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na IAAS:

Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando for de fato necessário;

Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da IAAS:

- as informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- a informação deve ser utilizada apenas para os fins sob os quais foi coletada;
- a concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;
- a identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- segregação de equipamentos e informações comuns, quando aplicável;
- a senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação deve ser reportado ao Diretor de *Compliance*.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros e, se necessário, da assessoria jurídica da IAAS.

A informação deve receber proteção adequada. Em caso de dúvida, o Colaborador deverá consultar o Diretor de *Compliance*.

Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na IAAS são de sua propriedade exclusiva.

A IAAS poderá, a qualquer momento, mediante prévia aprovação do Diretor de *Compliance*, e sem obrigação de aviso prévio:

- inspecionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários;
- disponibilizar esses recursos a terceiros, caso entenda necessário;
- solicitar aos usuários justificativas pelo uso efetuado.

O Diretor de *Compliance* pode definir bloqueio a sites caso necessário. O monitoramento pode ser feito sem necessidade de prévia ciência dos Colaboradores.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à IAAS.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da IAAS, mediante segregação física e lógica.

Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação e Backups

Os riscos e incidentes de segurança da informação devem ser reportados ao Diretor de Tecnologia, que adotará as medidas cabíveis.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de *Compliance* deverá ser imediatamente comunicado, para a tomada das medidas cabíveis.

Política de Segregação de Atividades

O bom uso de equipamentos e informações comuns é obrigatório para todos os funcionários.

Em atendimento ao art. 21 da Resolução CVM nº 19, caso a IAAS venha um dia a exercer outras atividades, ela o fará adotando procedimentos relativos: (i) à segregação das atividades, com o objetivo de demonstrar a total separação entre a área responsável pela atividade de consultoria e as das demais atividades exercidas; (ii) confidencialidade, definindo as regras de sigilo e conduta adotadas, com detalhamento das exigências cabíveis, no mínimo, para os seus sócios, administradores, colaboradores e empregados.

Todas as boas práticas aplicáveis a Segurança de Informação devem ser observadas, garantindo a confidencialidade de Informação de clientes, da empresa, de parceiros de negócios, fornecedores, colaboradores, sócios, etc.

Como regra geral, os Colaboradores detentores de Informações Confidenciais, em função de seu cargo ou função, devem estabelecer barreiras de acesso a dados e informações pelos demais colaboradores cujo acesso seja dispensável.

Essas barreiras servem para atender diversos propósitos, incluindo a conformidade com leis e regulamentos que governam o tratamento e a utilização de certos tipos de informações, evitar situações que possam suscitar um potencial conflito de interesses e coibir má utilização de dados e/ou informações.

Esta norma é parte integrante das normas que guiam as relações entre a IAAS e seus colaboradores, os quais, ao assinar o termo específico do Código de Ética, concordam absolutamente com as suas diretrizes nela fixadas. A desobediência a qualquer uma das normas aqui expostas é tida como infração contratual, sujeita o seu autor às sanções cabíveis.

3. IAAS - POLITICA DE SEGURANCA DA INFORMACAO.pdf

Documento número #3a07beaf-92a8-4f63-8f17-7348d8b7e5f6

Hash do documento original (SHA256): 15fe55e61cafd6bacf02746c1170adf4fb3761e2ef211d50c85eac829ffedf1f

Assinaturas

✓ **Patricia Lima**
CPF: 221.045.928-10
Assinou em 03 jan 2024 às 07:53:13

✓ **José Eduardo Ribeiro Brazuna**
CPF: 166.172.988-61
Assinou em 02 jan 2024 às 17:41:51

Log

- 02 jan 2024, 17:40:13 Operador com email jbrauna@iaasbr.com na Conta de420201-c03f-4c2d-998c-8337959eaa75 criou este documento número 3a07beaf-92a8-4f63-8f17-7348d8b7e5f6. Data limite para assinatura do documento: 01 de fevereiro de 2024 (17:39). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
- 02 jan 2024, 17:40:13 Operador com email jbrauna@iaasbr.com na Conta de420201-c03f-4c2d-998c-8337959eaa75 adicionou à Lista de Assinatura: plima@iaasbr.com para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Patricia Lima.
- 02 jan 2024, 17:40:13 Operador com email jbrauna@iaasbr.com na Conta de420201-c03f-4c2d-998c-8337959eaa75 adicionou à Lista de Assinatura: jbrauna@iaasbr.com para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo José Eduardo Ribeiro Brazuna e CPF 166.172.988-61.
- 02 jan 2024, 17:41:51 José Eduardo Ribeiro Brazuna assinou. Pontos de autenticação: Token via E-mail jbrauna@iaasbr.com. CPF informado: 166.172.988-61. IP: 177.32.137.254. Localização compartilhada pelo dispositivo eletrônico: latitude -23.5832488125 e longitude -46.7289823125. URL para abrir a localização no mapa: <https://app.clicksign.com/location>. Componente de assinatura versão 1.704.2 disponibilizado em <https://app.clicksign.com>.
- 03 jan 2024, 07:53:13 Patricia Lima assinou. Pontos de autenticação: Token via E-mail plima@iaasbr.com. CPF informado: 221.045.928-10. IP: 190.119.55.74. Localização compartilhada pelo dispositivo eletrônico: latitude -13.517206038026044 e longitude -71.97526897490795. URL para abrir a localização no mapa: <https://app.clicksign.com/location>. Componente de assinatura versão 1.704.2 disponibilizado em <https://app.clicksign.com>.

03 jan 2024, 07:53:13

Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 3a07beaf-92a8-4f63-8f17-7348d8b7e5f6.

**Documento assinado com validade jurídica.**

Para conferir a validade, acesse <https://validador.clicksign.com> e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.

As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 3a07beaf-92a8-4f63-8f17-7348d8b7e5f6, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.