# Política Interna de Segurança e Privacidade de Dados

## 1. Exposição de motivos

A proteção das informações da empresa é necessária para o sucesso de nossos negócios, e a proteção de dados, especialmente os dados pessoais, é vital para a construção de uma sociedade mais digna, composta por cidadãos conscientes de seus direitos e dos direitos dos outros.

Pensando nisso, e em conformidade com as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), estabelecemos esta Política Interna de Segurança e Privacidade de Dados como parte de um sistema interno de segurança da informação que engloba todos os processos necessários para identificar as informações que precisamos proteger o meio adequado para protegê-las, melhorias em nossos sistemas e fortalecimento da cultura de privacidade de dados junto ao nosso time de consultores e parceiros.

Além disso, temos consciência de que as necessidades da sociedade se encontram em constante mudança, reconhecendo então que quaisquer processos de segurança existentes devem ser continuamente aprimorados para atender à demanda social, o que inclui as nossas condutas e processos, que são regularmente revisados.

## 2. Objetivos

É objetivo desta Política de Segurança garantir que:

- As informações estarão acessíveis apenas a pessoas autorizadas e necessárias à operação de tratamento, dentro ou fora da empresa;
- A confidencialidade das informações é primordial e sempre será mantida;
- A integridade das informações será mantida durante todo o processo;
- A equipe entenderá que a conformidade com esta Política é obrigatória e que a não observância desta condição implicará na responsabilização pessoal, por previsão legal;
- Todas as violações à segurança da informação e suspeitas de vulnerabilidades serão relatadas e investigadas;
- Existem e existirão procedimentos técnicos para apoiar a Política;
- Todos os gestores são diretamente responsáveis por implementar a Política e garantir a conformidade da equipe em seus respectivos setores.
- O DPO é responsável por garantir a manutenção da Política em toda a corporação, devendo fornecer o suporte e os conselhos necessários a toda a equipe.

## 3. Da condição vinculante desta Política de Segurança e Privacidade de Dados

Todos os procedimentos e normas de conduta estabelecidos nesta Política deverão ser estritamente observados e praticados por todos os consultores.

A despeito de todas as outras formas de comunicação da presente Política, que ocorreram e ocorrerão, a partir do momento em que esta foi disponibilizada no ambiente virtual interno da empresa (Intranet), tornou-se pública, acessível e obrigatória a todos os consultores, os quais adquiriram plena consciência de sua condição vinculante e da inafastabilidade de sua aplicação enquanto perdurar a relação empregatícia ou a prestação de serviços.

Desse modo, o consultor que deixar de observar quaisquer das normas aqui definidas, fica ciente de que tal conduta implicará na adoção, pela empresa, das seguintes medidas administrativas:

- Descredenciamento da senha pessoal de acesso à internet;
- Suspensão temporária de acesso aos recursos informatizados definidos no item 4 desta política;
- Dependendo da gravidade da conduta, poderá acarretar o encerramento do contrato de trabalho ou prestação de serviços do consultor.

Além disso, o consultor fica ciente também de que sua conduta poderá implicar na aplicação, por parte da Autoridade Nacional de Proteção de Dados, das sanções administrativas previstas na LGPD, além de responsabilização civil e, se for o caso, criminal, nos termos da lei – sendo que, nestes casos, a empresa não possui poder decisivo e não poderá intervir.

## 4. **Da aplicabilidade das normas**

As regras aqui definidas se aplicam a acessos externos e internos, navegação na *internet*, acesso e troca de *e-mails*, acesso à rede interna, mensagens instantâneas, softwares de troca de arquivos, voz

e mensagens de texto, softwares de gestão de negócio e demais recursos informatizados que possam ser utilizados.

Todos os recursos informatizados deverão ser utilizados exclusivamente com vistas ao negócio da empresa, sendo vedada a sua utilização para quaisquer outros fins.

Em caso de dúvidas, a equipe de segurança e o DPO da empresa se encontram à disposição para prestar esclarecimentos e auxílio técnico.

## 5. Procedimentos de segurança da informação

### *5.1 Autenticação*

A autenticação nos sistemas de informática será baseada em um sistema de senhas. Esse meio foi escolhido por sua simplicidade para utilização pelos usuários e por sua eficácia.

Outra forma de autenticação utilizada juntamente com o sistema de senhas é a autenticação em nível de rede. Dentro da empresa, todos os serviços que suportam a validação do IP de origem estão configurados soment e para autorizar acesso a partir das nossas redes internas.

### 5.2 *Política de senhas*

Uma senha segura deverá conter no mínimo 8 (oito) caracteres alfanuméricos (letras maiúsculas, minúsculas e números, sendo obrigatório ao menos um elemento de cada).

Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, caneta) datas (11092001) são extr emamente fáceis de descobrir e não devem ser utilizadas.

Para facilitar a memorização das senhas, o usuário deverá utilizar padrões mnemônicos. Por exemplo:

- “eSus6Cres” (eu Sempre uso 6 Caracteres);
- “odIamp0709” (ouviram do Ipiranga as margens plácidas 7 de se tembro);
- “s3Nh45d4t4” (A palavra senha onde o 3 substitui o E, o 4 substi tui o A e o 5 substitui o S).

As senhas terão um tempo de vida útil de, no máximo, 90 (noventa) dias, devendo tal
prazo ser respeitado, caso contrário o usuário ficará sem acesso aos s istemas. Será mantido um histórico das últimas 3 (três) senhas, não podendo estas serem reutilizadas pelo usuário.

No caso de novos consultores, quando do primeiro acesso do consultor à estação de trabalho e aos respectivos sistemas, durante a integração, o sistema exigirá que o consultor proceda à alteração da senha *default*.

Boas Práticas:

- A senha do
usuário jamais deve ser repassada, nem mesmo para a equipe de Infr aestrutura. Caso desconfie que sua senha não está mais segura, o usuário deve alterá-
la, mesmo antes do prazo determinado de validade;
- Tudo que for executado com a senha do
usuário será de sua responsabilidade, por isso o usuário deverá tomar todas as precauções possíveis para manter sua senha secreta.

*5.3 Solicitação de acessos e liberações*

As solicitações de liberação ou bloqueio de acessos (a fim de viabilizar ou facilitar os processos internos) devem ser encaminhadas à central

de serviços (Service Desk) onde o incidente/solicitação de acesso será devidamente registrado, categorizado e posteriormente encaminhado para a equipe de Infraestrutura, que irá avaliar e realizar a liberação/bloqueio de acesso.

Para terceiros, visitantes e outros a solicitação de acesso deverá ser feita aos(às) recepcionistas e secretários(as) da empresa, que liberarão acesso à rede de visitantes – que provê acesso restrito.

*5.4 Política de e-mail*

Para comunicações que envolvem assuntos de interesse da empresa, devem ser utilizados os e-mails corporativos definidos previamente pela equipe de Infraestrutura para cada usuário e/ou setor.

Na utilização dos e-mails corporativos, devem ser observadas as seguintes regras:

- Anexos com as extensões .bat, .exe, .src, .lnk e .com não devem ser abertos se o usuário não tiver certeza de que o e-mail é legítimo;
- O usuário deve desconfiar de e-mails com assuntos estranhos;
- O usuário não deve encaminhar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, nem tratar qualquer tipo de assunto que não seja relacionado aos interesses da empresa pelo e-mail corporativo;
- Não devem ser enviados e-mails para mais de 20 (vinte) destinatários de uma vez só (to, cc, bcc);
- Anexos muito grandes devem ser evitados. Caso seja necessário envio de arquivos, deve ser utilizado o FTP disponibilizado pela Infraestrutura.

- O usuário deve evitar replicações desnecessárias de e-mails com muitas tramitações.

*5.5 Política de Acesso a recursos da Internet*

O padrão de todas as conexões a partir da rede interna com destino à internet é bloqueado. Todas as policies de firewall estão configuradas como bloqueadas. Todos os acessos necessários a partir da rede interna para a internet devem ser solicitados formalmente para que seja registrado, formalizado e posteriormente liberado pela Infraestrutura.

Para utilização das VPNs estabelecidas entre a empresa e seus clientes, também deverá ser solicitado o acesso para que seja registrado, categorizado e posteriormente realizada a liberação pela área de Infraestrutura. Tal norma permite à empresa ter certeza de que somente os consultores designados a determinado projeto tenham acesso ao ambiente do cliente.

O uso recreativo da internet não deverá ocorrer no horário de expediente.

Somente a navegação de sites liberados é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de Infraestrutura com prévia autorização do supervisor do departamento local.

O acesso a sites com conteúdo adulto, jogos, apostas e assemelhados é proibido, bloqueado e monitorado pela equipe de Infraestrutura.

Reforça-se que o uso da internet será auditado constantemente e o usuário poderá ser instado a prestar contas de seu uso. Os relatórios de todos os acessos realizados pelos usuários internos serão

armazenados por um período de seis meses, e poderão ser disponibilizados aos gestores dos setores, caso solicitem.

*5.6 Aplicativos de mensagens instantâneas*

Aplicativos de mensagens instantâneas (p. ex.: *Whatsapp*, *Skype* e similares) não devem ser utilizados como **meio oficial** de troca de informações. O meio oficial definido pela empresa para esse fim é o e-mail corporativo, o que deve ser respeitado.

Os aplicativos de mensagens instantâneas podem ser utilizados para comunicações rápidas e sem conteúdo muito relevante. Eventualmente, caso ocorra a troca de dados pessoais por esses aplicativos (uma vez que não há como controlar o recebimento), os dados deverão ser salvos no ambiente correto (em geral, nos diretórios) e **excluídos** do aplicativo.

Quando for necessário o envio de conteúdo (documentos, informações, etc.) que contenha dados pessoais, sempre deve ser utilizado o e-mail corporativo de cada setor.

Comunicações que contenham definições importantes, ainda que não contenham dados pessoais, devem sempre ser tratadas por e-mail.

*5.7 Política de uso de estação de trabalho*

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada usuário possui sua própria estação d e trabalho. Isso significa que tudo que venha a ser executado em cada estação de trabalho será de responsabilidade do usuário. Por esse motivo, sempre que sair de sua estação, o usuário deve se certificar de que efetuou *logoff* ou bloqueou o console.

Além disso, o usuário deverá observar as seguintes normas de utilização da estação de trabalho:

- Não instalar nenhum tipo de software/hardware sem a autorizaç ão e supervisão da equipe de Infraestrutura;
- Não salvar em sua estação de trabalho músicas, filmes, fotos, softwares, entre outros que configurem violação a direitos /pirataria;
- Manter salvo em sua estação somente o que for supérfluo ou pe ssoal. Todos os dados relativos ao desenvolvimento de suas funções na empresa devem ser mantidos no servidor, onde existe um sistema de backup diário;
- Caso haja dúvidas sobre como proceder, solicitar esclarecimentos da equipe de Infraestrutura.

*5.8 Política de Uso de Equipamentos Pessoais no Ambiente de Trabalho:*

A **Política de Uso de Equipamentos Pessoais no Ambiente de Trabalho** é uma política própria que regulamenta a utilização de equipamentos particulares dos consultores para desempenho das atividades funcionais.

A referida política é obrigatória e será apresentada a todos os consultores que utilizem ou queiram utilizar suas máquinas particulares para realizar suas atividades de trabalho, mediante assinatura de termo de responsabilidade.

*5.9 Documentação na rede (acesso a arquivos)*

Todos os tipos de arquivos criados e modificados dentro da estrutura da empresa e que contenham informações da empresa, principalmente dados pessoais, devem ser salvos exclusivamente na estrutura de diretórios/repositórios (conforme mapeamento definido para cada setor), que é mapeada e passa por backups diários.

Os arquivos não devem ser mantidos em outros ambientes (p. ex.: área de trabalho, pasta de *downloads* ou outras pastas salvas no HD da máquina, etc.) fora da estrutura oficial da empresa, uma vez que estariam suscetíveis a perdas ou outros incidentes de segurança. A inobservância destas disposições será de responsabilidade do próprio usuário, não cabendo ao setor de Infraestrutura a recuperação de arquivos em caso de perda ou manutenção de equipamentos.

Somente devem ser salvos arquivos que sejam de interesse da empresa para o desempenho das atividades funcionais. Todos os arquivos devem conter no seu rodapé a fonte dos dados.

*5.10 Revisão de arquivos*

Periodicamente, deve ser realizada a revisão dos arquivos dos setores, em meio físico e digital, a fim de promover a eliminação de dados cujo armazenamento já não se justifica em razão do alcance da finalidade específica para o qual foram coletados, observadas as obrigações legais ou regulatórias de manutenção de tais informações durante os prazos determinados por lei.

Em caso de dúvidas sobre a necessidade ou não de manutenção de determinadas informações, os representantes dos setores sempre poderão recorrer ao DPO.

*5.11 Utilização do controlador de versão*

Para o setor de desenvolvimento da empresa, é disponibilizado o software para controle de versões. O controle de acesso a este software está integrado com autenticação do Active Directory.

O acesso ao repositório é limitado aos técnicos que estão trabalhando no projeto, desta forma somente os técnicos incluídos em determinado projeto podem acessar, gravar ou ler fontes, documentos e arquivos do controlador de versões.

Para realizar a liberação, alteração ou revogação de acesso a projetos dentro do controlador de versão, é necessário o registro de solicitação formal para a central de serviços (Service Desk), para que o chamado seja categorizado e posteriormente encaminhado à área de Infraestrutura para efetuar a configuração de acesso.

*5.12 Vírus e códigos maliciosos/Antivírus:*

Todas as máquinas instaladas pelo setor de Infraestrutura têm o antivírus configurado para protegê-las quanto a vírus e programas mal-intencionados. O mesmo software de antivírus está configurado para que impossibilite às máquinas copiar arquivos do computador para dispositivos removíveis como pen drives, HDs externos e gravações de CD.

O usuário deverá adotar as boas práticas a seguir sobre cuidados com vírus e softwares maliciosos:

- Manter seu antivírus atualizado. Por padrão, a equipe técnica irá se encarregar dessa tarefa, mas caso o usuário perceba que não foi realizada a atualização ou que, realizada, ela não está funcional, deve entrar em contato com a central de serviços

(Service Desk) por meio de registro de chamado com o relato do incidente;

- Não trazer CDs, HDs externos ou pen drives de fora da empresa. Caso seja extremamente necessário, tais dispositivos devem primeiramente ser encaminhados ao setor de Infraestrutura, a fim de passarem por uma verificação, e somente podem ser utilizados após a liberação de seu uso pela equipe técnica;
- Reportar atitudes suspeitas em seu sistema ao setor de Infraestrutura, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.

*5.13 Outras disposições sobre segurança da informação*

Além de todo o disposto acima, devem ser observadas as seguintes práticas a fim de garantir a segurança da informação dentro da empresa:

- Não falar sobre a Política Interna de Segurança da empresa com terceiros ou em locais públicos;
- Não passar a senha de usuário para ninguém. Nossa equipe técnica jamais irá solicitar aos usuários que informem suas senhas;
- Não digitar as senhas ou informações de *login* em máquinas de terceiros, especialmente fora da empresa. Quando for necessário realizar acesso externo, o usuário deve se certificar de limpar todos os dados/cache do browser;
- Somente aceitar auxílio dos membros de nossa equipe técnica previamente apresentados e identificados;

- Nunca executar procedimentos técnicos cujas instruções tenham chegado por e-mail diferente dos domínios da empresa;
- Relatar à equipe de Infraestrutura pedidos/situações externos ou internos que estejam em desacordo com os tópicos anteriores.

*5.14 Equipe de Infraestrutura*

Os consultores da equipe de Infraestrutura são responsáveis pela implantação e implementação da presente Política, no que tange aos Procedimentos de Segurança. Sendo assim, todos os usuários de quaisquer setores deverão se reportar aos consultores da referida equipe para tratar de assuntos pertinentes a segurança da informação.

## 6. Proteção de dados pessoais e cumprimento da LGPD

*6.1 Das políticas da empresa para proteção de dados*

A Lei nº 13.709/2018, "Lei Geral de Proteção de Dados Pessoais" ou "LGPD" serve para regulamentar o tratamento dos dados pessoais de pessoas físicas, a fim de proteger seus direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento de sua personalidade.

Assim, considerando que a empresa, no exercício de suas atividades, direta ou indiretamente realiza tratamento de dados pessoais, faz-se necessário garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais e com os seus princípios e fundamentos.

Nesse ímpeto, como parte do processo de implementação da LGPD, foi instituído pela empresa um Comitê de Privacidade de Dados, a fim de

garantir a aderência dos processos de todos os setores da empresa à LGPD.

Ainda, foi nomeado um Data Protection Officer (DPO), que é a figura que se encontra à disposição de todos os consultores, permanentemente, para prestar esclarecimentos, capacitar e garantir a correta e segura execução de procedimentos de segurança de dados, e que todas essas ações são estritamente pautadas na Lei Geral de Proteção de Dados.

Isso posto, faz-se necessário esclarecer algumas questões e estabelecer algumas normas internas de proteção de dados.

*6.2 Das operações de tratamento realizadas por consultores em nome da empresa*

Independentemente das orientações e ações educativas sobre a LGPD que serão realizadas até e após a entrada da lei em vigor, todos os consultores devem estar cientes das seguintes situações:

- Ao realizar operações de tratamento de dados em nome da empresa, os consultores são considerados pela lei agentes de tratamento chamados **operadores**;
- Na condição de operadores, os consultores possuem responsabilidades atribuídas pela lei, e respondem solidariamente pelos danos causados pelo tratamento quando descumprirem as obrigações da legislação de proteção de dados ou quando não seguirem as instruções passadas pela empresa.

Desse modo, além do dever de observar todas as normas e procedimentos de segurança estabelecidos nesta Política e demais instruções que a empresa possa fornecer, é dever dos consultores,

também, conhecer a lei: os conceitos básicos apresentados, o que configura e o que autoriza o tratamento de dados pessoais, bem como saber reconhecer o que são dados pessoais e dados pessoais sensíveis, sejam eles de propriedade da empresa ou de terceiros.

Frise-se mais uma vez que, em caso de dúvidas, o consultor deverá buscar o apoio do DPO, que fornecerá orientações sobre como proceder para estar sempre em conformidade com a lei e com as normas da empresa.

Além disso, os consultores devem ter em mente que:

- Todos os dados aos quais tenham acesso e realizem tratamento no exercício de suas funções se encontram sob o domínio da empresa por ocorrência de alguma das hipóteses autorizadoras da LGPD (artigos 7º e 11º), e sob circunstância alguma podem ser tratados para fins secundários, diferentes do objetivo original para o qual o dado se encontra armazenado;
- As operações de tratamento serão rastreadas pela empresa e o consultor que, por ventura, realizar o tratamento de dados pessoais com desvio de finalidade, responderá disciplinarmente no âmbito da empresa, bem como civil e criminalmente – quando for o caso –, na medida dos atos praticados e dos danos causados;
- Os dados deverão ser armazenados em ambiente seguro, vedado o acesso de pessoas não autorizadas e/ou de pessoas que não sejam necessárias ao processo;
- Nesse sentido, nenhuma operação de extração de dados (planilhas, relatórios, e-mails, entre outros) deve ficar disponível em ambiente não seguro (acessível a pessoas não autorizadas), o que significa, também, que nenhum dado poderá ser duplicado ou

distribuído para ambientes de terceiros ou mesmo salvo no computador do próprio consultor, sem uma autorização formal do proprietário dos dados;

- A autorização formal mencionada no item anterior pode ocorrer por meio de um termo próprio, um e-mail, um chamado no Gesti, um projeto com atividade no Service. De todo modo, o importante é que a autorização tenha sido concedida ao consultor diretamente pelo titular do dado ou então pela empresa, e que fique registrada em algum ambiente oficial da empresa;
- Ao perceber qualquer falha de segurança que possa comprometer a conformidade da empresa com os termos da LGPD, o consultor deverá imediatamente comunicar o fato ao DPO e registrar um chamado no Gesti.

*6.3 Do tratamento de dados pessoais dos consultores*

Os consultores da empresa, na condição de pessoas naturais titulares de dados, ficam cientes desde já de que são necessários atos de tratamento de seus dados pessoais pela empresa, para a adequada execução do contrato de trabalho ou de prestação de serviços, a fim de viabilizar o cumprimento de obrigações que estão acima do poder discricionário da empresa, que compreendem mas não se limitam a: obrigações trabalhistas, previdenciárias, fiscais/tributárias, informações ao eSocial, etc.

Tal situação, portanto, enquadra-se na hipótese do artigo 7º, II da LGPD, em que é dispensado o consentimento do titular tendo em vista as obrigações legais e regulatórias impostas à relação de tratamento.

De todo modo, optou-se por agir com máxima transparência, esclarecendo aos consultores que os dados pessoais que disponibilizaram à empresa serão tratados durante toda a vigência do contrato de trabalho ou de prestação de serviços e possivelmente após o seu término, enquanto perdurarem as obrigações legais (art 7º, II) ou houver a possibilidade de ocorrência da hipótese prevista no artigo 7º, inciso VI da LGPD.

Além disso, a empresa se compromete a utilizar os dados pessoais dos consultores EXCLUSIVAMENTE para os fins mencionados neste item da Política (viabilizar o exercício de direitos e cumprimento de obrigações decorrentes do contrato de trabalho/prestação de serviços), bem como se compromete a zelar pela privacidade e segurança de tais informações por meio da adoção de medidas técnicas e jurídicas de segurança de dados.

Caso os consultores tenham qualquer dúvida sobre o tratamento de seus dados, ou desejem solicitar seu acesso, correção, portabilidade ou outras solicitações, poderão entrar em contato com o DPO da empresa, que estará sempre à disposição para prestar orientações e informações.

## 7. **Dependências físicas da empresa.**

A empresa disponibiliza àqueles que julgar adequado, diante da natureza das atividades a serem realizadas, as senhas de alarme, chaves de portas e controles de portões.

A empresa é guarnecida de ferramentas que possibilitam o controle das pessoas que circulam dentro da organização. Todos os ambientes da

empresa possuem câmeras de vigilância com armazenamento de imagens.

Para ambientes nos quais a entrada se faz por código de acesso ou biometria, o cadastro e manutenção deste código de acesso ou biometria deve ser solicitado por meio de registro de chamado que será categorizado e posteriormente encaminhado à equipe de Infraestrutura para realizar o cadastramento.

*7.1 Acesso às salas de servidores e ativos de rede:*

O acesso às salas de servidores e ativos de rede é restrito a pessoas cujas atividades demandem tal acesso, e é controlado por câmeras. As salas de servidores permanecem trancadas 24 horas por dia. Para ter acesso a essas salas, as chave deverão ser solicitadas à equipe de Infraestrutura, que irá acompanhar todos os procedimentos lá realizados.

*7.2 Acesso às salas de arquivo físico (ativo e morto):*

O acesso às salas de arquivo físico também é restrito a pessoas cujas atividades demandem tal acesso. As salas de arquivos ficam trancadas 24 horas por dia. Para ter acesso a essas salas, a chave deve ser solicitada ao departamento responsável pela guarda de chaves.

**8. Vigência e divulgação desta Política Interna de Segurança e Privacidade de Dados**

A presente Política Interna de Segurança e Privacidade de Dados passa a viger a partir da data de 14/08/2020, sendo válida até que uma nova versão seja publicada e venha a substituí-la.

A divulgação desta Política deverá ocorrer da seguinte forma dentro da empresa:

- Disponibilização para acesso de todos os consultores por meio do portal Intranet;
- Divulgação imediata por e-mail, aos consultores, acerca de sua disponibilização na Intranet;
- Cada gestor deverá reforçar à sua equipe a importância da leitura e entendimento do documento;
- Para colaboradores novos, será apresentada durante a integração.