POLÍTICA DE SEGURANÇA E PRIVACIDADE BISO

SUMÁRIO

1. INTRODUÇÃO

A presente Política Interna de Segurança da Informação da Biso (“Política”) dispõe sobre quais medidas de segurança da informação os funcionários da Biso devem seguir para evitar incidentes de segurança relacionados a dados tratados pela empresa por qualquer meio.

Esta versão da Política revisada entrará em vigor a partir de 10 de novembro de 2021, por tempo indeterminado, podendo sofrer revisões/alterações que serão divulgadas tempestivamente.

O conteúdo desta Política pode ser compartilhado com clientes da Biso desde que haja um acordo de confidencialidade devidamente firmado entre as partes.

O não cumprimento das obrigações indicadas nesta Política poderá resultar em ação disciplinar interna. Também poderá significar que o colaborador cometeu uma infração na esfera civil e/ou criminal.

Em caso de dúvidas, favor entrar em contato pelo e-mail privacidade@biso.digital.

2. DEFINIÇÕES

AGENTES DE TRATAMENTO: partes relacionadas à LGPD - Controlador, Operador, ANPD e Titular. **ANPD:** Autoridade Nacional de Proteção de Dados é o órgão regulamentador da LGPD.
COLABORADOR/FUNCIONÁRIO: toda pessoa física, estagiária, CLT ou freelancer que exerça alguma atividade na Biso.
CONTROLADOR: agente de tratamento que define como os dados serão tratados.
DADO CONFIDENCIAL: qualquer informação de acesso restrito que possa causar prejuízo se divulgada de forma indevida. Ex: relatórios de vendas, segredos comerciais, plano de lançamento de produtos ou serviços etc.
DADO PESSOAL: qualquer informação relacionada à uma pessoa natural que a torne identificável. Ex: nome, RG, CPF, e-mail, telefone, endereço etc.
DADO PESSOAL SENSÍVEL: é considerado sensível o dado étnico-racial, filiação a sindicato, órgão religioso, político ou filosófico, dado de saúde ou relacionado à vida sexual do titular, dado genético e/ou biométrico de uma pessoa natural.
INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: um evento adverso relacionado à segurança da informação que traz prejuízos à empresa.
OPERADOR: agente de tratamento terceiro que trata os dados em nome do controlador.
RISCO: probabilidade de impacto ao negócio em caso de incidente de segurança da informação. **TITULAR:** pessoa natural a quem os dados pessoais dizem respeito e cuja relação tenha como objetivo a oferta ou o fornecimento de bens ou serviços.
VULNERABILIDADE: fragilidade de algum sistema ou processo que possa gerar danos a Biso ou a seus clientes.

3. INFORMAÇÕES CONFIDENCIAIS

A classificação de dados é um método de classificação feito de acordo com o risco e a criticidade e seguindo as recomendações de segurança da informação da ISO (International Standards Organization) e do NIST (National Institute of Standards and Technology).

Os dados a serem categorizados podem ser aqueles tratados por meio digital ou físico e independem de sua forma de armazenamento.

As informações tratadas pela Biso deverão ser classificadas e identificadas da seguinte forma:

- Restritas - alto impacto
- Confidenciais ou não classificadas - médio impacto
- Públicas - baixo impacto

Classificação

I. Restritas

As informações restritas são informações internas relacionadas à Biso e de acesso restrito a um grupo de funcionários específico, não podendo, de forma alguma, serem compartilhadas com terceiros. Tais informações devem ser armazenadas em ambiente seguro e restrito, para garantir que não haja nenhum incidente de segurança nem que os dados sejam acessados por pessoas não autorizadas.

Caso seja necessário o compartilhamento de dados restritos que o destinatário não possa encaminhar, copiar, imprimir nem fazer o download do e-mail, seja no corpo de um e-mail ou como anexo, é necessário que o autor ative a opção de modo confidencial, que impede que o receptor encaminhe, copie, imprima ou faça o download. Nessa opção, deve ser definido por qual período o e-mail estará disponível e recomenda-se que o e-mail seja acessado mediante senha configurada pelo remetente e enviada automaticamente ao destinatário (acesse o link e saiba mais https://support.google.com/mail/answer/7674059?co=GENIE.Platform%3DDesktop&hl=pt-BR).

II. Públicas

As informações públicas são aquelas que estão em domínio público, não havendo necessidade de proteção ou tratamento específicos.

4. TREINAMENTOS

A Biso têm treinamentos e workshops voltados à privacidade e proteção de dados e os treinamentos são obrigatórios.

- Treinamento LGPD Biso
    - A nota deve ser igual ou superior a 70% para que o colaborador seja aprovado no treinamento
    - Obrigatório

O treinamento acima mencionado deve ser feito pelos novos colaboradores em até 15 dias desde seu primeiro dia de trabalho e os certificados de conclusão e/ou prints comprobatórios de conclusão do treinamento devem ser enviados.

Importante observar que os treinamentos serão atualizados e novos materiais serão compartilhados sempre que necessário.

5. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Incidente de segurança da informação é qualquer evento adverso que viola a segurança de dados tratados. Apesar de a LGPD tratar apenas de dados pessoais, os dados confidenciais tratados pela Biso também devem ser manuseados com segurança adequada, a fim de evitar um incidente de segurança da informação.

O incidente pode ser um acesso não autorizado, acidental e/ou ilícito aos dados tratados e que podem causar danos para seu titular e/ou cliente ou ataques com malware. Destruição, deleção, perda e vazamento são alguns dos tipos de incidentes de segurança da informação que podem ocorrer.

No mais, a LGPD prevê que o Controlador deve notificar a ANPD em até 48h úteis em casos de incidente de segurança da informação com dados pessoais e que o Operador deve notificar o Controlador sempre que houver suspeita de incidente de segurança.

Visto isso, é imprescindível que todo e qualquer colaborador comunique imediatamente para seu gestor e envie um e-mail para o time de privacidade (privacidade@biso.digital), comunicando o ocorrido caso haja suspeita e/ou confirmação de um incidente de segurança da informação.

Nossos clientes e prestadores de serviços também podem entrar em contato com o time de privacidade através do e-mail privacidade@biso.digital para comunicar uma suspeita ou confirmação de incidente de segurança com dados pessoais envolvendo a Biso..

Procedimentos de Resposta a Incidentes

Quando ocorre um incidente, nossa equipe segue um protocolo definido. Primeiramente, identificamos e detectamos imediatamente qualquer atividade suspeita por meio de nossos sistemas de monitoramento.

A resposta é imediata: isolamos o sistema afetado, interrompemos qualquer acesso não autorizado e preservamos evidências. Em seguida, realizamos uma análise detalhada para avaliar o alcance do incidente, investigar suas causas e determinar quais dados foram comprometidos.

Conforme as regulamentações vigentes, notificamos a ANPD em até 48h úteis em casos de incidentes de segurança da informação que envolvam dados pessoais. Além disso, seguimos um processo de comunicação transparente e clara, implementando medidas corretivas para mitigar o impacto do incidente e fortalecer a segurança do sistema. Adicionalmente, o Controlador é notificado sempre que houver suspeita de incidente de segurança, garantindo uma pronta comunicação em todos os estágios do processo.

Após o incidente, revisamos nossos procedimentos de segurança, identificamos áreas para melhorias e documentamos todas as etapas. Essa abordagem nos permite aprender com cada incidente e garantir aprimoramentos contínuos em nossos protocolos de segurança de dados pessoais.

Os incidentes são documentados para incluirmos nos processos de lições aprendidas e de planos de ação, a fim de identificarmos a causa do incidente e reduzirmos as chances de reincidir no problema.

Essa estrutura permite integrar as informações sobre a natureza dos incidentes de segurança, os procedimentos de resposta e a importância da notificação e documentação, mantendo a clareza e a organização do conteúdo.

6. GOVERNANÇA DE REDE

A gestão de acessos restringe o acesso a plataformas, sistemas e/ou documentos corporativos apenas para aqueles que possuem permissão para tal e evita que haja algum incidente de segurança da informação. A liberação e/ou revogação de acessos é feita para todas as plataformas corporativas da Biso (Ex: Google Workspace, Runrun.it, Microsoft Azure e Amazon Web Services) e também plataformas contratadas pelos clientes onde a Biso atua (Ex: VTEX, Shopify, Google Analytics, Google Ads, Facebook Ads, etc).

Solicitação de acesso para colaboradores

Sempre que houver a contratação, movimentação ou demissão de um funcionário, os seguintes passos deverão ser seguidos:

a. Para os casos de admissão de novos funcionários, o gestor imediato deverá solicitar os acessos que o funcionário necessitará para que exerça as atividades a ele designadas;
    i. A solicitação seguirá para aprovação do gestor da área e ciência dos demais gestores.
    ii. Uma vez aprovado, uma tarefa é aberta no Runrun.it para a equipe de Privacidade, que disponibiliza os acessos nas plataformas solicitadas, desde que a gestão dos acessos seja feita pela Biso e que não haja nenhuma inconsistência.

b. Para os casos de alteração de cargo, função e/ou área de um funcionário, o gestor deverá solicitar a revogação dos acessos que o funcionário não irá mais necessitar e a inclusão dos novos acessos que serão necessários para o cumprimento das novas atividades a ele designada;

c. Para os casos de demissão de funcionários, o gestor imediato deverá solicitar a revogação dos acessos dos funcionários.

Suspensão de acessos de ex-colaboradores

O RH deve ser formalmente informado via e-mail sobre o desligamento de um colaborador, para que seja possível abrir uma tarefa no Runrun.it contendo as informações abaixo e designá-la para os times de TI e privacidade:

a. Nome completo;
b. CPF;
c. Data de nascimento;
d. Cargo;
e. E-mail pessoal;
f. Superior hierárquico;
g. Área;
h. Endereço para retirada de equipamentos (se tiver); e
i. Data de desligamento.

Os times de TI e privacidade devem suspender os acessos do colaborador ao Google Workspace da Biso e ao Runrun.it na data do desligamento.

Os colaboradores alocados na tarefa poderão adicionar outros colaboradores das demais áreas para suporte no levantamento de tais informações, a fim de garantir a suspensão dos acessos de forma ágil e efetiva.

7. INDIVIDUALIZAÇÃO DE ACESSOS

Implementamos, de forma gradual, desde 10 de março de 2021, a individualização dos acessos que temos nas plataformas, a fim de garantir uma maior segurança da informação e garantir uma auditoria mais precisa nos logs de acesso.

Como regra, todos os usuários deverão ativar autenticação de 2 fatores (2FA) para acessar toda e qualquer plataforma relacionada à Biso. Todos os acessos são revisados periodicamente e serão suspensos caso não tenha sido implementada a dupla segurança no login.

8. ACESSO REMOTO

Dada a situação de trabalho remoto / home office, a Biso construiu uma arquitetura de rede baseada nos serviços Google Workspace para os serviços de comunicação (Chat, Gmail) e servidor de arquivos (Drive).

Essa prática tem como objetivo garantir a segurança na comunicação realizada entre os funcionários da Biso.

9. COMUNICAÇÃO INTERNA & MESAS LIMPAS

Visando garantir maior segurança de dados trafegados internamente entre colaboradores da Biso, os meios de comunicação interna e compartilhamento de materiais são o Google Workspace (Gmail, Hangouts e/ou Chat) e Runrun.it e devem ser utilizados para tal. Qualquer outro meio de comunicação não homologado pela Biso não deve ser utilizado no que diz respeito ao compartilhamento de dados pessoais e/ou confidenciais.

No atual cenário em que 100% dos colaboradores da Biso estão trabalhando no regime de home office, a Biso orienta que eventuais anotações e/ou materiais impressos deverão permanecer armazenados em local seguro e não sobre mesas de trabalho, bancadas, etc.

Os documentos eletrônicos que os colaboradores produzem no exercício de suas funções e no cumprimento de suas obrigações definidas no contrato de trabalho devem ser salvos nos aplicativos do Google Workspace.

A área de trabalho do computador de trabalho não deve conter nenhum tipo de arquivo, lembretes e/ou notas contendo dados confidenciais (como senhas, por exemplo) ou outro material contendo informações que devem ter seu acesso protegido, exceto os acessos às aplicações necessárias para a execução de suas atividades.

Ao levantar-se do posto de trabalho, deve-se sempre realizar o bloqueio do dispositivo através das teclas Windows + L (equipamentos com Windows) ou Control + Command + Q (equipamentos com OSX).

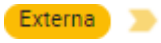
Quando o trabalho for executado no escritório da Biso, deve-se também vigorar uma política de mesas limpas. Todo material impresso/anotações devem ser armazenados em local seguro (como gaveteiros com chave e trancados) após o seu uso

10. GOOGLE WORKSPACE

Os serviços do Google Workspace possuem os certificados de segurança ISO 27001 e SOC 3. Embora os dados possam ser armazenados fora do Brasil, o Google garante a aplicabilidade da LGPD a estes dados, conforme indicado no seguinte link.

A governança do Google Workspace é constantemente aprimorada para que a segurança da informação seja priorizada.

Para evitar o envio de e-mails equivocados, sempre que o destinatário não for de nossa organização, o Gmail deixará o endereço de e-mail destacado. Além disso, todos os e-mails envolvendo pessoas de outro domínio serão sinalizados com a marcação “Externa”ao lado do assunto do email, da seguinte forma:



O ambiente de acesso aos aplicativos do Google Workspace em dispositivos móveis conta com a política básica de Gerenciamento de Dispositivos Móveis do Google.

A partir de dezembro 2021 daremos início a ativação do gerenciamento de computadores e demais dispositivos inteligentes de forma que somente equipamentos aprovados pelo time de TI/Privacidade possam acessar os serviços Google Workspace. A expectativa é 100% dos colaboradores sejam alcançado por essa medida até 31 de dezembro de 2021

Por fim, como medida de segurança da informação, configuramos o armazenamento de e-mails abrangente do Google Workspace. Tal controle possibilita que os administradores possam armazenar cópias de todas as mensagens enviadas ou recebidas em nosso domínio. Apesar de serem armazenados, tais e-mails e demais informações só serão acessados pelo time de privacidade em caso de auditoria, investigação e/ou processo judicial.

Como medidas de segurança, é exigida a autenticação em dois fatores para todos os usuários, assim como uso de senha forte (https://support.google.com/a/answer/139399).

O usuário, desde que tenha acesso à plataforma, pode gerar alguns códigos de verificação de backup e mantê-los em local seguro para utilização caso necessário. Abaixo o procedimento de como fazê-lo:

1. Acesse sua Conta do Google;
2. No painel de navegação à esquerda, clique em “Segurança”;
3. Em "Como fazer login no Google", clique em “Verificação em duas etapas” - talvez seja necessário fazer login;
4. Em "Códigos de backup", clique em “Continuar”;
5. Nessa página, você pode:

   Receber códigos de backup: para adicionar códigos de backup, clique em “Receber códigos de backup”;
   Criar um novo conjunto de códigos de backup e desativar códigos antigos: para criar novos códigos, clique em “Atualizar”;
   Excluir seus códigos de backup: para excluir e desativar automaticamente seus códigos de backup, clique em “Excluir” ;

   Fazer o download dos códigos de backup: clique em “Fazer o download dos códigos” ; e

   Imprimir códigos de backup: clique em “Imprimir” .

O Google Workspace possui uma central de logs e alertas que permite verificar eventos realizados, como compartilhamento de arquivos, por exemplo. Entre os alertas configurados, estão a criação, suspensão e exclusão de usuários, em que o time de privacidade recebe uma notificação a cada ocorrência desses eventos.

11. AMAZON WEB SERVICES

A AWS implementa e mantém medidas de segurança técnica e organizacional aplicáveis a serviços de infraestrutura da Nuvem AWS em estruturas e certificações de garantia de segurança reconhecidas mundialmente, incluindo ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI DSS Level 1 e SOC 1, 2 e 3. Essas medidas de segurança técnica e organizacional são validadas por auditores externos independentes e são projetadas para impedir o acesso não autorizado ao conteúdo de clientes ou a divulgação não autorizada desse conteúdo.

- A política de privacidade completa da AWS pode ser consultada através deste link e link 2.

A Biso usa o ambiente e as ferramentas da AWS para construir e gerenciar toda a infraestrutura do serviço que presta, sempre aplicando as melhores práticas.

12. MICROSOFT AZURE

A Microsoft adere aos princípios da Estrutura de Proteção de Privacidade UE-EUA e Suíça, mas não considera a Estrutura de Proteção de Privacidade UE-EUA como base legal para a transferência de dados pessoais, seguindo decisão do Tribunal de Justiça Europeu no Processo C-311/18.

- A política de privacidade completa do AZURE pode ser consultada através deste link.

A Biso usa o ambiente e as ferramentas do AZURE para construir e disponibilizar relatórios de (POWER BI), que fazem parte do serviço que oferecemos, onde todo e qualquer relatório disponibilizado estará devidamente protegido de acessos não permitidos.

13. ARMAZENAMENTO E TRANSFERÊNCIA INTERNACIONAL DE DADOS

Fazemos uso de tecnologia de ponta e infraestrutura em nuvem, destacando-se Google, Amazon Web

Service e Microsoft. Portanto, as operações de tratamento de dados feitas por nós ou por intermédio de nossos parceiros podem ocorrer no Brasil ou em território estrangeiro. Independente da localização geográfica, essas operações estão de acordo com as práticas descritas neste documento e seguirão as medidas de segurança aqui descritas.

A eventual ocorrência de transmissão internacional dos dados pessoais realizada pelos nossos parceiros será realizada sempre dentro dos limites estabelecidos nesta política e nas legislações de proteção de dados aplicáveis, principalmente na Lei n. 13.709/18 (LGPD).

14. RETENÇÃO DE DADOS

A Biso tem como compromisso primordial o respeito pela privacidade, a proteção e a segurança dos dados pessoais sobre os quais realiza tratamento, motivo pelo qual compromete-se a não reter esses dados por período maior do que o necessário a/ao:

- cumprimento do objetivo para o qual os dados foram originalmente coletados, mantidos e tratados;
- cumprimento de obrigações legais ou regulatórias;
- exercício regular de direitos;
- consecução dos interesses legítimos da Biso.

Visando conferir a máxima transparência ao processo de retenção e descarte dos dados pessoais que trata, abaixo disponibilizamos o período total que os dados são mantidos:

- **Dados extraídos das plataformas do cliente (VTEX, Google Analytics e etc)** - os dados que extraímos das plataformas que o cliente faz uso de seus serviços e mediante a sua autorização, são mantidos pelo período que se rege o contrato entre a Biso e o cliente, ou seja, o período em que o mesmo está fazendo uso dos serviços da Biso.

- **Dados do cliente** - os dados desenvolvidos, usados ou recebidos relacionados a um cliente são mantidos pelo período que se rege o contrato entre a Biso e o cliente, ou seja, o período em que o mesmo está fazendo uso dos serviços da Biso e, até 30 (trinta) dias após a data da rescisão contratual, como está previsto no contrato do cliente. Caso os dados do cliente servirem de suporte aos registros contábeis, as informações devem ser mantidas de acordo com os períodos de retenção dos registros contábeis e, em caso de conflito com o contrato do cliente, os períodos de retenção do registro contábil prevalecerão.

15. CONTROLE DE VERSÕES

VERSÃO	DATA	REDATOR	REVISOR	APROVADOR	OBS.
V 1.0	02/12/2021	Breno Berman	Breno Berman	Breno Berman	
V 1.1	12/09/2022	Jonathan Raphael	Breno Berman	Breno Berman	
V 1.2	06/11/2023	Jonathan Raphael	Breno Berman	Breno Berman	