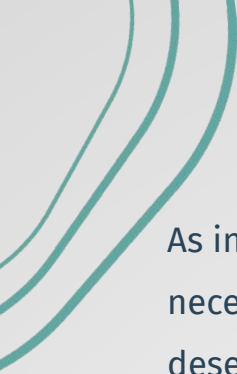


# Política de Segurança da Informação

 Bridg e 3



As informações e os recursos de informação são ativos críticos da Bridge3, necessários para a realização de tarefas, tomada de decisão e desenvolvimento contínuo dos negócios e, por isso, devem ser adequadamente produzidos, adquiridos, utilizados, atualizados, administrados e descartados, de forma segura, independentemente do meio ou forma em que estejam armazenados.

O primeiro passo para a implementação da segurança da informação é a adoção de uma Política de Segurança da Informação (Política), cujo cumprimento depende, principalmente, das ações dos colaboradores e de terceiros, independentemente do nível hierárquico, da Empresa Controlada e da atividade desenvolvida.

Para proteger seus ativos tangíveis e intangíveis, a Bridge3 elaborou esta Política, pautada na legislação nacional vigente, nas melhores práticas do mercado e nos princípios da ética e da transparência, e que deve ser cumprida diariamente por todos.

A CEO da Bridge3 está comprometida com a proteção dos ativos tangíveis e intangíveis e aprova os princípios de Segurança da Informação contidos nesta Política para garantir a confidencialidade, integridade, disponibilidade e autenticidade desses ativos, e o seu uso em conformidade com a legislação pertinente, as necessidades de negócio e contratos estabelecidos.

A segurança das informações e dos recursos de informação da Bridge3 é uma responsabilidade de todos os colaboradores, terceiros de todas as pessoas que se relacionam, direta ou indiretamente, com a Bridge3 e suas empresas controladas.

## **OBJETIVO**

Esta Política tem por objetivo:

- a) Definir os princípios de segurança das informações da Bridge3, a fim de proteger os seus ativos tangíveis e intangíveis;
- b) Servir de fundamento para as diretrizes e processos relacionados à garantia da segurança das informações;
- c) Estabelecer as responsabilidades e limites de atuação dos colaboradores da Bridge3 e de terceiros em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias em conformidade com os objetivos do negócio e requisitos aplicáveis.
- d) Assegurar que todas as informações da organização recebam um nível adequado de proteção, de acordo com sua importância, valor, requisitos legais, sensibilidade e criticidade.
- e) Esta política visa assegurar que a informação receba um nível adequado de proteção, de acordo com sua importância para a empresa, prevenindo modificação ou divulgação não autorizada.

## **ABRANGÊNCIA**

Esta Política é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos colaboradores e terceiros da Bridge3 e de todas as suas empresas controladas, nos âmbitos administrativo (recursos de TIC) e de internet das coisas (recursos de IoT).

## TERMOS E DEFINIÇÕES

- a) Ameaça: Causa potencial de um incidente indesejado que pode resultar em dano à Bridge3.
- b) Ativo: Qualquer coisa que tenha valor para a Bridge3 e precisa ser adequadamente protegido.
- c) Ativo Intangível: Todo elemento que possui valor para a Bridge3 e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à reputação, imagem, marca e conhecimento.
- d) Autenticidade: Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.
- e) Colaborador: Empregado, estagiário, menor aprendiz ou qualquer outro indivíduo que venha a ter relacionamento profissional, direta ou indiretamente, com a Bridge3.
- f) Confidencialidade: Garantia de que as informações sejam acessadas e divulgadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.
- g) Conformidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com os requisitos legais, regulatórios, organizacionais e contratuais.
- h) Dado pessoal: informação relacionada a pessoa natural (física) identificada ou identificável independente do meio em que estiver armazenada.
- i) Dado pessoal sensível: dado pessoal sobre origem racial, etnia, saúde, genética, biometria, e de orientação política, sexual e religiosa.
- j) Disponibilidade: Garantia de que as informações e os recursos de informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.



- k) **Informação:** Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
- l) **Integridade:** Garantia de que as informações estejam completas e fidedignas em relação à última alteração desejada durante o seu ciclo de vida, além de protegida contra alteração ou destruição não autorizada.
- m) **Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.
- n) **Nível de Confidencialidade:** identifica o nível de proteção necessário para as informações, de acordo com a sua natureza e o impacto estimado para a Bridge3 no caso de divulgação indevida:
- **Informações públicas:** são as informações que, por não apresentarem riscos, podem ser distribuídas livremente dentro e fora dos limites físicos e dos Recursos de TIC da Bridge3;
  - **Informações internas:** são informações cuja divulgação a terceiros não autorizados poderia promover desvantagem comercial, questionamento de condições contratuais, ou a boa execução das atividades;
  - **Informações restritas:** são informações cuja divulgação a pessoas não autorizadas poderia promover o comprometimento do sigilo de decisões gerenciais, cobertura em mídia local, o nível de segurança físico e lógico do ambiente corporativo, ou a divulgação indevida de dados pessoais;
  - **Informações confidenciais:** são as informações cuja divulgação a pessoas não autorizadas poderia promover o comprometimento dos objetivos estratégicos da Bridge3 ou de suas empresas controladas, a perda de negócios, cobertura negativa em mídia nacional, afetar de forma negativa no faturamento da Bridge3, ou a divulgação indevida de dados pessoais sensíveis.
- o) **Risco:** Efeito da incerteza sobre os objetivos, verificado pela combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos (consequências).

- p) Recursos de Tecnologia da Informação e Comunicação (recursos de TIC): Hardwares, softwares, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.
- q) Recursos de Internet das Coisas (recursos de IoT): conjunto de recursos de TIC que formam uma rede de objetos que possuem tecnologia embarcada para identificar, comunicar e interagir com seu estado interno ou com o ambiente externo.
- r) Recurso de Informação: é o conjunto de todos os recursos de TIC e IoT.
- s) Segurança da Informação: É a preservação da confidencialidade, integridade, disponibilidade, conformidade e autenticidade da informação. Visa proteger a informação e os recursos de informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.
- t) Tentativa de Burla: Fazer esforços para não respeitar ou tentar violar as diretrizes e os controles estabelecidos nos normativos da Bridge3.
- u) Violação: Qualquer atividade que desrespeite as regras estabelecidas nos normativos da Bridge3.

## **PRINCÍPIOS GERAIS DA SEGURANÇA DA INFORMAÇÃO**

A Bridge3 tem os seguintes princípios gerais de segurança da informação:

- a) Preservar e proteger as informações e os recursos de informação da Bridge3 ou de terceiros, ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça e em todo o seu ciclo de vida, contidas em qualquer suporte ou formato;
- b) Prevenir, monitorar, identificar e responder aos incidentes de segurança da informação, reduzindo os seus impactos e assegurando a confidencialidade, integridade, disponibilidade, autenticidade das informações e a conformidade no uso dos recursos de informação no desenvolvimento das atividades profissionais;
- c) Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação e aos objetivos corporativos, morais e éticos da Bridge3.

As medidas de prevenção e controle adotadas pela Bridge3 visam, em essência, gerenciar e manter os riscos em um nível adequado ao negócio.

### **PROPRIEDADE**

As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os recursos de informação e demais ativos tangíveis e intangíveis disponibilizados, são de propriedade da empresa controlada pela Bridge3 ou, quando de terceiros, estão sob sua guarda e sujeitos às determinações desta Política e documentos normativos que a complementam.

## ESTRATÉGIA DE AÇÃO

A estratégia utilizada para o cumprimento dos princípios de segurança definidos nesta Política é a adoção de um Programa de Segurança da Informação que define os papéis, responsabilidades e as atividades de gestão e de melhoria contínua do nível de Segurança das Informações da Bridge3 e de suas empresas controladas, e também a adoção de ações táticas de segurança que incluem a definição de Diretrizes, padrões, e a implementação de processos e controles para a adequada:

- a) Gestão dos riscos relacionados à falta de segurança das informações e do uso dos Recursos de informação;
- b) Proteção dos ativos tangíveis e intangíveis relacionados às informações e recursos de informação da Bridge3 e de terceiros, de acordo com a sua importância para o negócio e nível de confidencialidade;
- c) Garantia da legalidade e conformidade do uso das informações e recursos de informação;
- d) Proteção da privacidade dos dados pessoais das pessoas que se relacionam com a Bridge3, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo seu tratamento autorizado nos termos da legislação de proteção de Dados Pessoais vigente;
- e) Conscientização e treinamento dos colaboradores e terceiros para o adequado uso das informações e recursos de informação;
- f) Identificação de ameaças, correção de vulnerabilidades e de problemas, e prevenção e resposta a incidentes de segurança da informação;
- g) Gestão de projetos e de mudanças nos recursos de informação e nos processos que os utilizam;
- h) Gestão das operações dos recursos de informação;
- i) Gestão da continuidade das atividades de negócio;
- j) Verificação e monitoramento do uso das informações e dos recursos de informação;



- k) Atuação em caso de violação dos princípios, dos controles estabelecidos e dos normativos da Bridge3;
- l) Monitoramento e a melhoria contínua do nível de segurança das informações;
- m) Plano de workflow.

As ações para a gestão e o uso seguro das informações e dos recursos de informação devem ser aplicadas em todos os empreendimentos e processos corporativos, de forma a garantir alinhamento com o Planejamento Estratégico Empresarial, com os requisitos de negócio, e com a gestão dos riscos às atividades de negócio e à segurança das informações e recursos de informação.

As contratações em que ocorra o compartilhamento de informações de propriedade ou sob a responsabilidade da Bridge3, ou a concessão de acesso aos seus ambientes ou ativos, devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à segurança da informação, além de controles que assegurem o conhecimento e o cumprimento desta Política e demais Diretrizes e processos aplicáveis.

A Bridge3 está em processo de implementação do Microsoft 365, bem como do Microsoft Defender, nos equipamentos de seus colaboradores, de forma que atenda ao NISP SP-800-53 e ao PCI-DSS.

## **GESTÃO DE MUDANÇAS**

Todas as mudanças nos sistemas e processos de TI serão geridas por um processo formal de gestão de mudanças, garantindo que sejam avaliadas, aprovadas e documentadas antes da implementação. As mudanças devem ser testadas em um ambiente controlado para minimizar riscos e impactos na segurança da informação. A comunicação das mudanças deve ser clara e direcionada a todas as partes interessadas relevantes. Revisões pós-implementação devem ser realizadas para assegurar que os objetivos de segurança foram alcançados.

## **GESTÃO DE ACESSO LÓGICO**

O processo formal para a concessão, alteração e exclusão de acessos de usuários aos sistemas e dados da organização, garantindo a segurança e integridade das informações, inclui:

- a) acesso aos sistemas deve ser concedido apenas mediante solicitação formal e aprovação do gestor responsável.
- b) Os acessos devem ser atribuídos com base no princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para suas funções.
- c) Qualquer alteração nos acessos de um usuário deve ser solicitada formalmente e aprovada pelo gestor responsável.
- d) As alterações devem ser documentadas e revisadas periodicamente para garantir a conformidade com as políticas de segurança.
- e) acesso de usuários deve ser revogado imediatamente após a rescisão do contrato de trabalho ou mudança de função que não requeira mais o acesso.
- f) A exclusão de acessos deve ser documentada e verificada para garantir que não haja acessos não autorizados.

Este processo visa proteger os sistemas e dados da organização contra acessos não autorizados, garantindo que apenas usuários autorizados tenham acesso às informações necessárias para suas funções.

## **PAPEIS E RESPONSABILIDADES**


A CEO da Bridge3 tem a responsabilidade de analisar, aprovar e declara formalmente o seu comprometimento com esta Política.

Para o cumprimento desta Política a Bridge3 define o Comitê de Segurança da Informação e Privacidade, formado pelas áreas Tecnologia da Informação, Operação e Administração da Bridge3, que é responsável por:

- a) Manter esta Política atualizada e submetê-la para aprovação do Comitê Executivo da Bridge3;
- b) Garantir que o Comitê de Segurança da Informação e Privacidade seja composto por uma equipe multidisciplinar, tenha atuação permanente, e reúna-se periodicamente;
- c) Definir e manter o Programa de Segurança da Informação da Bridge3;
- d) Promover e realizar a gestão da Segurança da Informação na Bridge3;
- e) Analisar e aprovar, ou não, os pedidos de exceções a esta Política;
- f) Garantir a publicidade e disponibilidade desta Política, e o seu cumprimento através da definição e implementação de documentos normativos, modelos, padrões, processos, controles e recursos necessários para a Segurança da Informação.

A gestora de TI é responsável por coordenar as atividades do Comitê de Segurança da Informação e Privacidade e do Programa de Segurança da Informação da Bridge3.

Os colaboradores da Bridge3 são responsáveis pela adoção desta Política e por definir o responsável pela gestão da segurança da informação nas empresas sob sua responsabilidade.



Os Gestores da Bridge3 e empresas controladas são responsáveis por:

- a) Garantir e gerenciar o cumprimento desta Política e demais documentos normativos pelos colaboradores e terceiros sob sua responsabilidade;
- b) Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de negócio sob sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir o risco ao negócio;
- c) Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por colaboradores e terceiros sob sua responsabilidade, e comunicar eventuais ocorrências à área responsável pela gestão de incidentes de segurança da informação da respectiva empresa controlada.

Os colaboradores da Bridge3 e empresas controladas são responsáveis por estarem cientes, cumprir e manterem-se atualizados com esta Política e demais documentos normativos que a complementem.

## **PROCEDIMENTO PARA INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

Esse procedimento visa garantir uma resposta rápida e eficaz a incidentes de segurança da informação, minimizando impactos negativos e fortalecendo a resiliência da organização.

### **a) Identificação de Incidentes:**

Todos os colaboradores devem estar cientes dos sinais de possíveis incidentes de segurança da informação, como acessos não autorizados, perda de dados ou atividades suspeitas. Qualquer suspeita de incidente deve ser reportada imediatamente ao responsável pela segurança da informação.

### **b) Resposta a Incidentes:**

O responsável pela segurança da informação deve avaliar rapidamente a situação para confirmar se um incidente ocorreu. Medidas imediatas devem ser tomadas para conter o incidente e evitar danos adicionais.

### **c) Ações de Remediação:**

Após a contenção, o responsável deve investigar a causa raiz do incidente e implementar ações corretivas para prevenir recorrências. Documentar todas as etapas do processo de remediação e as lições aprendidas.

### **d) Notificações:**

Se o incidente afetar dados pessoais ou informações sensíveis, as partes afetadas devem ser notificadas conforme exigido por leis e regulamentos aplicáveis, como a LGPD. Notificações a clientes ou parceiros devem ser feitas de forma transparente e oportuna, mantendo a confiança e a reputação da empresa.

### **e) Revisão e Melhoria Contínua:**

Após a resolução de um incidente, realizar uma revisão para avaliar a eficácia da resposta e identificar oportunidades de melhoria. Atualizar políticas e procedimentos conforme necessário para fortalecer a segurança da informação.



## **EXCEÇÕES**

As exceções que ocorram de forma exclusiva e excepcional a esta Política e aos demais documentos normativos complementares devem ser formalizadas e fundamentadas pelo Gestor responsável pela atividade de negócio, analisadas pelos responsáveis pela área gestora dos recursos de informação, e aprovadas pelo Comitê de Segurança da Informação e Privacidade, que poderá a qualquer tempo revoga-las.

## **MONITORAMENTO DO USO DAS INFORMAÇÕES E DOS RECURSOS DE INFORMAÇÃO**

Os ambientes físicos e lógicos da Bridge3 e empresas controladas são monitorados visando a eficácia dos controles implantados e a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referentes a segurança da informação.

A Bridge3 se esforça e toma ações para proteger a privacidade dos dados pessoais de colaboradores e todas as pessoas que se relacionem com a Bridge3, dentro dos seus processos de negócio, mas não pode garantir a privacidade de informações pessoais de usuários gravadas sem proteção nos recursos de informação corporativos, tais como arquivos em áreas acessadas por outros usuários e mensagens eletrônicas sem proteção.

## **VIOLAÇÕES**

As violações a esta Política serão avaliadas pelas áreas de Segurança da Informação, Tecnologia da Informação e Comunicação, Recursos Humanos e Jurídico das empresas controladas da Bridge3 e pelo Comitê de Segurança da Informação e Privacidade, que poderão encaminhar ao Comitê de Ética da empresa controlada e apurar as responsabilidades dos envolvidos em procedimento disciplinar, visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

A tentativa de burla das diretrizes e controles estabelecidos, quando constatada, será tratada como uma violação.

## DISPOSIÇÕES FINAIS

### Gerais

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pela Bridge3.

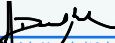
Esta Política, bem como os demais documentos que a complementam, encontram-se disponíveis no site da Bridge3 ou, em caso de indisponibilidade, podem ser solicitadas às áreas responsáveis por Segurança da Informação, Tecnologia da Informação e Comunicação, Recursos Humanos e Assuntos Jurídicos das empresas controladas da Bridge3.

### Revisão desta Política


A revisão desta Política é realizada pelo Comitê de Segurança da Informação e Privacidade a cada dois anos ou quando ocorrerem mudanças significativas na legislação pertinente, na estrutura organizacional, nos objetivos de negócio, nos processos internos, nos riscos à segurança das informações, e nas Políticas da Bridge3.

As proposições de alteração desta Política serão validadas pelo Comitê de Segurança da Informação e Privacidade e, se acatadas, serão submetidas ao Comitê Executivo para apreciação e aprovação.

Esta versão da Política de Segurança da Informação entra em vigor na data de sua aprovação.

**Validado por:**   
Daniela Manole (16 de setembro de 2024 16:41 ADT) **(CEO da Bridge3)**

**Revisões: 1ª edição revisada publicada em janeiro de 2024.**

**Aprovada por:**   
Daniela Manole (16 de setembro de 2024 16:41 ADT) **(Daniela Manole – CEO)**



**B** r i d g e 3





# Política de Segurança da Informação (PSI) da Bridge3.pptx

Relatório de auditoria final

2024-09-16

Criado em:	2024-09-16
Por:	Eliane Otani - Bridge3 (eliane@bridge3.com.br)
Status:	Assinado
ID da transação:	CBJCHBCAABAAOv3FIV-UyqYoODDy-2oXnYr0mCagJMJx

## Histórico

-  Documento criado por Eliane Otani - Bridge3 (eliane@bridge3.com.br)  
2024-09-16 - 16:10:59 GMT
-  Documento enviado por email para Daniela Manole (daniela@bridge3.com.br) para assinatura  
2024-09-16 - 16:11:05 GMT
-  Documento assinado eletronicamente por Daniela Manole (daniela@bridge3.com.br)  
Data da assinatura: 2024-09-16 - 19:41:00 GMT - Fonte da hora: servidor
-  Contrato finalizado.  
2024-09-16 - 19:41:00 GMT