

POLÍTICA
DE SEGURANÇA DA INFORMAÇÃO
E SEGURANÇA CIBERNÉTICA

BELLUNO INSTITUIÇÃO DE PAGAMENTO
LTDA.

Data: 29.09.2022

Versão 01

SUMÁRIO

A. ESCOPO DESSA POLÍTICA.....	4
1. Apresentação e Objetivo.....	4
2. Abrangência.....	4
3. Responsabilidades.....	4
4. Normas Aplicáveis.....	5
5. Aprovação e Revisão.....	5
6. Definições.....	6
B. PRINCÍPIOS.....	6
C. DIRETRIZES GERAIS.....	7
D. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA.....	8
1. Gestão de Ativos.....	8
2. Autenticação.....	9
3. Autorização.....	9
4. Segmentação de rede.....	9
5. Classificação da Informação.....	9
6. Controle de acesso.....	10
7. Gestão de riscos.....	10
8. Gestão de fornecedores.....	11
9. Segurança física do ambiente.....	11
10. Backup e gravação de LOG.....	11
11. Proteção contra vírus, arquivos e softwares maliciosos.....	12
12. Testes de varredura para detecção de vulnerabilidade.....	12
13. Criptografia.....	12
14. Plano de continuidade.....	12
15. Incidentes de segurança.....	13
a. Classificação de relevância dos incidentes.....	13
b. Gestão de incidentes.....	13
c. Plano de compartilhamento de incidentes.....	13
d. Plano de ação e resposta a incidentes.....	14
e. Relatório anual de incidentes.....	14
16. Mecanismos de rastreabilidade.....	14
17. Registro de impacto.....	14
18. Treinamentos e conscientização.....	15
19. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem.....	15
a. Seleção de terceiros.....	15
b. Execução de aplicativos pela internet.....	16
c. Serviços de computação em nuvem.....	16
d. Contratação de serviços de computação em nuvem no exterior.....	17
e. Contrato de prestação de serviços.....	17

f. Comunicação ao Bacen	19
20. Continuidade dos serviços de pagamento	19
21. Arquivamento de informações.....	20
E. DECLARAÇÃO DE RESPONSABILIDADE	21
F. DISPOSIÇÕES GERAIS	21
ANEXO I	22
ANEXO II	23

A. ESCOPO DESSA POLÍTICA

1. Apresentação e Objetivo

Esta Política de Segurança da Informação e Segurança Cibernética (“Política”) tem o objetivo de estabelecer diretrizes que permitem à **BELLUNO INSTITUIÇÃO DE PAGAMENTO LTDA. (“BELLUNO IP”)** preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e da própria BELLUNO IP contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da instituição a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A BELLUNO IP deve implementar e manter esta Política, formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Esta Política será compatível com:

- O porte, o perfil de risco e o modelo de negócio da BELLUNO IP;
- A natureza das atividades da BELLUNO IP e a complexidade dos produtos e serviços oferecidos; e
- A sensibilidade dos dados e das informações sob responsabilidade da BELLUNO IP.

A BELLUNO IP designará diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes, sendo que o diretor designado poderá desempenhar outras funções na instituição, desde que não haja conflito de interesses.

2. Abrangência

A Política se aplica a todos os Sócios e Administradores da (coletivamente “Alta Administração”), funcionários e empresas prestadoras de serviço¹ da BELLUNO IP (coletivamente, “Colaboradores”) cujas atividades sejam desempenhadas visando ao desenvolvimento das operações atinentes a esta Política.

3. Responsabilidades

¹ Quaisquer terceiros que atuem em nome da BELLUNO IP, tais como Auditoria Externa, Tecnologia da Informação, Infraestrutura de TI, dentre outras.

São deveres e responsabilidades de implementação, execução e manutenção desta Política:

- 3.1. **Área de Compliance:** responsável, em conjunto com o diretor responsável pela execução e manutenção desta Política, pela aprovação e atualização periódica da Política;
- 3.2. **Diretor responsável pela execução e manutenção desta Política:** responsável pela implementação, execução e manutenção da política, pela execução do plano de ação e de resposta a incidentes, assim como, pela convocação das reuniões periódicas do comitê de segurança da informação e segurança cibernética;
- 3.3. **Comitê de Segurança da Informação e Segurança Cibernética:** comitê formado por Colaboradores indicados pelas áreas de atuação da BELLUNO IP e aprovadas pela Alta Administração, com o objetivo de deliberar a respeito de assuntos relacionados à esta Política;
- 3.4. **Usuários:** Alta Administração e Colaboradores da BELLUNO IP, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da instituição, e que devem, no que couber: (i) cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta Política; (ii) informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivos, serviços ou processos relacionados à Segurança da Informação e Segurança Cibernética, para que sejam tomadas ações de forma tempestiva; (iii) utilizar as informações relacionadas à esta Política, como patrimônio da BELLUNO IP, e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade.

4. Normas Aplicáveis

- **Lei nº 12.865/2013:** dispõe sobre os Arranjos de Pagamento e as Instituições de Pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).
- **Resolução BCB nº 80/2021:** estabelece os requisitos e os procedimentos para constituição e funcionamento, e de pedido de autorização de funcionamento das Instituições de Pagamento, e dispõe sobre a prestação de serviços de pagamento por outras instituições autorizadas a funcionar pelo Bacen.
- **Resolução BCB nº 85/2021:** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

5. Aprovação e Revisão

Esta Política foi elaborada pela Área de Compliance, pelo Diretor responsável por esta política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes, e foi aprovada pela Alta Administração e será revisada com a periodicidade mínima anual.

A Política também poderá ser alterada, a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.

6. Definições

- **Ativos:** todas as formas de tratamento de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.
- **Alta Administração:** Formado pelos sócios e administradores da BELLUNO IP.
- **Bacen:** Banco Central do Brasil.
- **Cliente:** são os usuários, pessoa física ou jurídica, que contratam os serviços da BELLUNO IP.
- **Gestão de Ativos:** são as boas práticas utilizadas pela BELLUNO IP em seu processo de controle de ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas e materiais, *know-how*) que buscam alcançar um resultado desejado e sustentável para a operação.
- **Informações Sensíveis:** que tem valor estratégico para o desenvolvimento dos negócios e das operações da BELLUNO IP, ganhando tangibilidade por meio de transações, processamentos, bancos de dados, entre outras formas, e que serão tratados com base no legítimo interesse da BELLUNO IP, estritamente necessários para a finalidade pretendida nos termos desta Política e da legislação em vigor.
- **Instituição de Pagamento:** para fins desta Política, é a BELLUNO IP.
- **Log:** registro de eventos de um sistema.
- **Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da BELLUNO IP.
- **Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da BELLUNO IP contra ataques, danos, ameaças ou acesso não autorizado.

B. PRINCÍPIOS

A BELLUNO IP tem como compromisso buscar garantir a segurança e o tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos seguintes princípios:

- **Autenticidade:** garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação;
- **Confidencialidade:** garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;
- **Disponibilidade:** garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário; e
- **Integridade:** garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

C. DIRETRIZES GERAIS

Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na BELLUNO IP;
- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A BELLUNO IP adotará mecanismos que visam a assegurar a utilização segura de senhas;
- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela BELLUNO IP;
- Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar ou, ao menos, registrar acessos indevidos, modificações, destruições ou divulgações não autorizadas;
- Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização;
- Assegurar o cumprimento dos procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações;
- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis;
- Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da BELLUNO IP;

- Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;
- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da BELLUNO IP;
- Classificar os dados e as informações quanto à relevância;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:
 - A implementação de programas de capacitação e de avaliação periódica de pessoal;
 - A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.
- Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen;
- Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros;
- Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com as atividades da BELLUNO IP.

D. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a BELLUNO IP adotará políticas e procedimentos para os processos elencados a seguir.

1. Gestão de Ativos

Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com armazenagem de documentos físicos deve ser restrito e limitado, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A BELLUNO IP deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da autenticidade, confidencialidade, disponibilidade e integridade sejam cumpridos integralmente.

2. Autenticação

A BELLUNO IP adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados.

3. Autorização

Prever processos de autorização levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

4. Segmentação de rede

A BELLUNO IP deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

Caso o Colaborador queira criar, alterar ou excluir regras nos *firewalls* e Ativos de rede deverá enviar uma requisição ao departamento de tecnologia da informação, que fará análise e aprovação.

5. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a BELLUNO IP deve adotar a seguinte classificação:

- **Informação Pública:** aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e dados promocionais;
- **Informação Interna:** aquela que pode ser acessada somente por Colaboradores da BELLUNO IP. São exemplos de Informação Interna: normas, procedimentos e formulários da BELLUNO IP;
- **Informação Restrita:** aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos e documentos estratégicos da BELLUNO IP.
- **Informação Confidencial:** aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.

6. Controle de acesso

A BELLUNO IP deve adotar controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados, aos sistemas internos e às informações que não sejam de livre acesso e sem permissão prévia. Desta forma, a BELLUNO IP deve implementar mecanismos para a autenticação de usuários, manutenção de segregação de funções, rastreabilidade de acesso e aprovação de acesso, quando aplicável, de forma a garantir procedimentos internos adequados e consistentes.

7. Gestão de riscos

A BELLUNO IP possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

Os processos de gestão de riscos englobam os controles de mudanças no ambiente de tecnologia da BELLUNO IP, que são estruturados e aplicados através de um conjunto de medidas que vão atuar em todas as áreas potencialmente impactadas, bem como envolvem a capacitação e o engajamento dos Colaboradores diretamente envolvidos nas ações mitigatórias dentro da BELLUNO IP, com o objetivo da preparação para essas situações.

Neste processo, será levado em conta: (i) o levantamento dos impactos organizacionais; (ii) a priorização das ações de mudanças no ambiente de tecnologia da BELLUNO IP; (iii) o planejamento; (iv) os testes; (v) a mobilização; (vi) a comunicação; e (vii) os treinamentos contínuos para a devida capacitação das pessoas diretamente envolvidas no processo de gestão de riscos e controle dos respectivos ambientes de tecnologia da BELLUNO IP, da seguinte forma:

- i. O levantamento dos impactos organizacionais irá detalhar quais áreas da BELLUNO IP podem vir a ser impactadas direta e/ou indiretamente;
- ii. A priorização das ações de mudanças no ambiente de tecnologia irá avaliar e elencar todas as mudanças que precisam ser implementadas, definindo quais demandas serão tratadas com prioridade e quais poderão ser mitigadas;
- iii. O planejamento irá definir os planos de implementação, impactos e correções, visando a maximizar a segurança e integridade dos ambientes de tecnologia, e minimizar ao máximo riscos de ações ineficientes e ineficazes;
- iv. Os testes irão monitorar todo o processo e se certificar que tudo está acontecendo conforme o planejamento realizado. Após os testes serão elaborados relatórios, os quais serão revisados pelo Diretor responsável pela execução e manutenção desta Política, que descreverão os resultados, funcionalidades e correções;

- v. A mobilização irá, através do Diretor responsável por esta Política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes, direcionar a BELLUNO IP e todos os Colaboradores ao encontro do objetivo deste processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da BELLUNO IP;
- vi. A comunicação irá informar e detalhar os objetivos da mudança através dos canais de comunicação e do desenvolvimento do plano de comunicação, para que todos os Colaboradores da BELLUNO IP tenham conhecimento da relevância e da necessidade do engajamento para o alcance de todas as medidas adequadas e mitigatórias, para neutralizar ou minimizar os eventuais ou potenciais danos;
- vii. O treinamento contínuo irá garantir a transferência e o nivelamento de conhecimentos relacionados ao trabalho desenvolvido no processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da BELLUNO IP.

8. Gestão de fornecedores

A BELLUNO IP verifica o grau de comprometimento com relação a controles de Segurança da Informação e Segurança Cibernética de todos os seus prestadores de serviços, fornecedores, provedores e parceiros que processam e armazenam dados da BELLUNO IP, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A BELLUNO IP deve disponibilizar um canal para que seus prestadores de serviços, fornecedores, provedores e parceiros comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da BELLUNO IP.

9. Segurança física do ambiente

A BELLUNO IP deve implementar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível devem ser mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

10. Backup e gravação de LOG

A BELLUNO IP deve adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

A BELLUNO IP também deve realizar gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acessos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

11. Proteção contra vírus, arquivos e softwares maliciosos

A BELLUNO IP deve adotar mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.g., *phishing*, *spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a BELLUNO IP a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, devem estar instalados e atualizados em toda a rede interna da BELLUNO IP.

12. Testes de varredura para detecção de vulnerabilidade

A BELLUNO IP se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

A BELLUNO IP adota processo de atualização periódica de segurança no parque tecnológico, de forma a prevenir vulnerabilidades que possam ocasionar brechas de segurança para ataque de vírus e outros tipos de software, que se propaguem nos computadores, sistemas e servidores da BELLUNO IP.

13. Criptografia

Os Ativos de informação da BELLUNO IP devem possuir criptografia adequada, conforme a classificação da informação, em todo tráfego que ocorrer em rede pública, a fim de se garantir proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

14. Plano de continuidade

A BELLUNO IP realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da BELLUNO IP sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, a BELLUNO IP realizará o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança.

Devem ser aplicados testes de continuidade de serviços de pagamento e realização testes periódicos para garantir a eficácia e segurança dos processos. O teste deve ser conduzido em um ambiente controlado que permita que a BELLUNO IP certifique a conformidade dos planos desenvolvidos com os objetivos da BELLUNO IP e requisitos legais.

15. Incidentes de segurança

a. Classificação de relevância dos incidentes

A BELLUNO IP classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios da BELLUNO IP.

b. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio dos canais indicados pela BELLUNO IP através do e-mail dpo@belluno.digital.

Os incidentes reportados serão classificados segundo o risco que representam para a BELLUNO IP e o impacto na continuidade dos negócios da BELLUNO IP. Além disso, devem ser devidamente registrados, tratados e comunicados.

A BELLUNO IP adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

c. Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a BELLUNO IP deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com outras Instituições de Pagamento por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a BELLUNO IP comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas, informando o prazo para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, estabelecendo e documentando os critérios que configuraram a situação de crise.

d. Plano de ação e resposta a incidentes

A BELLUNO IP deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

e. Relatório anual de incidentes

A BELLUNO IP deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

- A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional, com o objetivo de adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta Política;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes deve ser apresentado à Alta Administração da BELLUNO IP até 31 de março do ano seguinte ao da data-base.

16. Mecanismos de rastreabilidade

A BELLUNO IP deve adotar controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

17. Registro de impacto

A BELLUNO IP deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da BELLUNO IP, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

18. Treinamentos e conscientização

A BELLUNO IP preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para toda a Alta Administração e todos os seus Colaboradores.

A BELLUNO IP promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, no que couber, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

Além disto, a Alta Administração da BELLUNO IP deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética.

19. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

a. Seleção de terceiros

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a BELLUNO IP deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da BELLUNO IP aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A aderência do prestador de serviço a certificações exigidas pela BELLUNO IP para a prestação do serviço a ser contratado;

- O acesso da BELLUNO IP aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da BELLUNO IP por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da BELLUNO IP.

Na avaliação da relevância do serviço a ser contratado, a BELLUNO IP também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos devem ser documentados.

Ademais, a BELLUNO IP deve adotar recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

b. Execução de aplicativos pela internet

No caso da execução de aplicativos por meio da internet, a BELLUNO IP deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

c. Serviços de computação em nuvem

Os serviços de computação em nuvem disponibilizados à BELLUNO IP, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à BELLUNO IP implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela BELLUNO IP ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela BELLUNO IP, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A BELLUNO IP é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pela BELLUNO IP ao Bacen.

d. Contratação de serviços de computação em nuvem no exterior

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, a BELLUNO IP deverá observar os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;
- Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
- Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços;
- Previsão de alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a BELLUNO IP solicitará autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, a BELLUNO IP deverá solicitar autorização 60 dias antes da alteração contratual.

A BELLUNO IP deve assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso da BELLUNO IP e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deverão ser documentados.

e. Contrato de prestação de serviços

A BELLUNO IP deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;

- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;
- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à BELLUNO IP, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.
- O acesso da BELLUNO IP às informações fornecidas pela empresa contratada; bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação da empresa contratada notificar a BELLUNO IP sobre a subcontratação de serviços relevantes para a instituição;
- A permissão de acesso do Bacen aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;
- A adoção de medidas pela BELLUNO IP, em decorrência de determinação do Bacen;
- A obrigação de a empresa contratada manter a BELLUNO IP permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Em caso de decretação de regime de resolução da BELLUNO IP pelo Bacen, o contrato de prestação de serviços deve prever:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços.

A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:

- A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
- A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da BELLUNO IP.

f. Comunicação ao Bacen

A comunicação ao Bacen, referente a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, deve conter as seguintes informações:

- O nome da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual, salvo na hipótese prevista no item 18 “d”.

20. Continuidade dos serviços de pagamento

No tocante à continuidade dos serviços de pagamento prestados, a BELLUNO IP deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético, relacionados ao registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da BELLUNO IP;
- Os procedimentos a serem seguidos no caso de interrupção de serviços de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da BELLUNO IP;
- Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados, com as diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;
- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados, com o registro, a análise da causa e do impacto, bem

como o controle dos efeitos de incidentes relevantes para as atividades da BELLUNO IP;

- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela BELLUNO IP, bem como das providências para o reinício das suas atividades;
- Estabelecer e documentar os critérios que configurem a situação de crise.

A BELLUNO IP deve instituir mecanismos de acompanhamento e de controle visando a assegurar a implementação e a efetividade desta Política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Os mecanismos de acompanhamento e controle devem incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.

21. Arquivamento de informações

A BELLUNO IP deve armazenar em meio físico ou digital, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;
- O documento relativo ao plano de ação e de resposta a incidentes;
- O relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro;
- A documentação sobre os procedimentos que contemplem a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas, e a verificação da capacidade do potencial prestador de serviço de assegurar tais procedimentos definidos nesta Política;
- A documentação de todos os requisitos regulatórios, no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados;
- A documentação com os critérios que configurem a situação de crise, bem como a respectiva a comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, e as providências para o reinício das suas atividades.

E. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores da BELLUNO IP, a ela devem aderir formalmente por meio de um termo em que se comprometem a agir de acordo com esta Política.

Os contratos celebrados com terceiros pela BELLUNO IP e que tratem de Ativos de informação referentes a esta Política devem possuir cláusula que assegure a segurança das informações.

F. DISPOSIÇÕES GERAIS

Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética e Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética, que deverão ser assinados por todos os Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site <https://belluno.digital> .