POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Woh Instituição de Pagamento Ltda.

Bezz Sociedade de Crédito Direto S.A.

1. Propósito

Este documento define a estrutura de segurança de informação e segurança cibernética conjunta das instituições:

(i) Woh Instituição de Pagamento Ltda.

(ii) Bezz Sociedade de Crédito Direto S.A.

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem o objetivo de estabelecer diretrizes que permitem ao Conglomerado preservar e proteger as informações de seus clientes, colaboradores, partes interessadas e do próprio Conglomerado contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implantar controles e procedimentos que visam reduzir a vulnerabilidade do Conglomerado a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

2. Definições e Princípios

2.1. Definições

- Ativos de informação: 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 por todos os diretores do Conglomerado.
- Bacen: Banco Central do Brasil.
- Gestão de Ativos: são as boas práticas utilizadas pelo Conglomerado 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 do Conglomerado, ganhando tangibilidade por meio de transações, processamentos, bancos de dados, entre outras formas, e que serão tratadas com base no legítimo interesse do Conglomerado, estritamente

necessários para a finalidade pretendida nos termos desta Política e da legislação em vigor.

- Log: registro de eventos de um sistema.
- Segurança da Informação: conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos do Conglomerado.
- Segurança Cibernética: conjunto de práticas, tecnologias e processos desenvolvidos para proteger as informações e os sistemas internos, computadores, redes, softwares e dados do Conglomerado de ataques cibernéticos, danos, ameaças ou acesso não autorizado.

2.2. Princípios

O Conglomerado tem como compromisso garantir a segurança e o tratamento adequado das informações, sistemas internos, computadores, redes, softwares e dados. Para tanto, adota atividades que 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 somente às pessoas autorizadas e sempre que for necessário;
- Integridade: garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

3. 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.
- 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 a elaboração de cenários de incidentes considerados nos testes de continuidade dos negócios.
- 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 do Conglomerado;
- 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 implantação 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 financeiros oferecidos.

- Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com as demais instituições autorizadas a funcionar pelo Bacen.
- Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Conglomerado, inclusive de informações recebidas de empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis.
- Assegurar que os prestadores de serviço utilizem procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pelo Conglomerado e por esta Política.

3.1. 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, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. O Conglomerado 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.

3.2. Autenticação

O Conglomerado adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, bem como deverá prever processos de autorização levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

3.3. Segmentação de rede

O Conglomerado 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.

3.4. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, o Conglomerado 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 do Conglomerado. São exemplos de Informação Interna: normas, procedimentos e formulários do Conglomerado;
- Informação Restrita: aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos, sistemas e documentos estratégicos do Conglomerado.
- 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.

3.5. Controle de acesso

O Conglomerado deve adotar controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados, aos

sistemas internos e as informações que não sejam de livre acesso e sem permissão prévia.

3.6. Gestão de Riscos

O Conglomerado 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 do Conglomerado, que são estruturados e aplicados através de um conjunto de processos que vão atuar em todas as áreas potencialmente impactadas, bem como a capacitação e o engajamento dos Colaboradores diretamente envolvidos nas ações mitigatórias dentro do Conglomerado, 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 do Conglomerado; (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 do Conglomerado.

3.7. Gestão de Fornecedores

O Conglomerado 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 do Conglomerado, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

O Conglomerado 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 do Conglomerado.

3.8. Segurança física do ambiente

O Conglomerado deve implantar 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.

3.9. Backup e gravação de LOG

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

O Conglomerado 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.

3.10. Proteção contra vírus, arquivos e softwares maliciosos

O Conglomerado adotará mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (*phishing, spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham o Conglomerado a vulnerabilidades.

3.11. Testes de varredura para detecção de vulnerabilidade

O Conglomerado 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.

O Conglomerado 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 do Conglomerado.

3.12. Criptografia

Os Ativos de informação do Conglomerado 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.

3.13. Plano de continuidade

O Conglomerado 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 do Conglomerado sejam devidamente identificados e preservados após a ocorrência de uma contingência.

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

3.14. Incidentes de segurança

a. Classificação de relevância dos incidentes

O Conglomerado classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade de negócios do Conglomerado.

b. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador ou cliente devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio dos canais indicados pelo Conglomerado através dos e-mails segurança@bezz.com.br e seguranca@wohpag.com.br.

Os incidentes reportados serão classificados segundo o risco que representam para o Conglomerado e o impacto na continuidade de negócios do Conglomerado. Além disso, devem ser devidamente registrados, tratados e comunicados.

O Conglomerado 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, o Conglomerado deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com as demais instituições autorizadas a funcionar pelo Bacen, por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, o Conglomerado 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 de resposta a incidentes

O Conglomerado deve estabelecer plano de ação e de resposta a incidentes visando à implantação 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

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

- A efetividade da implantação das ações de adequação de suas estruturas organizacional e operacional;
- O resumo dos resultados obtidos na implantação das rotinas, dos procedimentos, dos controles e das 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 de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

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

3.15. Mecanismos de rastreabilidade

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

3.16. Registro de impacto

O Conglomerado deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Conglomerado,

que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

3.17. Treinamentos e conscientização

O Conglomerado 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.

3.18. 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 serão realizados 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.

b. Execução de aplicativos pela internet

No caso da execução de aplicativos por meio da internet, o Conglomerado 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 ao Conglomerado, 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 ao Conglomerado implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pelo Conglomerado ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pelo Conglomerado, 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.

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, o Conglomerado 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 de negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

e. Contrato de prestação de serviços

O Conglomerado 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 ao Conglomerado, 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 do Conglomerado 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 o Conglomerado sobre a subcontratação de serviços relevantes para o Conglomerado;
- 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 pelo Conglomerado, em decorrência de determinação do Bacen;
- A obrigação de a empresa contratada manter o Conglomerado permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

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.

3.19. Continuidade de negócios

No tocante à continuidade de negócios, o Conglomerado deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
- 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 do Conglomerado;
- Os cenários de incidentes considerados nos testes de continuidade de negócios.
- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
- 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 pelo Conglomerado, bem como das providências para o reinício das suas atividades;
- Estabelecer e documentar os critérios que configurem a situação de crise.

3.20. Arquivamento de informações

O Conglomerado 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;
- A ata da reunião com a aprovação da Alta Administração referente a esta Política e ao plano de ação e de resposta a incidentes;
- O relatório anual sobre a implantação do plano de ação e de resposta a incidentes;
- A documentação sobre os procedimentos desta Política;
- A documentação com os critérios que configurem uma situação de crise;
- A documentação no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implantação dos mecanismos mencionados.

4. Versões

Versão	data de aprovação	Alterações
1ª	31/10/2022	▪ Versão inicial
2ª	28/02/2023	Versão compilada para divulgação para clientes