Number One
CORRETAGEM DE CÂMBIO

POLÍTICA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

3ª Edição
PO-SC

Data de Criação: 10/12/2020

Data da última Revisão: 30/12/2024

Elaboração / Aprovação: Equipe de TI / Diretoria

Sumário

1. OBJETIVO

Nossa política de segurança cibernética, em conformidade com à legislação e regulamentação vigente, em especial à Resolução BCB 85/21, e as melhores práticas de mercado, visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de nossa propriedade e/ou sob nossa guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que o representam, em nível estratégico, os princípios fundamentais incorporados pela empresa para o alcance dos objetivos de segurança da informação.

A NUMBER ONE também busca cumprir a Lei Geral de Proteção de Dados Pessoais (LGPD) e outras legislações de proteção de dados aplicáveis. Assim, são implementadas medidas para garantir a privacidade e a segurança dos dados pessoais sob nossa responsabilidade, em conformidade com os princípios de confidencialidade, integridade e transparência.

2. ALCANCE

Aplica-se a todos os colaboradores da NUMBER ONE.

3. ÁREA GESTORA

Gerência de Tecnologia da Informação.

4. INTRODUÇÃO

Segurança Cibernética é o conjunto de processos e controles voltados à proteção de informações e ativos digitais contra acessos não autorizados, danos e interrupções. Na NUMBER ONE, essa segurança é considerada essencial para a

continuidade dos negócios, sendo integrada ao Plano de Continuidade de Negócios (PCN) para assegurar resiliência e resposta rápida a incidentes.

O foco da segurança cibernética está em preservar a confidencialidade, integridade e disponibilidade das informações. Esses princípios garantem que os dados sejam usados e compartilhados de forma controlada, com monitoramento constante e tratamento de incidentes relacionados a ataques cibernéticos.

Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Riscos cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares

- Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
- Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;
- Spyware: software malicioso para coletar e monitorar o uso de informações;
- Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia Social

- Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

- Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
- Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

5. DIRETRIZES

O cumprimento da política de segurança cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;

- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Number One;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam as atividades da Number One e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Todos os sistemas críticos e aplicações que armazenam informações sensíveis ou confidenciais devem implementar autenticação multifatorial (MFA) para aumentar a segurança e mitigar o risco de acessos não autorizados;
- É estritamente proibido o uso de dispositivos pessoais para acessar sistemas corporativos. Apenas dispositivos autorizados e monitorados pela TI podem se conectar aos sistemas da empresa.
- Todos os colaboradores têm o dever de reportar atividades suspeitas, comportamentos anômalos ou descumprimentos da política que possa indicar uma tentativa de comprometimento de segurança, além de documentar todos os incidentes reportados. A área de TI deve ser notificada imediatamente para avaliação e resposta.

6. PLANO DE AÇÃO / RESPOSTA A INCIDENTES

6.1 Implementação

Visando a implementação das práticas da Política de Segurança Cibernética na Number One está implementando um Plano de Ação e de resposta a incidentes abrangendo o seguinte:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética.
- Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes.
- Área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Plano de Ação e de Resposta a Incidentes será aprovado pelo Diretor responsável pela Política de Segurança Cibernética e pela diretoria e será revisado no mínimo anualmente.

6.2 Relatório sobre a implementação do plano de ação e de resposta a incidentes

Será emitido anualmente, com data base de 31 de dezembro, relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes. Esse Relatório deve contemplar, no mínimo, as seguintes informações:

- A efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética.
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- 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 deve ser elaborado até 31 de março do ano seguinte ao da data base devendo ser aprovado pelo Diretor responsável pela Segurança Cibernética e a diretoria.

7. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Os Prestadores de serviços e parceiros de serviços de processamento de dados e armazenamento em nuvem podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações, envolve determinados riscos que são levados em conta pela Corretora, demandando assim cuidados proporcionais a esta identificação de ameaças.

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem deve seguir critérios rigorosos de segurança, aderindo às normativas dispostas na Resolução BCB 85/21, nos seus respectivos artigos.

7.1 Exigências para a contratação de serviços

A Number One ao realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende às seguintes exigências:

a) Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo:
   - Se mantém Política de Segurança da Informação;
   - Se possui Plano de Continuidade de Negócios;
   - Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças);
   - Se mantém Gestão de Incidentes.

b) Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:
   - Cumprimento da legislação e da regulamentação em vigor;
   - Permissão de acesso da Number One aos dados e as informações a serem processadas ou armazenadas pelo Prestador de serviços;

- Confidencialidade, integridade, disponibilidade e recuperação dos dados e das informações processadas ou armazenadas pelo Prestador de serviços;
- Aderência a certificações que a Number One possa exigir para a prestação do serviço a ser contratado;
- Acesso da Number One aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
- Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;
- Identificação e segregação dos dados dos clientes da Number One por meio de controles físicos ou lógicos;
- Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da Number One.

7.2 Avaliação dos serviços a serem contratados

A Number One deve proceder a uma avaliação da relevância dos serviços prestados por empresas com possibilidades de serem contratadas considerando o seguinte:

- criticidade dos serviços a serem prestados;
- sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;
- verificação quanto a adoção, por parte do prestador de serviços quanto a adoção de controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet.

7.3 Comunicações ao Banco Central do Brasil

A Number One deverá informar previamente ao Banco Central do Brasil a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada até 10 dias após a contratação ou alteração dos serviços prestados e deve conter as seguintes informações:

a) denominação da empresa a ser contratada;

b) os serviços relevantes a serem contratados;

c) a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela, deve observar os seguintes requisitos:

a) a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

b) assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

c) definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

d) prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anterior a Number One deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações já mencionadas.

A Number One deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações.

7.4 Dos contratos

Os contratos firmados entre a Number One e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) a indicação dos países e da região, em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

b) a adoção de medidas de segurança para a transmissão e armazenamento dos dados.

c) a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes.

d) a obrigatoriedade, em caso de extinção do contrato, de:

- transferência dos dados ao novo prestador de serviços ou a Number One;
- exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade.

e) O acesso da Number One a:

- Informações fornecidas pela empresa contratada visando verificar o cumprimento dos itens previstos nos itens a), b) e c) acima.
- Informações relativas às Certificações exigidas pela Corretora e aos relatórios de auditoria especializada contratada pelo prestador de serviços.
- Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f) a obrigação da empresa contratada notificar a Number One sobre a subcontratação de serviços relevantes para a Corretora.

g) a permissão de acesso do Banco Central do Brasil às seguintes informações:

- contratos e acordos firmados para a prestação de serviços
- documentação e informações referentes aos serviços prestados
- os dados armazenados
- as informações sobre processamento
- as cópias de segurança dos dados e das informações
- códigos de acesso aos dados e as informações.

h) a adoção de medidas pela Number One em decorrência de determinação do Banco Central do Brasil.

i) a obrigatoriedade da empresa contratada manter a Number One permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor.

j) o contrato deve também prever, para o caso de decretação de regime de resolução da Corretora pelo Banco Central:

- A obrigação da empresa contratada para a prestação de serviços conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos
  acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:

(I) A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução.

(II) A notificação prévia deve ocorrer também na situação em que a interrupção for motivava por inadimplência da Corretora.

8. PROCEDIMENTOS PARA PREVENÇÃO E PROTEÇÃO AO RISCO CIBERNÉTICO

8.1 Ações de Prevenção

Devem ser criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da Corretora através das seguintes ações:

- Manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição. Por exemplo, computadores não autorizados ou software não licenciado.
- Manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.
- Monitorar as rotinas de backup, executando testes regulares de restauração dos dados.
- Realizar, periodicamente testes de invasão externa e phishing.
- Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.
- Periodicamente testar o plano de resposta a incidentes, simulando os cenários.

8.1.1 Configuração de Situação de Crise

Considerando a definição a seguir:

Crise cibernética: Crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização.

Podemos destacar os critérios abaixo, como preponderantes, para a configuração de uma situação de crise instalada e deverão ser classificados na categoria de incidentes relevantes:

(I) Sabotagem, de forma intencional, a processos, sistemas, máquinas;
(II) Ataque terrorista
(III) Crimes cibernéticos.

8.2 Tratamento de Incidentes

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Corretora, como por exemplo:

- queda de energia elétrica
- falha de um elemento de conexão
- servidor fora do ar
- ausência de conexão com internet
- Indisponibilidade de acesso a corretora
- Ataques DDOS

Todo colaborador que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato para que o mesmo seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

AVALIAÇÃO INICIAL

Avaliar o incidente em conjunto com a Diretoria para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas.

Deve-se ainda analisar motivos e consequências imediatas, bem como a gravidade da situação, classificando o incidente nas categorias de Relevante e Não Relevante.

INCIDENTE CARACTERIZADO

Caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

- Iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros.
- O Diretor responsável pela Política de Segurança Cibernética estará avaliando o impacto do incidente nos diversos riscos envolvidos.
- Conforme a relevância (sabotagem, terrorismo, etc.) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências.
- Conforme a relevância do incidente comunicar os clientes que por ventura tenham sido afetados.
- Configurado e classificado como Incidente relevante, com interrupção de serviço essencial (situação de crise), realizar comunicação tempestiva ao Banco Central o Brasil, incluindo providências tomadas.

RECUPERAÇÃO

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros-chave notificados. Quaisquer dados faltando ou corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados à Diretoria e ao Diretor responsável pela Política de Segurança Cibernética.

RETOMADA (Normalização)

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

9. MONITORAMENTO E TESTES (Mecanismos de Controle)

O ambiente de TI da Corretora deve ser supervisionado e monitorado com o objetivo de verificar sua efetividade e detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados. É possível a ocorrência de algum risco de segurança cibernética através de uma das seguintes situações descritas:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas;
- Comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”)
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com condições internamente estabelecidas.
- Vazamento de informações durante tráfego de dados não criptografados.

Anualmente a Corretora deve providenciar a execução de testes de cibersegurança através da verificação dos seguintes itens:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos da Corretora;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Corretora;
- Vulnerabilidades que possam causar incidentes (vírus, trojans, furtos, acessos indevidos, etc.);
- Inspeção física nas máquinas de hardware, se mantido servidor físico.

Os referidos testes devem ter seus dados, informações e resultados, devidamente registrados em documentos, armazenados e disponíveis aos órgãos

reguladores e auditorias, pelo prazo de 05 (cinco) anos a contar da implementação dos mecanismos de controle.

A política de segurança cibernética será revisada e auditada anualmente, com auditorias internas e externas para avaliar a efetividade dos controles, identificar vulnerabilidades e garantir a adequação das medidas de segurança às melhores práticas de mercado.

10. INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela Number One é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas.

A Number One poderá revelar as informações confidenciais nas seguintes hipóteses:

- Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
- Aos órgãos reguladores do mercado financeiro; e
- Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

11. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

O gerenciamento dos controles de segurança objetiva assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta política.

O Gerenciamento de Risco de Segurança Cibernética, deve estar previsto na Matriz Geral de Risco e na Política de Plano de Continuidade de Negócios da NUMBER ONE.

11.1 Gestão de acessos às informações

A concessão de acesso às informações segue o princípio de menor privilégio, onde cada colaborador possui acesso apenas ao mínimo necessário para realizar suas funções. Os privilégios são revistos periodicamente para garantir a conformidade com este princípio, minimizando o risco de acessos indevidos. Esses acessos são cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores e terceiros da Number One são treinados, periodicamente, sobre os conceitos de segurança da informação, através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

11.2 Proteção do Ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica da Number One por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

11.3 Uso de inteligência Artificial (IA)

A utilização de ferramentas de Inteligência Artificial (IA) é permitida apenas para fins autorizados e previamente definidos pela empresa. Qualquer aplicação de IA deve estar em total conformidade com as normas de proteção de dados e privacidade, e seu uso para análise de dados sensíveis deve respeitar rigorosamente a confidencialidade e integridade das informações.

O uso não autorizado de IA em operações que envolvam dados da empresa ou dados de clientes é estritamente proibido. Qualquer desenvolvimento, aplicação, ou solicitação para uso de IA deve ser previamente aprovado pela área de TI e Compliance, garantindo o alinhamento com as regulamentações vigentes e os direitos de privacidade dos indivíduos. Os colaboradores devem evitar o uso de ferramentas externas de IA que não estejam alinhadas com as diretrizes de segurança e privacidade da empresa.

12. DISPOSIÇÕES FINAIS

Com a publicação da política de segurança cibernética, a Number One demonstra boa-fé na orientação de seus clientes e colaboradores quanto às melhores práticas de segurança da informação para o uso de seus serviços e na preocupação em manter os dados de seus clientes protegidos, colocando-se à disposição para responder a denúncias e tirar dúvidas através dos seus canais oficiais.

13. Histórico de Revisões

Revisão	Data	Item	Descrição	Alterado / solicitado por	Área	Aprovado por
01	10/12/2020	-	Implantação	-	TI	Diretoria
02	24/03/2023	-	Atualização Geral da Política e Revisão	Lourival Amaral	TI	Diretoria
03	30/12/2024	-	Revisão Geral	Mauri Henrique / Rodrigo Reyero	TI	Diretoria