voiter

Política da Segurança da Informação e Cibernética

Área responsável: Segurança da Informação

Atualização: 30.03.2022

voiter

Sumário

1. Objetivo 4
2. Classificação do Documento e Alvo 4
3. Seções da Política e Responsabilidades 4
   3.1. Organizando a Segurança da Informação 4
      3.1.1. Papeis e Responsabilidades da Segurança da Informação 5
      3.1.2. Segregação de Funções 9
      3.1.3. Contato com as Autoridades Externas 10
      3.1.4. Segurança da Informação no Gerenciamento de Projetos 10
   3.2. Política de Segurança em Recursos Humanos 10
   3.3. Política de Gestão de Ativos 10
   3.4. Política de Controle de Acesso 11
   3.5. Política de Criptografia 11
   3.6. Política de Segurança Física e do Ambiente 11
   3.7. Política de Segurança nas Operações 12
   3.8. Política de Segurança nas Comunicações 12
   3.9. Política de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação 12
   3.10. Política de Gestão de Prestadores de Serviço 12
   3.11. Política de Gestão de Incidentes de Segurança da Informação 13
   3.12. Política de Continuidade de Negócios 13
   3.13. Política de Dispositivos Móveis 13
   3.14. Conformidade 13
4. Diretrizes 14
   4.1. Contratação de Serviços de Processamento e Armazenamento de Dados de Computação em Nuvem 15
      4.1.1. Diretrizes para contratação de serviços para processamento e armazenamento de dados e de computação na Nuvem 15
      4.1.2. Os serviços de computação em nuvem abrangem a disponibilidade sob demanda e de maneira virtual, de, ao menos, um dos seguintes serviços 16
      4.1.3. Da prestação de serviço por terceiros no exterior 16
      4.1.4. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever 17
      4.1.5. Para a decretação de regime de resolução do Voiter pelo Banco Central do Brasil 17

voiter

5. Glossário 18
6. Regulamentação Associada 19
7. Responsáveis 19
8. Validade 19

voiter

1. Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação do Voiter para todos os colaboradores, prestadores de serviços e parceiros. O Conselho de Administração do Voiter adotou esta política de segurança cibernética e da informação com o objetivo de atingir suas metas comerciais, conformidade com normas ou leis aplicáveis, estabelecendo as diretrizes para execução das atividades relacionadas à manutenção da confidencialidade, integridade e disponibilidade da informação no Conglomerado Voiter, considerando as regulamentações vigentes e melhores práticas de mercado e observando os seguintes princípios:

- Confidencialidade: Assegurar que a informação é acessível somente por pessoas autorizadas;
- Integridade: Proteger a exatidão e a completeza da informação e dos métodos de processamento; e
- Disponibilidade: Assegurar que todos os usuários autorizados tenham acesso à informação e ativos associados, quando necessário.

Todos os ativos de informação são de propriedade intelectual do Voiter, não importando a sua forma ou meio de armazenamento (digital ou impresso). Portanto, o uso deste ativo só deve acontecer dentro das atividades de negócio que a administração do Voiter julgar pertinente.

2. Classificação do Documento e Alvo

Esta Política aplica-se a todo o Conglomerado, inclusive às empresas subsidiárias e unidades estabelecidas no exterior, as quais deverão, no que couber, adequá-la às exigências da legislação e regulamentação locais. Exceções da política serão permitidas somente quando aprovadas antecipadamente pela alçada pertinente.

3. Seções da Política e Responsabilidades

3.1.1. Organizando a Segurança da Informação

Constitui-se nesta política a Área de Segurança da Informação, que tem a missão de assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e proporcionar confiança ao negócio onde o Voiter atua.

3.1.2. Papeis e Responsabilidades da Segurança da Informação

Conselho de Administração

O Conselho de Administração e a alta gestão estão comprometidos com a melhoria contínua dos procedimentos relacionados à segurança da informação e cibernética do Voiter. Para tanto, as responsabilidades específicas do Conselho de Administração são:

- Ler e aprovar a política de Segurança da Informação e Cibernética anualmente;
- Deliberar orçamento para iniciativas de Segurança da Informação e Cibernética.

Diretoria Executiva

A Diretoria Executiva é responsável por:

- Revisar e aprovar a política de Segurança da Informação e Cibernética anualmente.
- Gerenciar o cumprimento desta Política por parte de seus supervisionados.
- Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações.
- Impedir o acesso de empregados demitidos ou demissionários aos ativos, utilizando-se dos mecanismos de desligamento do empregado.
- Prover recursos de gestão para que os times responsáveis possam monitorar os serviços a serem prestados, garantindo um melhor nível de qualidade.
- Tomar decisões de alto nível pertinentes às Políticas de Segurança da Informação e Cibernética e seu conteúdo.
- Aprovar, antecipadamente, exceções a estas políticas com base em análise caso-a-caso.
- Coordenar, anualmente, uma verificação de risco formal para identificar novas ameaças e vulnerabilidades e identificar controles apropriados para minimizar qualquer novo risco.
- Patrocinar iniciativas de Segurança e Governança Corporativa pautadas nas melhores práticas de mercado ou exigências regulatórias.

Área de Compliance

A Área de Compliance é responsável por:

- Coordenar o cumprimento, pela área de Segurança da Informação, de suas obrigações regulatórias;
- Assegurar que a área de Segurança da Informação realize a manutenção e atualização das políticas e procedimentos de Cibersegurança;
- Publicar, em portal institucional, as políticas e procedimentos de Cibersegurança.

Auditoria Interna

O processo de auditoria de verificação de conformidade dos processos estabelecidos nesta Política será executado periodicamente conforme calendário da Área de Auditoria Interna, ou a qualquer momento de acordo com a necessidade do negócio, para garantir que todas as partes estão executando corretamente as suas atividades e garantir que todos os outros requisitos de Segurança da Informação estão sendo constantemente observados.

A auditoria poderá ser realizada por auditor externo ou equipe interna, seguindo a programação de auditoria estabelecida pelo Gerente de Segurança da Informação.

As responsabilidades específicas da Área de Auditoria Interna incluem:

- Auditar processos de segurança e tecnologia da informação;
- Realizar interface e acompanhamento de auditorias externas.

Gerência de Segurança da Informação

A proteção bem-sucedida dos sistemas do Voiter requer que vários departamentos e grupos sigam consistentemente uma visão compartilhada de segurança.

A Área de Segurança da Informação é dedicada ao planejamento, educação e conscientização sobre segurança. As responsabilidades específicas da Área incluem:

- Criar novas políticas e procedimentos de segurança da informação quando necessário.
- Manter e atualizar políticas e procedimentos de segurança da informação existentes.
- Rever anualmente as políticas e auxiliar a administração com o processo de aprovação.

- Agir como um departamento central de coordenação para implantação das políticas de Segurança da Informação.
- Criar, manter e distribuir procedimentos de resposta a incidentes e de encaminhamento.
- Monitorar e analisar alertas de segurança e distribuir informações ao pessoal apropriado de segurança, técnico e da administração da unidade de negócios.
- Fazer a revisão diária dos eventos de segurança (*logs* e alertas).
- Restringir e monitorar o acesso a áreas restritas e informação confidencial.
- Assegurar que os controles adequados estejam disponíveis onde houver informações sensíveis.
- Gerir a Matriz de Segregação de Funções e realizar periodicamente a revisão de acessos.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional.
- Promover a divulgação desta política a todos os administradores, funcionários, prestadores de serviços, consultores e fornecedores, doravante denominados usuários.
- Apoiar ou avaliar as solicitações de acesso em exceção, em conjunto com o gestor imediato avaliando se o acesso será permitido ou não, podendo este ser submetido à aprovação de um diretor caso necessário.
- Rever anualmente as políticas e procedimentos de segurança da informação para manter a adequação face às emergentes necessidades de negócio ou ameaças à segurança.
- Manter atualizados e distribuir o Plano de Resposta e Procedimentos para todos os usuários.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional.
- Tratar incidentes de Segurança da Informação, dando o devido direcionamento.

Gerência de Tecnologia da Informação

O departamento de Tecnologia da Informação do Voiter é o elo direto entre as políticas de Segurança da Informação e a rede, os sistemas e os dados.

Suas responsabilidades incluem:

- Aplicar as políticas e procedimentos de segurança da informação de acordo com sua aplicabilidade a todos os ativos de informação.
- Administração das contas de usuários e gerenciamento de autenticação.
- Auxiliar a Área de Segurança da Informação com o monitoramento e controle de todos os acessos aos dados do Voiter.
- Manter um diagrama de rede atualizado, incluindo as redes sem fio. O diagrama deve incluir a data em que se deu a última atualização.
- Restringir o acesso físico a pontos de rede acessíveis ao público, pontos de acesso sem fio, *gateways* e equipamentos portáteis (*hand held*).
- Manter procedimentos operacionais de administração de redes e sistemas claramente definidos e documentados, de forma a garantir uma operação correta e segura.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional.

Gente, Gestão e Inspiração

Devido a seu relacionamento direto e constante com os funcionários existentes, assim como sua posição única de ter a primeira e última interações com novos/ex-funcionários, o departamento de Recursos Humanos tem um papel importante no que se refere à segurança das informações do Voiter. É responsabilidade da Área:

- Solicitar ao time de Compliance verificações necessárias para ingresso novos funcionários que poderão ter acesso a dados sensíveis do Banco.
- Certificar-se que o funcionário participe do treinamento de conscientização sobre segurança após a contratação e, pelo menos, uma vez por ano.
- Trabalhar com o Área de Segurança da Informação na disseminação de informações de conscientização sobre segurança, utilizando diversos métodos de comunicação de conscientização e educação dos funcionários (ex. pôsteres, cartas, memorandos, e-mails, treinamento via web, reuniões, etc).
- Trabalhar com o Área de Segurança da Informação e Compliance para administrar sanções e ações disciplinares referentes a violações da Política de Segurança da Informação.
- Comunicar a admissão de novos funcionários às diversas áreas da Instituição que atuam nas concessões de acesso, quer sejam físicos ou lógicos, para que

os respectivos acessos básicos inerentes à função desempenhada sejam adequadamente concedidos.

- Informar o desligamento dos usuários para que a área de Segurança da Informação possa remover os acessos físicos e lógicos dos colaboradores.
- Manter todos os Formulários de Conscientização sobre Segurança e Uso Aceitável e de Solicitação de Autorização nos arquivos dos funcionários.

Usuários

Todo usuário de recursos computacionais e de informação do Voiter devem estar cientes da importância fundamental de tais recursos e reconhecer sua responsabilidade pela manutenção segura dos mesmos. Os usuários devem protegê-los contra abusos que interrompam ou ameacem a viabilidade de todos os sistemas.

As seguintes responsabilidades são especificas a todos os usuários de sistemas computacionais do Voiter:

- Entender as consequências de suas ações relacionadas às práticas de segurança computacional e agir de forma condizente. Aceitar que a filosofia que "Segurança é responsabilidade de todos", para auxiliar o Voiter no atingimento de seus objetivos comerciais.
- Manter a conscientização sobre o conteúdo das políticas de Segurança da Informação.
- Ler e assinar as Políticas do Voiter quando de sua contratação e, ao menos, uma vez ao ano.
- Classificar informações confidenciais e sensíveis que sejam recebidas sem classificação, de acordo com a Política de Classificação e Controle de Informação, e limitar a distribuição destas informações.
- Cumprir as Políticas e Diretrizes estabelecidas neste documento e nos controles internos disponíveis na Intranet, conforme termo firmado na contratação.

3.1.3. Segregação de Funções

Para todos os ambientes do Voiter, sejam eles de produção, homologação, desenvolvimento ou teste, é desejável a implementação de segregação de funções.

A segregação de funções determina que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada, ou para coibir o mau uso dos ativos da organização intencional ou não intencional. Para casos de exceção, seja por limitação técnica ou de negócio, é obrigatório o uso de controles adicionais de segurança e aprovação da Diretoria Executiva.

3.1.4. Contato com as Autoridades Externas

Como parte do plano de comunicação interno e externo e do plano de resposta a incidentes de segurança da informação do Voiter, declara-se que qualquer comunicação relacionada a segurança da informação, junto às autoridades externas que incluem, mas não se limitam, a entidades reguladoras, entidades de conformidade e governo, devem ser previamente autorizadas e aprovadas pela Diretoria Executiva.

3.1.5. Segurança da Informação no Gerenciamento de Projetos

Como parte da metodologia de gerenciamento e projetos do Voiter, todos os projetos devem incluir segurança da informação dentro do seu ciclo de vida. A inclusão tem como objetivo avaliar os riscos de segurança da informação, bem como propor controles adequados e acrescentar aos objetivos do projeto os objetivos de segurança de informação.

3.2. Política de Segurança em Recursos Humanos

A área de Gente, Gestão e Inspiração deve criar e manter atualizados os critérios de seleção para candidatos (funcionários) que tenham como objetivo garantir a veracidade e honestidade das informações fornecidas, sendo que estes critérios devem respeitar e atender as regulamentações e leis vigentes.

Além disso, os acordos de confidencialidade devem ser anexados ao contrato de trabalho ou prestação de serviço, aos quais devem ser assinados e devolvidos para os seus representantes legais.

3.3. Política de Gestão de Ativos

É desejável que ativos de informação do Voiter sejam classificados de acordo com o seu nível de confidencialidade, disponibilidade, integridade e controles

legais. Uma vez classificados, devem ser respectivamente relacionados ao modo como são acessados, armazenados, movimentados e, por fim, descartados.

Todos os ativos de informação em forma de mídias removíveis ou impressos devem ter sua classificação de modo claro e visível para que se possa dar o devido grau de tratamento.

3.4. Política de Controle de Acesso

Todos os sistemas de informação do Voiter devem estar integrados à um sistema de controle de acesso homologado pela Área de Tecnologia e Área de Segurança da Informação.

A concessão de acessos (recursos ou sistemas) devem ser aprovados pelo gestor da informação. Além disso, deve ser instituída a segregação de função de acordo com nível funcional ou responsabilidade, assim como uma revisão periódica dos acessos concedidos, a fim de se evitar acessos indevidos.

3.5. Política de Criptografia

Toda informação do Voiter que precise ser protegida contra acesso não autorizado ou estabelecido por normas externas ou internas de conformidade deve utilizar criptografia robusta, conforme os padrões aceitos pelo mercado, de modo a garantir a confidencialidade, autenticidade e integridade da informação.

Além disso, todas as chaves de criptografia utilizadas devem ser gerenciadas por um processo que determine as diretrizes do ciclo de vida da chave e outros aspectos relevantes.

3.6. Política de Segurança Física e do Ambiente

É de responsabilidade dos seus respectivos proprietários proteger os ativos de informação contra danos, roubo ou qualquer evento que possa gerar indisponibilidade.

É necessário estabelecer o perímetro de segurança física, de modo a preservar o acesso somente a pessoas autorizadas. Além disso, deve ser instituído de modo obrigatório o uso de identificação funcional (crachá), para que seja possível monitorar os mais diversos níveis de acesso para colaboradores, prestadores de serviço, parceiros de negócios e visitantes.

3.7. Política de Segurança nas Operações

A Área de Tecnologia, com apoio da Área de Segurança da Informação, deve estabelecer as diretrizes para garantir a operação segura e correta dos recursos de processamento da informação. Para isso, deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários.

Estes procedimentos operacionais devem incluir, e não se limitar a, procedimentos de instalação e configuração de sistemas, procedimentos para manipulação de informação, procedimentos de cópias de segurança (*backup*), procedimentos para gerenciamento de trilhas de auditoria e procedimentos de monitoramento de eventos.

Além disso, deve ser estabelecido um processo único de gestão de mudanças com o objetivo de controlar e garantir a autorização e documentação de toda mudança no ambiente.

3.8. Política de Segurança nas Comunicações

A Área de Tecnologia, com apoio da Área de Segurança da Informação, deve estabelecer as diretrizes para garantir a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Para isso, deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários, estabelecendo as responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede.

3.9. Política de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação

Todos os processos que envolvam aquisição, desenvolvimento ou manutenção de sistemas de informação somente devem ser feitos a partir das áreas custodiantes, mediante autorização da Área de Tecnologia e a Área de Segurança da Informação. Além disso, deve ser contemplado, em cada processo, a execução de testes de segurança para garantir que os riscos relacionados sejam conhecidos e tratados.

3.10. Política de Gestão de Prestadores de Serviço

Todo relacionamento com prestadores de serviço deve seguir as diretrizes estabelecidas, de modo a garantir a proteção dos ativos do Voiter acessados por

estes fornecedores. Além disso, todo relacionamento acordado deve ser formalizado e estabelecido entre as partes através de cláusulas de confidencialidade e de responsabilidade na manipulação de informações e prestação de serviços.

3.11. Política de Gestão de Incidentes de Segurança da Informação

O processo de gestão de incidentes de segurança da informação tem como objetivo garantir que eventos de segurança da informação associados a ativos de informação do Voiter sejam comunicados a Área de Segurança da Informação.

É de responsabilidade da Área de Segurança da Informação coordenar todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação. É dever de todos os usuários de informação comunicar um incidente de segurança da informação para área responsável.

3.12. Política de Continuidade de Negócios

O processo de gestão de continuidade do negócio deve ser implementado com o objetivo de reduzir os impactos sobre os negócios do Voiter. É responsabilidade do gestor da unidade de negócio solicitar à Área de Tecnologia a condução e suporte dos planos de continuidade.

3.13. Política de Dispositivos Móveis

A Área de Tecnologia e a área de Recursos Humanos, com apoio da Área de Segurança da Informação, devem estabelecer as diretrizes para garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis do Voiter. Para isso, devem estabelecer uma política formal e acessível, com as condições e restrições.

Esta Política deve incluir, e não se limitar a, procedimentos de registro dos dispositivos móveis, proteção física, instalação de *software*, acesso a informações classificadas, controle de acesso, desativação ou bloqueio remoto e cópias de segurança (backup).

3.14. Conformidade

Todos os ativos e sistemas de informação do Voiter, assim como os seus funcionários e prestadores de serviço, devem estar em conformidade com as obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação estabelecidos pelo Voiter.

Uma 'não conformidade' é qualquer falha decorrente do não atendimento dos requisitos especificados nas documentações internas, regulamentações, contratos e outras obrigações dentro do Sistema de gestão da segurança da informação (SGSI).

Não conformidades podem ser identificadas durante uma auditoria interna ou externa, com base na revisão de gestão, após incidentes, durante operações de negócio normais ou em qualquer outra ocasião.

Com objetivo de prevenir violações, todas as informações armazenadas ou que trafeguem dentro dos perímetros físicos e lógicos do Voiter podem ser monitoradas, mediante o processo de aprovação instituído e revisado pela Área de Segurança da Informação. Violações não serão toleradas e as sanções apropriadas serão aplicadas.

4. Diretrizes

As informações devem ser protegidas contra acesso, modificação, destruição ou divulgação não autorizada, independentemente do meio em que se encontrem.

As informações são de propriedade da Instituição e são monitoradas rotineiramente, não havendo privacidade ou sigilo para seus conteúdos entre funcionários e o Voiter.

É proibido enviar materiais de uso exclusivo da Instituição para pessoas de fora dela, sem as devidas autorizações.

As informações confidenciais deverão ser tratadas com o sigilo necessário.

Os recursos disponibilizados devem ser utilizados somente para os propósitos e finalidades aprovados pela Instituição, sendo vedada a utilização para fins pessoais.

As senhas de acesso corporativo são de uso pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto a sua guarda.

É proibido o compartilhamento de senhas de acesso, sendo passíveis de sanções os descumprimentos.

Para os acessos *core* do Conglomerado, foram desenvolvidas as matrizes de segregação de acessos. Nelas estão detalhados os sistemas, módulos, perfis e departamentos autorizados a utilizarem os acessos à determinados perfis dos sistemas.

É proibido o uso de câmeras fotográficas ou de filmagem, sem autorização prévia, a ser concedida pela área de Segurança da Informação, dentro das instalações do Conglomerado.

Todas as instalações de processamento e guarda de informações deverão ser mantidas em áreas seguras e protegidas.

O Voiter disponibilizará acesso à Internet via rede *Wireless*, segregado da rede corporativa, sendo este meio exclusivo para utilização de visitantes e acessos não corporativos. (ex. Utilização de dispositivos móveis).

As atividades de processamento da informação serão monitoradas, detectadas e registradas através de trilha de auditoria. O monitoramento e o registro devem estar de acordo com a legislação vigente.

O Conglomerado realizará *backups* rotineiros e testes periódicos de restauração de dados, visando salvaguardar os ativos de informação da Instituição.

Todo *hardware*, *desktop*, *hardware* móvel, *mobile*, deverão ser utilizados para fins corporativos, de acordo com as regras estipuladas pela Instituição, sendo responsabilidade do funcionário a guarda e zelo do equipamento.

Não será permitida, sem autorização prévia do gestor imediato e da área de Segurança da Informação, a utilização de *hardware* externos do tipo: unidade de armazenamento de dados, dispositivos de comunicação externas, dispositivos de transmissão de dados e unidade de leitura de dados internos e externos.

A violação ou não aderência às políticas e procedimentos de segurança de informações podem ocasionar sanções disciplinares e, em alguns casos, levar ao desligamento do funcionário, inclusive por justa causa, se aplicável, ou ao cancelamento do contrato de serviço.

4.1. Contratação de Serviços de Processamento e Armazenamento de Dados de Computação em Nuvem

4.1.1. Diretrizes para contratação de serviços para processamento e armazenamento de dados e de computação na Nuvem

- Verificar a capacidade do potencial do prestador de serviço, assegurando o acesso aos dados e às informações a serem processados ou armazenados pelo prestador do serviço, visando a mitigação de eventuais vulnerabilidades;
- Considerar os três princípios da Segurança da Informação;
- Verificar a aderência a certificações exigidas;

- Acesso a 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;
- Identificar, proteger e segregar os dados de clientes por meio de controles físicos ou lógicos.

4.1.2. Os serviços de computação em nuvem abrangem a disponibilidade sob demanda e de maneira virtual, de, ao menos, um dos seguintes serviços

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a implantação ou execução de *softwares*, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela Instituição ou por ela adquiridos;
- Implantar e executar aplicativos desenvolvidos pelo Voiter ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Executar por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

Observação: A contratação de serviços de processamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil após a contratação do serviço, bem como alterações contratuais.

4.1.3. Da prestação de serviço por terceiros no exterior

- Verificar 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, em caso de inexistência de convênio, deverá ser solicitada a autorização do Banco Central do Brasil para a contratação;
- Assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

- 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;
- Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

4.1.4. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever

- 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;
- 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 clientes;
- A obrigatoriedade, em caso de extinção do contrato, de transferência dos dados ao novo prestador de serviços ou à instituição contratante e a exclusão dos dados citados no pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;
- O Voiter deverá ser notificado sobre a subcontratação de serviços e a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações.

4.1.5. Para a decretação de regime de resolução do Voiter pelo Banco Central do Brasil

- O prestador de serviço deve obrigar-se a conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos

acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações e aos códigos de acesso, que estejam em poder da mesma.

- Realizar a notificação prévia sobre a intenção de a empresa contratada interromper a prestação de serviços (pelo menos trinta dias de antecedência) da data prevista para a interrupção;
- O prestador de serviço deve aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução e a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

5. Glossário

Segurança da Informação: é a proteção de dados de propriedade das organizações contra ameaças diversas. Trata-se de um esforço pautado por ações que objetivam mitigar riscos e garantir a continuidade das operações.

Risco Cibernético: geralmente se refere a qualquer risco de perda financeira, interrupção ou dano à reputação de uma organização resultante da falha de seus sistemas de tecnologia da informação.

Usuário: todos os funcionários, prestadores de serviços, terceiros ou estagiários aos quais possuem acesso a algum recurso sistêmico ou de infraestrutura do Conglomerado.

Controle de Acesso Lógico: são qualquer tipo de aplicação ou equipamento que usa da tecnologia para impedir que pessoas acessem documentos, dados ou qualquer tipo de informação sem a autorização adequada. Uma tela de login de um e-mail qualquer, em que se pede um nome de usuário e senha, é uma forma de controle de acesso lógico.

Controle de Acesso Físico: composto, basicamente, por uma barreira perimetral, como um muro, cerca ou alambrado, e um ou mais pontos de acesso, controlados

por dispositivos como portas e portarias que usem meios mecânicos (ex.: portões, cancelas) ou eletrônicos (ex.: catracas e fechaduras eletrônicas).

6. Regulamentação Associada

Resolução CMN n° 4.893, de 26 de fevereiro de 2021

Procedimentos associados à Segurança da Informação publicados no Portal Corporativo

Norma ISO/IEC 27001

Resolução CMN nº 4.658, de 26 de abril de 2018

Resolução CMN nº 4.557, 23 de fevereiro de 2017

Edital de Consulta Pública 57/2017 do BACEN

Guia ANBIMA de Cibersegurança

Procedimento de Gerenciamento de Incidentes

Procedimento de Gerenciamento de Incidentes Cibersegurança

Política de Continuidade de Negócio

Procedimento de Continuidade de Negócio

Política de Contratação de Fornecedores e Prestadores de Serviços

7. Responsáveis

Elaboração	Revisão	Aprovação
Segurança da Informação	Segurança da Informação	Conselho de Administração 30.03.2022

8. Validade

Um ano.