PCG_004 – Segurança Cibernética e de Informação

Objetivos

Esta política de Segurança Cibernética e de Informação ("Política") é a declaração formal do Banco Votorantim S.A. ("Banco") e sociedades controladas, integrantes do Conglomerado Financeiro Votorantim, em conjunto denominadas nesta Política como ("Conglomerado"), referente ao compromisso com a proteção de suas informações e ativos de informação, bem como das informações e ativos de informação de seus clientes e fornecedores.

Esta Política tem como objetivo estabelecer diretrizes e princípios gerais de segurança da informação e segurança cibernética para o Conglomerado, em um esforço para garantir que os usuários atuem em observância às regras referentes ao tratamento e proteção das informações e ativos de informação, bem como assegurar a capacidade do Conglomerado em prevenir, detectar e reduzir sua vulnerabilidade a incidentes.

Diretrizes

1. Público-Alvo

1.1. Esta Política é aplicável a todos os colaboradores e usuários de informações e ativos de informação do Conglomerado no Brasil e no exterior.

1.2. Fornecedores do Conglomerado também estão sujeitos às diretrizes, procedimentos e controles estabelecidos nessa Política sempre que realizarem o tratamento de informações ou utilizarem os ativos de informação do Conglomerado.

1.3. Para os fins desta Política, "colaborador" significa empregados, contratados, subcontratados, estagiários, menores aprendizes e administradores do Conglomerado, e "fornecedor" significa todas as empresas fornecedoras, parceiras e prestadoras de serviços a terceiros que celebraram um contrato de fornecimento, parceria e/ou prestação de serviços com o Banco e/ou suas controladas, bem como seus representantes, empregados e subcontratados.

1.4. Para os fins desta Política, os termos "informações" e "ativos de informação" incluem o conceito de dado pessoal e/ou dado pessoal sensível, tal como definido pela Lei Geral de Proteção de Dados, Lei Federal nº 13.709/18.

2. Princípios da Segurança da Informação

2.1. Por princípio, a segurança da informação abrange 4 (quatro) aspectos básicos destacados a seguir:

a) Confidencialidade: Garante que a informação e ativos de informação sejam acessíveis somente pelos usuários autorizados, pelo período necessário.

b) Disponibilidade: Garante que a informação e ativos de informação estejam disponíveis para os usuários autorizados sempre que necessários aos processos de negócio ou a clientes do Conglomerado.

c) Integridade: Garante que a informação e ativos de informação estejam completos e íntegros e que não tenham sido modificados ou destruídos de maneira não autorizada ou acidental durante o seu ciclo de vida.

d) Autenticidade: Garante a propriedade da informação e que esta seja proveniente da fonte anunciada e não foi alvo de alterações indevidas ao longo de um processo estabelecido.

2.2. Para os fins desta Política, o termo usuário significa qualquer indivíduo, processo, dispositivo ou mecanismo que acesse, use, manipule ou trate uma informação ou ativo de informação.

3. Aspectos Gerais

3.1. As diretrizes desta Política constituem os principais pilares do Sistema de Gestão de Segurança da Informação do Conglomerado, norteando a elaboração de instruções normativas e manuais de procedimento pelas áreas responsáveis.

3.2. A proteção das informações e ativos de informação do Conglomerado deve ser uma prioridade constante das áreas de negócio e de suporte do Conglomerado, de forma a reduzir riscos de falhas, bem como danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais do Conglomerado.

3.3. A proteção das informações e ativos de informação deve ser aplicada de forma compatível com seu impacto ao Conglomerado, abrangendo todos os processos, informatizados ou não.

3.4. Uma atitude engajada e proativa no que diz respeito à proteção das informações do Conglomerado deve ser prioridade constante de todas as áreas de negócio, reduzindo-se os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais.

3.5. As informações sob responsabilidade do Conglomerado devem ser manuseadas de acordo com as leis vigentes e normas internas e utilizadas apenas para a finalidade para a qual foi coletada, evitando o comprometimento de sua confidencialidade, integridade, disponibilidade, autenticidade e privacidade.

3.6. Todos os processos do Conglomerado devem garantir a segregação das funções por meio da participação de mais de um colaborador ou equipe de colaboradores nas atividades, a fim de evitar o conflito de interesse e reduzir o risco de uso indevido acidental ou proposital dos ativos de informação e sistemas do Conglomerado.

3.7. Todos os colaboradores do Conglomerado ou de fornecedores, conforme aplicável, devem ter ciência de que o uso dos ativos de informação, dos sistemas e ambientes podem ser monitorados e que os registros podem ser utilizados para detecção de violações desta Política e normas de segurança da informação, servindo de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais.

3.8. Os papéis e responsabilidades quanto à segurança da informação são amplamente divulgados aos colaboradores, que devem conhecer e cumprir essas diretrizes.

3.9. Os riscos de segurança da informação do Conglomerado, bem como dúvidas sobre a Política e normas relacionadas devem ser reportados à Superintendência de Segurança da Informação.

3.10. Os sistemas, aplicações e infraestruturas tecnológicas, marcas, metodologias e quaisquer informações do Conglomerado não devem ser utilizados para fins pessoais. Sobre o uso da internet, para fins pessoais, deve ser responsável, seguindo as legislações vigentes (sobre ações discriminatórias, privacidade, pirataria, pedofilia, terrorismo e etc.), não deve contrariar as normas internas, que possa trazer riscos de contaminação ao ambiente ou de vazamento de informações e não deve prejudicar os princípios de Segurança da Informação contidos nesta política ou o Código de Conduta.

3.11. Exceto com a expressa autorização do seu proprietário responsável, as tecnologias, marcas, metodologias e quaisquer informações do Conglomerado não devem ser repassadas ou compartilhadas com terceiros, ainda que tenham sido obtidas ou desenvolvidas pelo próprio colaborador do Conglomerado durante o exercício de suas funções.

4. Classificação das Informações

4.1. Toda informação criada ou recebida pelo Conglomerado deve ser classificada e protegida ao longo de todo seu ciclo de vida, nos termos das Instruções Normativas e Manuais de Procedimentos de Segurança da Informação do Conglomerado. O ciclo de vida das informações compreende sua criação ou coleta, manuseio, armazenamento, transporte e descarte.

4.2. Para assegurar a proteção adequada das informações, elas devem ser classificadas de acordo com o seu valor, requisitos legais, relevância, sensibilidade e criticidade para o Conglomerado. Os critérios de classificação devem considerar as necessidades de negócio, demandas regulatórias, compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

4.3. As diferentes classificações para as Informações estão definidas em Instrução Normativa específica.

5. Tratamento das Informações

5.1. As informações devem ser tratadas de acordo com as leis vigentes, regulamentação aplicável, Instruções Normativas e sua classificação, e utilizadas apenas para a finalidade para a qual foram coletadas, ou para outras finalidades autorizadas por lei.

5.2. As informações poderão ser tratadas em legítimo interesse do Conglomerado para proteger a segurança dos ativos de informação ou a segurança das operações comerciais do Conglomerado.

5.3. As informações são atribuídas a um proprietário formalmente designado como responsável pela autorização de acesso às informações sob sua responsabilidade.

5.4. Para fins desta Política, o "proprietário" significa o indivíduo ou grupo com autoridade operacional sobre uma Informação específica e responsabilidade para estabelecer os controles por sua criação, coleta, processamento, disseminação e descarte.

5.5. As atividades de tratamento das Informações devem ser rastreáveis e registradas em trilhas auditáveis.

6. Segurança Cibernética

6.1. O Conglomerado também aplica controles de segurança de informação de forma a garantir sua segurança cibernética, com o objetivo de assegurar a disponibilidade, confidencialidade, integridade e autenticidade das informações e ativos de informação em seus ambientes tecnológicos.

6.2. De forma a auxiliar na implementação das diretrizes estabelecidas nesta Política e dos controles, processos e procedimentos do Sistema de Gestão de Segurança de Informação e da Segurança Cibernética do Conglomerado, são adotados, por padrão, os seguintes mecanismos e as melhores práticas disponíveis no mercado:

a) medidas de autenticação capazes de individualizar usuários que acessam ativos de informação, sistemas e ambientes do Conglomerado;

b) emprego de criptografia, mascaramento e ofuscação, quando aplicável, para o armazenamento de Informações relevantes e sensíveis em ativos de informação, sistemas e ambientes do Conglomerado e de fornecedores;

c) uso de tecnologia de criptografia e comunicação segura para a transmissão de informações entre colaboradores, usuários e fornecedores;

d) soluções de prevenção e detecção de intrusão e acessos não-autorizados aos ativos de informação, sistemas e ambientes do Conglomerado;

e) uso de procedimentos e controles para prevenir o vazamento de informações;

f) testes e varreduras periódicas para a detecção de falhas e vulnerabilidades nos procedimentos, controles, sistemas e ambientes do Conglomerado;

g) soluções de proteção contra softwares maliciosos (malwares, spywares, trojans, vírus, botnets, etc.) que podem afetar ativos de informação, sistemas e ambientes do Conglomerado;

h) sistemas de rastreamento de atividade e registros (logs) para as atividades realizadas em seus sistemas e ambientes, com o objetivo de garantir a segurança das informações;

i) controle de acesso pelos usuários que façam uso dos sistemas e ambientes do Conglomerado;

j) segregação e segmentação dos diferentes ambientes de rede disponibilizados pelo Conglomerado ou fornecedores por ele contratado aos seus colaboradores, fornecedores e clientes;

k) manutenção de cópias de segurança das informações.

6.3. Os controles mínimos listados no item 6.2 também devem ser aplicados no desenvolvimento de novos produtos, soluções, aplicativos, sistemas e ambientes, bem

como na aquisição de novas tecnologias e serviços que integrarão as atividades operacionais do Conglomerado.

6.4. Da mesma forma, os controles mínimos listados no item 6.2 também deverão ser adotados, conforme aplicável, por fornecedores que processam ou armazenam informações sensíveis ou relevantes para a condução das atividades operacionais do Conglomerado.

7. Gestão de Acessos

7.1. Os processos de concessão, alteração e exclusão de acesso aos ativos de informação, sistemas de informação e/ou ambientes do Conglomerado são realizados pela área competente mediante aprovação formal do gestor do solicitante e do respectivo proprietário do sistema e/ou perfil.

7.2. São concedidos acessos para os colaboradores do Conglomerado e/ou de fornecedores somente às informações necessárias ao desempenho de suas funções e/ou determinação legal.

7.3. São concedidos acessos privilegiados às informações, ativos de informações, sistemas e ambientes do Conglomerado aos seus colaboradores e/ou colaboradores de fornecedores mediante o cumprimento de regras específicas. Acessos privilegiados implicam em responsabilidades adicionais ao usuário.

7.4. As exclusões de acesso devido ao desligamento de colaboradores devem ocorrer tempestivamente mediante comunicado de desligamento enviado à Superintendência de Segurança da Informação pela área de Pessoas e Cultura, no caso de colaborador do Conglomerado. No caso de colaborador de fornecedor, a comunicação deve ser feita com igual tempestividade, ao gestor do respectivo contrato.

7.5. Toda credencial de acesso ao ambiente, seja ele físico ou lógico, é única, individualmente identificada e atribuída a um proprietário, qualificando-o como responsável pelas ações realizadas por esta credencial, não podendo ser transferida ou compartilhada entre usuários ou terceiros.

7.6. Contas de serviço e usuários genéricos, destinadas usualmente à execução de processamentos automatizados, devem seguir a governança estabelecida pela área de Segurança da Informação, garantindo a rastreabilidade dos acessos, bem como, os vínculos a área responsável e o processo de revisão periódico.

7.7. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria identifiquem individualmente o usuário, para que ele possa ser responsabilizado por suas ações.

8. Gestão de Riscos em Segurança da Informação

8.1. O Conglomerado possui um processo estruturado de monitoramento, análise e identificação de vulnerabilidades, ameaças e impactos sobre os ativos de informação, para que sejam identificados os controles adequados e a eficácia periodicamente testada.

8.2. O Conglomerado desenvolve, documenta, homologa e testa periodicamente planos de contingência, e os aprova para ativação no caso de previsão, suspeita ou ocorrência de

situações que comprometam a integridade, a disponibilidade e a continuidade das atividades do Conglomerado.

9. Gestão de Incidentes de Segurança da Informação

9.1. O Conglomerado adota procedimentos, requisitos e controles específicos para a prevenção e resposta a incidentes ocorridos. Os procedimentos, controles e requisitos para fornecedores devem estar alinhados com os próprios níveis de complexidade, abrangência e precisão do Conglomerado.

9.2. Para os fins desta Política, o termo "incidente" significa qualquer ocorrência no acesso, no uso das Informações ou Ativos de Informação que afete ou possa afetar a confidencialidade, disponibilidade, integridade, autenticidade das informações ou dos ativos de informação ou a privacidade dos titulares dos dados.

9.3. A classificação de relevância de incidente deve seguir o critério de impacto nos processos de negócios do Conglomerado mensurados por meio de análises qualitativas e/ou quantitativas, que avaliam potenciais impactos decorrentes da violação das diretrizes desta Política, conforme previstos nas respectivas instruções normativas.

9.4. O tratamento de incidentes relevantes que se caracterize como crise deve ser acompanhado pela área de Continuidade, Crises e Vendors, seguindo política e instrução normativa própria para garantia da execução das ações e todos os envolvimentos necessários.

9.5. Compete à área de Segurança da Informação realizar o registro, análise de causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Conglomerado.

9.6. Cenários de incidentes de segurança de informação são incluídos nos testes de continuidade de negócio do Conglomerado.

9.7. Todo incidente de segurança da informação no Conglomerado ou em fornecedores, que envolvam informações e ativos de informação do Conglomerado, deve ser formalmente reportado à Superintendência de Segurança da Informação.

9.8. O Conglomerado informará, em atenção ao arcabouço regulatório aplicável, ao Banco Central do Brasil e aos demais reguladores, todos os incidentes relevantes e interrupções de serviços relevantes, bem como as medidas tomadas para o reinício das atividades. Quando o incidente acarretar risco ou dano relevante à privacidade e proteção de dados do titular, o Encarregado do Dado comunicará à Autoridade Nacional de Proteção de Dados.

9.9. Sem prejuízo do dever de sigilo e da livre concorrência e por dever regulatório, o Conglomerado compartilhará as informações que possuir sobre incidentes relevantes de segurança de informação com demais instituições financeiras, incluindo informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros, por meio de canais estabelecidos para esse fim e sempre que tais informações forem para benefício e segurança do mercado financeiro.

10. Plano de Ação e Resposta a Incidentes

10.1. O Conglomerado possui um Plano de Ação e Resposta a Incidentes, que deve conter as ações a serem desenvolvidas pelo Conglomerado para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta Política, e rotinas, procedimentos, controles e tecnologias que serão utilizadas na prevenção e resposta de incidentes.

10.2. O Plano de Ação e Resposta a Incidentes deve ser revisto anualmente e aprovado pelo Conselho de Administração do Conglomerado.

10.3. O Conglomerado elaborará anualmente um relatório contendo a efetividade das ações e um 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, previstas no Plano de Ação e Resposta a Incidentes, os incidentes relevantes ocorridos no período, e os resultados dos testes de continuidade de negócios.

10.4. O relatório anual deve ser submetido ao Comitê de Controles e Riscos do Conglomerado e apresentado ao Conselho de Administração.

11. Conscientização em Segurança da Informação

11.1. A alta administração do Conglomerado, comprometida com a melhoria contínua do sistema de gestão de segurança de informação do Conglomerado, publica e assume seu compromisso em cumprir com as diretrizes elencadas nesta Política de SI.

11.2. Os papéis e responsabilidades quanto à segurança da informação são amplamente divulgados aos colaboradores e alta administração, que devem conhecer e cumprir essas diretrizes.

11.3. Como parte do seu compromisso, o Conglomerado adota ações e iniciativas para promover a capacitação, aculturamento e avaliação dos colaboradores sobre o tema segurança da informação, reforçando as diretrizes declaradas nesta política.

11.4. O Conglomerado também promove ações e iniciativas junto aos seus clientes com informações sobre precauções na utilização de seus produtos e serviços financeiros.

12. Divulgação desta Política

12.1. Um comunicado contendo uma versão resumida desta Política é divulgada aos colaboradores do Conglomerado e a sua versão completa fica disponível em local de fácil acesso para consulta.

12.2. Uma versão desta Política é apresentada para os fornecedores do Conglomerado, contendo as diretrizes aplicáveis aos fornecedores que prestarem serviços ou acessem informações, ativos de informação ou ambientes do Conglomerado, com o nível de detalhamento compatível com as funções desempenhadas ou sensibilidade das informações tratadas.

12.3. Um resumo com linhas gerais desta Política é divulgado ao público geral, contendo linguagem clara e de fácil acesso.

13. Contratos

13.1. Os contratos entre o Conglomerado e empresas ou pessoas prestadoras de serviços, colaboradores, parceiros, contratados e estagiários, que tiverem acesso às informações, aos sistemas ou aos ambientes tecnológico corporativos devem conter cláusulas que garantam o devido tratamento de dados pessoais de acordo com as diretrizes da Lei Geral de Proteção de Dados e com as exigências do Termo de Tratamento de Dados Pessoais, bem como, a confidencialidade entre as partes, requisitos mínimos de segurança alinhados com os mesmos quesitos de segurança adotados pelo Conglomerado, e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a política e as normas de segurança da informação do Conglomerado.

13.2. Os contratos de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem estarão sujeitos a regime de contratação específico, obedecidos as disposições previstas pelas áreas de Segurança da Informação, Compras e Jurídico em observância ao arcabouço regulatório aplicável..

14. Avaliação Independente da Auditoria

14.1. A efetividade desta Política é verificada por meio de avaliações periódicas das áreas corporativas de controle, órgãos reguladores, auditorias internas e externas.

15. Medidas Disciplinares

15.1. As violações a esta Política estão sujeitas a sanções disciplinares previstas nas normas internas do Conglomerado, na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas.

16. Revisão desta Política de Segurança de Informação

16.1. Esta Política deve ser revisada ao menos uma vez por ano, e eventuais alterações devem ser aprovadas pelo Conselho de Administração do Banco.

As diretrizes constantes nesta política são regulamentadas e operacionalizadas por meio de normas e procedimentos que definem regras e processos para o correto cumprimento das políticas.

17. Documentos relacionados

Instruções Normativas de Segurança da Informação

IN	Título	Temas
IN_1164	Controle de Segurança da Informação para Fornecedores	Controle de Segurança da Informação para Fornecedores
IN_1270	Chaves Criptográficas, Certificados Digitais e Assinaturas Eletrônicas	Chaves Criptográficas, Certificados Digitais e Assinaturas Eletrônicas
IN_253	Gerenciamento de Identidade e Acessos	Gerenciamento de Identidade e Acessos Proprietários e Gestores dos Sistemas de Informação e Perfis RBAC

		Senhas dos Sistemas de Informação Utilização de Contas com Privilégios Administrativos ou de Serviço Criação e Desativação de Login de Rede, Contas e Grupos de E-mail Intercâmbio de Informações e Domínios de Internet
IN_009	Controle de Comunicações de Rede	Controle de Comunicações de Rede Configuração de Firewalls Acesso Remoto aos Computadores Corporativos Utilização da Rede Corporativa Wireless e Cabeada
IN_677	Gestão da Segurança da Informação	Gestão da Segurança da Informação Classificação da Informação Condições e Regras para Mesa Limpa Armazenamento e Descarte de Documentos, Mídias e Equipamentos Utilização de Skype for Business e Internet Utilização de Correio Eletrônico
IN_675	Ciclo de Desenvolvimento Seguro de Software	Ciclo de Desenvolvimento Seguro de Software
IN_016	Gestão de Incidentes de Segurança da Informação	Gestão de Incidentes de Segurança da Informação
IN_674	Gestão de Planos de Continuidade de Negócios e Gestão de Crises	Gestão de Planos de Continuidade de Negócios e Gestão de Crises Análise de Impacto nos Negócios (BIA) Gestão de Crises
IN_1249	Gestão de Vulnerabilidade	Gestão de Vulnerabilidade Configuração Segura de Servidores Segurança nas Estações de Trabalho - Permissões de Acessos e Gravação de Informações
IN_1393	Utilização do Laboratório de Cibersegurança	Utilização do Laboratório de Cibersegurança

ANEXO I

Diretrizes de Segurança da Informação para Fornecedores

1. Público-Alvo

Estas diretrizes são aplicáveis a todos os fornecedores, nacionais ou estrangeiros, que, direta ou indiretamente, acessem ou de qualquer forma façam o tratamento das informações, ou acessem e utilizem os ativos de informação, sistemas ou ambientes do Conglomerado no Brasil e/ou no exterior. Para os fins destas Diretrizes, os termos "informações" e "ativos de informação" incluem o conceito de dado pessoal e/ou dado pessoal sensível, tal como definido pela Lei Geral de Proteção de Dados, Lei Federal nº 13.709/18. A observância dessas diretrizes não substitui a necessidade de as empresas do Conglomerado exigirem a assinatura de Termo de Tratamento de Dados Pessoais como parte integrante dos contratos com os fornecedores.

A aplicabilidade dos controles estabelecidos neste documento depende da natureza do fornecimento de bens e/ou serviços contratados entre o fornecedor e o Conglomerado, bem como da relevância e/ou sensibilidade das informações, dos ativos e sistemas de informação e dos ambientes a que o fornecedor tenha acesso, utilize ou trate, conforme definido pelo Conglomerado.

2. Princípios da Segurança da Informação

Por princípio, a segurança da informação abrange 4 (quatro) aspectos básicos, destacados a seguir:

Confidencialidade: Garante que a informação e/ou ativos de informação seja(m) tratada(os) com o devido zelo e acessíveis somente por usuários autorizados, pelo período necessário.

Disponibilidade: Garante que a informação e/ou ativos de informação correspondentes esteja(m) disponível(is) para os usuários autorizados, sempre que se fizer necessária aos processos de negócio ou aos clientes do Conglomerado.

Integridade: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

Autenticidade: Garante a propriedade da informação e que esta seja proveniente da fonte anunciada e não foi alvo de alterações indevidas ao longo de um processo estabelecido.

3. Aspectos Gerais

O Conglomerado possui um sistema de gestão de segurança da informação formalmente estabelecido e com suas principais diretrizes e controles para segurança de suas informações e ativos de informação de sua propriedade e/ou sob sua guarda.

O Conglomerado exige que todos os seus fornecedores possuam políticas e controles alinhados com os apresentados neste documento e seus adendos.

O Conglomerado espera que seus fornecedores tenham uma atitude engajada e proativa no que diz respeito à proteção das informações, ativos de informação, e ambientes do Conglomerado, de forma a reduzir os riscos de falhas, os danos e/ou prejuízos que possam causar um incidente.

O tratamento das informações, bem como o acesso e uso dos ativos de informação por fornecedores no ambiente estarão sujeitos às normas e procedimentos de segurança de informação do Conglomerado.

O tratamento das informações, bem como o acesso e uso dos ativos de informação do Conglomerado, se e quando efetuados pelo fornecedor no local do fornecedor devem ser realizados de acordo com as leis e regulamentações vigentes e aplicáveis, bem como pelas disposições previstas neste documento.

O Conglomerado utiliza controles de acesso físico e lógico a seus ambientes que tem como função reduzir ou mitigar o risco de acesso, divulgação ou uso indevido, seja acidental ou proposital, de suas informações ou ativos de informação, tais como a segregação de

função de eventuais usuários dos fornecedores, bem como o monitoramento de sistemas e ambiente do Conglomerado que são acessados ou utilizados por fornecedores.

Os riscos, eventos e incidentes, bem como dúvidas sobre segurança da informação que o fornecedor tenha devem ser imediata e formalmente reportados à superintendência da Área Segurança da Informação do Conglomerado [csirt@bv.com.br | (11) 5171-4998], observadas as disposições previstas neste documento e respectivos adendos.

O tratamento informações, bem como o acesso e/ou uso ativos de informação estão restritos à finalidade para a qual o fornecedor foi contratado. As informações e ativos de informação do Conglomerado não devem ser acessados, utilizados e/ou de qualquer forma tratados para qualquer outro fim, inclusive fins pessoais. O fornecedor somente poderá compartilhar as informações e ativos de informação do Conglomerado, conforme previamente acordado com o Conglomerado e desde que necessário para a consecução da finalidade contratada.

4. Tratamento e Classificação das Informações

O Conglomerado classifica todas as suas informações de acordo com a sua relevância ou sensibilidade e somente as disponibiliza ao fornecedor, se for o caso, por meio de seu proprietário ou representante autorizado, já devidamente classificadas e mediante um compromisso de sigilo e confidencialidade.

Todas as informações do Conglomerado em posse do fornecedor devem estar adequadamente protegidas pelo fornecedor em conformidade com este documento em todo o seu ciclo de vida, que compreende a geração, manuseio, armazenamento, transporte e descarte.

O fornecedor deve preservar a confidencialidade, integridade, disponibilidade, autenticidade e conformidade na gestão, custódia e uso das informações e ativos de informação do Conglomerado, sendo considerado proibido todo tratamento que não seja explicitamente autorizado em contrato.

O fornecedor deve adotar mecanismos e as melhores práticas disponíveis no mercado para a proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens e furtos quanto à coleta, uso, armazenamento, tratamento, compartilhamento, proteção e descarte de informações do Conglomerado.

5. Gestão de Acesso

O Conglomerado estabelece diferentes perfis de acesso às suas informações, sistemas e ambientes. Todo e qualquer usuário terá um ou mais perfil(is) de acesso atribuído pelo Conglomerado de acordo com as diretrizes contidas neste documento e/ou adendos aplicáveis.

Os processos de atribuição, configuração, alteração e revogação de acesso a ativos de informação e sistemas, ou ambientes do Conglomerado são realizados mediante solicitação formal do gestor da área responsável pelo fornecedor e aprovação do respectivo responsável pelo sistema e/ou perfil em conjunto com a superintendência da Área Segurança da Informação do Conglomerado, observadas as disposições previstas neste documento.

O fornecedor será o responsável por comunicar quaisquer alterações nos perfis ou desligamento de seus colaboradores para o gestor da área responsável do Conglomerado.

São atribuídos acessos para os fornecedores somente aos ativos de informação e sistemas e ambientes necessários ao desempenho das atividades contratadas, não podendo ser concedidos por prazo indeterminado.

Toda credencial de acesso aos ambientes do Conglomerado é individualmente identificada e atribuída a um colaborador do fornecedor, permanecendo o fornecedor como o principal responsável pelos atos praticados com o uso dessa credencial.

6. Gestão de Riscos em Segurança da Informação

O Conglomerado possui um processo estruturado de monitoramento, análise e identificação de vulnerabilidades, ameaças e impactos sobre os ativos de informação, sistemas e ambientes.

Compete ao fornecedor estabelecer processos estruturados de monitoramento, análise e identificação de vulnerabilidades sobre os ativos de informação, sistemas e ambientes do Conglomerado, conforme aplicável, que respeitem o disposto neste documento.

O fornecedor estará sujeito ao monitoramento e análise de suas atividades no curso do acesso e uso dos ativos de informação, sistemas e ambiente, nos termos deste documento.

Qualquer risco identificado pelo Conglomerado ou representante autorizado, durante o monitoramento e análise das atividades do fornecedor será imediatamente informado ao fornecedor, que deverá avaliar o risco apresentado e apresentar ao Conglomerado um plano de ação e prazo para o tratamento e mitigação desse risco.

7. Gestão de Incidentes de Segurança da Informação

Todo incidente deve ser imediata e formalmente reportado à superintendência da Área Segurança da Informação [csirt@bv.com.br | (11) 5171-4998]. Quando o incidente envolver dados pessoais e/ou dados pessoais sensíveis do Conglomerado, o fornecedor deverá reportar, por meio do seu Encarregado do Dado, à superintendência da Área Segurança da Informação. O fornecedor deverá colaborar com o Conglomerado para a identificação e tratamento da causa, impactos e efeitos do incidente, conforme solicitado pelo Conglomerado. O fornecedor deve se certificar que a superintendência da Área Segurança da Informação e o Encarregado do Dado do Conglomerado tomou ciência de sua comunicação do incidente.

8. Conscientização em Segurança da Informação

O fornecedor deve realizar ações e iniciativas para promover o aculturamento de seus colaboradores sobre o tema de segurança da informação.

9. Requisitos Adicionais

Além das diretrizes indicadas neste documento, os fornecedores também devem cumprir com os requisitos de segurança de informação contidos em outra documentação ("anexo ll - Requisitos de Segurança e Tecnologia da Informação para Fornecedores").

10. Avaliação de Segurança da Informação para o Conglomerado

A efetividade da adequação do fornecedor com as diretrizes indicadas neste documento e/ou adendos é verificada por meio de avaliações periódicas das áreas Segurança da Informação, Compliance e Controles Internos, Riscos, Tesouraria, TI ou outras áreas a serem definidas pelo Conglomerado, que poderão solicitar documentação, evidência e/ou realizar auditorias internas e externas junto ao fornecedor, seja no local do Conglomerado ou do fornecedor.

11. Violações

As violações as diretrizes indicadas neste documento estão sujeitas a sanções previstas no respectivo contrato celebrado com o Conglomerado, na legislação e/ou regulamentação aplicáveis.

12. Declaração de Recebimento

A [Denominação da Contratada] declara ter recebido, lido e concordado com todos os termos e condições das presentes Diretrizes de Segurança da Informação para Fornecedores, bem como dos Requisitos de Segurança e Tecnologia da Informação para Fornecedores, os quais cumprirá integralmente.

Ciente e de acordo em: ___/___/_____

[Denominação da Contratada]

ANEXO II

Requisitos de Segurança e Tecnologia da Informação para Fornecedores

1. Objetivo

Este documento constitui um adendo ao documento que consta as diretrizes de segurança da informação para fornecedores ("anexo I - Diretrizes de Segurança da Informação para Fornecedores") do Conglomerado e tem por objetivo estabelecer disposições adicionais sobre os controles mínimos de segurança e tecnologia da informação, visando a proteção das informações, ativos de informação e sistemas do Conglomerado. Quando aplicável, os termos definidos no documento que consta as diretrizes de segurança da informação para fornecedores terão o mesmo significado neste documento.

2. Escopo e Aplicação

O fornecedor deve assegurar a implementação de controles de segurança e técnicos que atendam aos requisitos delineados abaixo, e dar prova objetiva da sua existência para o Conglomerado, sempre que solicitado. Controles adicionais poderão ser exigidos e/ou recomendados dependendo da natureza do contrato, relevância dos serviços ou classificação das informações a que o fornecedor tem acesso.

Esses requisitos aplicam-se a todo ambiente computacional, infraestrutura, colaboradores, terceiros e outros recursos que suportem, direta ou indiretamente, o fornecedor na prestação do serviço.

Os controles listados abaixo nos subitens 2.1 a 2.12 são requisitos mínimos necessários, alinhados e aderentes aos principais normativos, resoluções de mercado, a serem aplicados nos ambientes dos fornecedores para proteção das informações, não estando limitados a:

2.1 Política e Organização de Segurança da Informação

O fornecedor deve possuir políticas de segurança da informação aprovadas e disseminadas para todos os colaboradores, expressando suas orientações e apoio, inclusive da alta direção, quanto à segurança da informação e a relação com os requisitos do negócio, leis e regulamentações relevantes.

O fornecedor deve nomear um representante com qualificação técnica apropriada e disponibilidade para coordenar as atividades e demandas relacionadas com segurança da informação na prestação dos serviços e atuar como ponto focal para os temas relacionados junto ao Conglomerado.

2.2 Gestão de Ativos de Informação

O fornecedor deve realizar a gestão dos ativos de informação, no que tange à sua identificação, e definição de papéis e responsabilidades de seus colaboradores para assegurar que as informações recebam um nível adequado de proteção (divulgação não autorizada, modificação, remoção ou destruição), alinhado à classificação das informações atribuída pelo Conglomerado, nos termos do documento que consta as diretrizes de segurança da informação para fornecedores.

No caso dos ativos de informação do fornecedor, o fornecedor concorda em conceder acessos privilegiados, como administradores de domínios, recursos de rede e telecomunicações, aplicações, banco de dados e outros recursos de infraestrutura crítica do fornecedor mediante necessidade e solicitação formal, e estejam de acordo com os papeis e responsabilidades de cada colaborador.

No caso dos ativos de informação do Conglomerado, o fornecedor entende e concorda que acessos privilegiados, como administradores de domínios, recursos de rede e telecomunicações, aplicações, banco de dados e outros recursos de infraestrutura crítica do Conglomerado são concedidos exclusivamente pelo Banco aos seus empregados.

Todos os acessos mencionados acima deverão possuir dupla custódia, revisão periódica, monitoramento, sendo que os respectivos registros deverão ser mantidos como evidência da realização desses processos a ser fornecida ao Conglomerado, mediante solicitação formal do Banco.

Adicionalmente, o fornecedor deve implementar os seguintes mecanismos mínimos de proteção, e devidamente configurados e gerenciados:

a. Antivírus e produtos de gerenciamento de segurança nas máquinas (servidores e estações de trabalho);

b. Bloqueio da liberação de compartilhamentos administrativos;

c. Proteção de tela por inatividade;

d. Bloqueio da adição de contas de administração no grupo administrador local, assim como renomeação e troca de senha;

e. Restrição e monitoramento das portas USB, incluindo o uso de modems e dispositivos de cópia/armazenamento;

f. Administração de sistema operacional deve ser realizada somente por colaboradores e/ou terceiros devidamente credenciados e capacitados para aquela função;

g. Download e *upload* de dados, informações e softwares da Internet devem ser evitados e monitorados;

h. Processo de aquisição de software e seu licenciamento deve ser formalizado e monitorado de forma a garantir a não utilização de softwares não autorizados;

i. Processo de controle e monitoramento de versionamento, atualização e manutenção de software;

j. Procedimento formal e monitoração de uso de equipamentos pessoais na rede da empresa;

k. Procedimento formal e monitoração para acesso remoto, considerando fatores de autenticação forte e mecanismos de criptografia atualizados na conexão e transferência dos dados e informações;

l. A topologia e arquitetura de redes deve ser definida e documentada, contemplando inclusive serviços em nuvem, quando utilizado;

m. Ferramentas que viabilizem a consulta e/ou a manutenção do inventário;

n. Caso aplicável, a contratada deve possuir a certificação com as bandeiras relacionadas aos produtos da contratante, (MasterCard, VISA, Cirrus, Plus, Tecban, e desejável Elo/Discover), identificando e analisando as novas demandas provenientes dos mandates das bandeiras (inclusive Tecban e Febraban) e comunicando a contratada dos impactos, os prazos e frequência, através de uma equipe especializada, conforme fluxo de gestão de demandas definido pelas partes, sem ônus à contratante;

o. Caso a aplicável, a contratada deve possuir a certificação PCI-DSS, com aderência em todo fluxo de processamento (sistemas, Infraestruturas, atendimento à clientes e demais processos) de meios eletrônicos de pagamento. Disponibilizar os resultados obtidos no último período, que deverão estar contidas na resposta deste documento;

p. Caso a aplicável, a contratada deve possuir a certificação ISAE3402 tipo 1 e 2, descrever que informações são disponibilizadas a contratante e em que formato, bem como a cópia do relatório/certificação ISAE3402.

2.3 Segurança em Recursos Humanos

O fornecedor deve assegurar que seus colaboradores entendam suas responsabilidades e estejam em conformidade com os papéis para os quais foram contratados.

Os papéis e responsabilidades dos colaboradores do fornecedor devem ser definidos, revisados e atualizados periodicamente para que possam ser utilizados como referência para a concessão de acessos.

2.4 Segurança Física e Lógica

O fornecedor deve efetuar a gestão de acesso físico e lógico para impedir e/ou prevenir o acesso não autorizado, dano e interferências (perdas, furto ou roubo) aos ativos de informação que possam afetar as operações.

Em caso de uso de local de terceiros, incluindo data centers terceirizados, o fornecedor deverá assegurar que os fornecedores e administradores desses locais possuam controles de acesso físico e lógico implementados de forma a prevenir os eventos indicados acima.

O acesso às instalações deve ser coerente com os papéis e responsabilidades dos colaboradores e devidamente autorizados e validados por seus gestores.

Para os serviços relacionados à atendimento ao cliente (*call center*, cobrança, suporte comercial, entre outros), o ambiente deve ser segregado mantendo os colaboradores que prestam serviços ao Conglomerado apartados fisicamente dos demais ambientes, e alinhados a um procedimento de mesa limpa que assegure que informações do Conglomerado não fiquem expostas ou sejam acessíveis para terceiros não-autorizados (restrição do uso de celular, impressão de documentos, etc.).

2.5 Segurança das Operações e Comunicações

O fornecedor deve efetuar a gestão da operação e ativos de informação (recursos de processamento e armazenamento) que a suporta, de maneira a assegurar que as informações e os recursos estejam protegidos contra ameaças (códigos maliciosos), vazamento e/ou perda de dados e de auditabilidade (falha no registro de eventos e evidências).

O fornecedor deve assegurar que as informações armazenadas estejam disponíveis para que sejam manipuladas ou recuperadas pelo Conglomerado sempre que solicitado, e que possam ser acessadas e consultadas pelo Banco Central do Brasil ou outro órgão governamental de supervisão aplicável.

Além disso, o fornecedor deve assegurar a proteção das informações em redes e recursos de processamento quando transferida dentro da organização e com entidades externas.

Adicionalmente, o fornecedor deve implementar os seguintes mecanismos mínimos de proteção, devidamente configurados e gerenciados:

a. Padrões, processos e/ou ferramentas utilizadas para detectar ataque em sistema de rede (Network IDS, Firewall, WAF, anti-DDoS);

b. Ferramentas e solução contra vazamento de dados e informações (ex.: ferramentas de DLP - *data loss prevention*);

c. Solução implementada e configurada para monitoramento de e-mails (ex.: anti-spam, anti-phishing);

d. Política formal de webmail ao sistema de correio eletrônico, incluindo monitoramento quando o uso é permitido;

e. Software de criptografia de e-mails enviados para internet;

f. Solução e ferramentas de criptografia das informações armazenadas de forma que elas somente possam ser acessadas pelo Banco ou terceiros autorizados pelo Banco;

g. Backup efetuando a gravação de todos os tipos de mensagens das caixas de e-mail (enviadas, recebidas, excluídas);

h. Permissão de acesso e monitoramento do e-mail pessoal através da internet da empresa;

i. Configuração de sistema de gravação telefônica nos ramais de áreas críticas de negócios e garantia de seu armazenamento, recuperabilidade e monitoração, de acordo com as exigências legais;

j. Procedimento para descarte de ativos de informações (papel, disco rígido, computadores);

k. Armazenamento em HSM (Hardware Security Module) das chaves criptográficas necessárias para o processamento de meios eletrônicos de pagamento. As chaves são de propriedade do Emissor, e a Processadora terá apenas acesso para manutenção do que for necessário, sempre de forma autorizada e acompanhada pelo Emissor.

2.6 Controle de Acesso

O fornecedor deve possuir um processo formal de registro e cancelamento de usuário para permitir atribuição de direitos de acesso, de acordo com os papéis e responsabilidades dos colaboradores e demais pessoas envolvidas.

Os acessos devem ser concedidos mediante fluxo formal, contemplando o registro e a aprovação de acordo com a criticidade de cada ativo de informação (por exemplo: sistema, aplicação, banco de dados, diretórios de rede e acessos privilegiados). O monitoramento dos acessos críticos e privilegiados deve ser registrado e mantido como evidência para a conformidade do processo e futuras auditorias.

2.7 Aquisição, Desenvolvimento e Manutenção de Sistemas

2.7.1 Desenvolvimento Seguro

O fornecedor deve possuir um processo de desenvolvimento seguro como parte integrada do ciclo de vida do desenvolvimento do software. Adicionalmente, o mesmo deve possuir um ambiente produtivo, segregado de forma física e lógica, do ambiente de testes/desenvolvimento.

Em relação aos itens de desenvolvimento seguro, o fornecedor deverá ter implementado os seguintes itens, seguindo algum *framework* ou entidade de mercado reconhecidos:

a. Requisitos de segurança para desenvolvimento seguro (web/mobile/serviço)

b. Modelagem de Ameaça

c. Fluxo de Dados e Processo

d. Diagramas (Caso de Uso, Cenários de Uso e Casos de Abuso)

e. SAST - *Static Application Security Testing*

f. DAST - *Dynamic Application Security Testing*

g. *Ethical Hacking Test*

h. Revisão de Código

i. Treinamento e/ou *Workshop* sobre desenvolvimento seguro

j. Política de Desenvolvimento Seguro

k. Política de Gestão de Vulnerabilidade

O fornecedor é responsável por executar uma análise de segurança na aplicação/serviço/software, por acompanhar as vulnerabilidades e corrigir os apontamentos identificados, antes de promover novas versões em ambiente produtivo. Caso o fornecedor não execute a análise, o mesmo deverá permitir a execução da avaliação pela equipe do Conglomerado e posteriormente deverá priorizar as vulnerabilidades identificadas.

2.7.2 Monitoração da Infraestrutura

O fornecedor deve fornecer ferramentas para consulta da disponibilidade, saúde e desempenho do serviço/infraestrutura contratada e preferencialmente dispor de comunicação via SNMP ou API para encaminhamento dos eventos e status para as consoles de gerenciamento de serviços e disponibilidade utilizadas pelo Conglomerado.

Declarar a agenda de manutenções programadas (paradas físicas ou atualizações de software) que possam causar parada completa ou parcial do ambiente/serviço contratado.

Além disso, o fornecedor deve dispor de um catálogo de serviços além de mantê-lo atualizado e sempre que possível informar (por e-mail, *workshops*, treinamentos, etc.) sobre os novos serviços ofertados, para que o Banco fique ciente dos novos serviços.

Quando possível, o fornecedor deve disponibilizar opções de armazenamento das informações, incluindo opções de baixo custo (mas que atendam aos requisitos de segurança), para retenção das informações a longo prazo.

2.7.3 Computação na Nuvem

Caso o fornecedor seja um provedor de serviços de computação em nuvem (IaaS, PaaS ou SaaS), ou faça uso de tecnologia de computação em nuvem como parte da prestação dos serviços para o Banco, os controles adicionais devem ser implementados:

- Conexão ao ambiente para o provisionamento, orquestração e automação de novos serviços ou infraestrutura através de APIs que serão utilizadas por soluções de gerenciamento de computação em nuvem hibrida (pública e privada) disponíveis no mercado.
- Os dados sensíveis e/ou confidenciais devem ser transmitidos, registrados e/ou armazenados de forma segura entre fornecedores e entre o fornecedor e o Conglomerado;
- O sistema deve fazer uso de HTTPS em todas as páginas de navegação, porém se em alguma parte não for possível a utilização do mesmo minimamente deve-se utilizar nas páginas de autenticação;
- Fazer uso de um canal seguro para a troca ou redefinição de chaves criptográficas atualizadas;
- Quando as chaves são armazenadas em seu sistema, elas devem estar adequadamente protegidas e somente acessíveis ao pessoal apropriado em uma base de conhecimento devidamente controlada;
- Os certificados HTTPS devem ser assinados por uma CA confiável. O nome do certificado deve ser igual ao FQDN do site no qual ele será utilizado. O certificado deve ser válido;
- Deve-se impedir que as credenciais de acesso (login e senha) sejam armazenadas diretamente no código do software;
- O processo de redefinição de senha deve ser baseado em questões que são difíceis de adivinhar por meio de força bruta. A mensagem de erro não deve expressar nenhuma informação relevante da conta;
- Suportar múltiplos métodos de autenticação de usuários, como tokens, OTPs via SMS e similares;
- Tokens de sessão devem ser gerados quando o usuário se autentica no sistema e quando o nível de privilégio do usuário precisa ser alterado. Além disso, se o status de criptografia mudar, o token de sessão sempre deve ser atualizado;
- O cookie de sessão deve ser definido com os sinalizadores "HTTP Only" e "Secure";
- Para cada campo de entrada do usuário, deve haver validação no conteúdo de entrada. Fazer uso de *whitelisting* na entrada é a abordagem requerida sempre que possível;
- Deve-se incorporar um valor aleatório que não é conhecido por terceiros no formulário HTML. Este token de proteção CSRF deve ser exclusivo para cada solicitação;

- Ao hospedar conteúdo carregado pelo usuário que pode ser visualizado por outros usuários, deve-se usar o cabeçalho "X-Content-Type-Options: nosniff" evitando que os navegadores tentem adivinhar o tipo de dados;
- Deve-se validar toda e qualquer entrada de dados no sistema;
- Faça uso de cabeçalhos de Política de Segurança de Conteúdo (CSP), como: X-XSS-Protection e Public-Key-Pins;
- Estabelecer procedimento para federação (via SAML ou qualquer integração com diretórios sob premissas) com redes corporativas;
- SLA de disponibilidade, de atendimento e endereçamento de chamados, política de continuidade/resiliência/recuperação de desastres, redundância de infraestrutura e plataforma, política de backup, direito de auditar periodicamente;
- Reportes de cumprimento ou descumprimento do SLA entregues de forma periódica;
- Armazenamento das informações do banco de forma segregada e exclusiva;
- Suporte para ambientes híbridos quando as soluções forem desenhadas para trabalhar com troca de informações entre ambientes de computação em nuvem e ambientes do Banco Votorantim;
- Serviço de *autoscaling*, que permita ao Banco adicionar e remover capacidade ou outros recursos computacionais de acordo com suas políticas e métricas;
- Indicar país e região do armazenamento/processamento de dados no Brasil ou em países/regiões onde o Banco Central possui convênio de colaboração com entidades reguladoras;
- Políticas de acesso com logs, definição de perfis (RBAC), documentação do permissionamento de telas e transações, mapa de acessos;
- Trilhas de auditoria (criação, exclusão, manutenção, alteração) de perfis de acesso e outras funcionalidades do sistema;
- Exportação das informações do banco mantidos no ambiente e sistemas do fornecedor em formato aberto;
- Portal ou outro canal para acesso à evidências, documentação e relatórios de auditoria de procedimentos e controles para a proteção das informações do banco;
- Portal ou outro canal para monitoramento do estado do serviço e cálculo de cumprimento dos indicadores e níveis de serviço acordados; e
- Portal ou outro canal de comunicação para informar sobre eventuais limites, problemas e interrupções de serviço;
- O fornecedor deve realizar testes de intrusão (EHT-Ethical Hacking Test) em seu ambiente e evidenciar o resultado ou apresentar uma certificação que comprove os controles de segurança ao Banco. (aplicável para contratação SaaS);
- O fornecedor deve manter atualizado o ambiente onde os serviços são disponibilizados (aplicável para contratação SaaS, PaaS e IaaS). As evidências devem ser geradas e apresentadas para a avaliação do Banco);

- O fornecedor deve também assegurar que a monitoração da capacidade (*capacity)* dos serviços prestados ao Banco esteja adequada à carga de trabalho contratada (aplicável para contratação IaaS).

2.8 Gestão de Incidentes

Soluções ITSM do fornecedor devem ter a capacidade de abrir chamados automáticos através de recebimento de e-mail via SMTP, Trap via SNMP ou REST/API originadas do Banco.

O fornecedor deve efetuar a gestão de incidentes para assegurar um processo efetivo na atuação de pessoal treinado e equipado para detectar, relatar e tratar fragilidades e eventos de segurança da informação.

É necessário a presença de monitoração e resposta tempestiva para retomada da disponibilidade do serviço com menor impacto ao negócio, como por exemplo, o uso de serviços de segurança gerenciados (SOC - *security operation center*).

Caso o fornecedor tome conhecimento ou possua suspeita da ocorrência de um evento ou incidente envolvendo informações ou ativos de informação do Conglomerado, o fornecedor deverá comunicar imediatamente a superintendência da Área Segurança da Informação [csirt@bv.com.br | (11) 5171-4998] e manter a área gestora do contrato informada. Além disso, o fornecedor deve possuir procedimentos para identificação, tratamento, monitoramento e reporte do incidente.

2.9 Gestão da Continuidade do Negócio e Recuperação de Desastres

O fornecedor deve possuir um processo para a gestão de continuidade de negócios e considerar os aspectos de segurança da informação para assegurar a disponibilidade dos recursos de processamento da informação.

Um local alternativo de trabalho deve ser definido nos casos onde haja total indisponibilidade do local principal, visando a continuidade do fornecimento ao Banco Votorantim, garantindo a mesma qualidade (serviços, rede, link, etc.) do local principal.

O fornecedor deve possuir plano de recuperação em caso de desastres, que descreva o RPO e RTO, SLAs aplicáveis, bem como estratégia para a continuidade das operações/serviços contratados e, divulgar para o Banco. O prazo do plano de recuperação para serviços críticos (autorização, processamento, atendimento) deve estar adequado a estratégia definida pelo Banco.

Os testes de continuidade deverão ser realizados com periodicidade mínima anual e comunicados previamente ao Banco e os resultados e processos verificados deverão ser compartilhados com o Banco. Adicionalmente, quando os testes forem executados pelo Banco, o fornecedor será notificado com antecedência e deverá estar preparado para a participação no teste, caso solicitado.

Eventuais impactos na disponibilidade ou qualidade do fornecimento, necessitam ser imediatamente comunicados ao Banco.

O fornecedor deve desenvolver o backup de seus componentes críticos, bem como de todos os dados do Conglomerado e disponibilizá-los sempre que solicitado.

O fornecedor deve garantir a disponibilidade de todos os dados através de ferramentas de backup, e se possível permitir um *backup/restore* de ambiente híbrido.

O fornecedor deve possuir serviços de alta disponibilidade para garantir a manutenção/estabilidade do serviço/aplicação em caso de desastres.

2.9.1 Governança

Toda e qualquer alteração nos ambientes utilizados pelo Conglomerado que impacte sua disponibilidade deve ser comunicada por escrito pela área responsável pelo ambiente, com antecedência e deve ser reversível.

Alterações e/ou remoções de recursos dos serviços pelo fornecedor devem ser informadas ao Banco por escrito e com antecedência para que as áreas relevantes possam avaliar o impacto e mitigar os problemas dessas alterações e/ou remoções.

O fornecedor deve informar o EoL (*End Of Life*) e o EoS (*End Of Support*) dos Ativos de Informação e Sistemas periodicamente por escrito e com antecedência.

O fornecedor deve disponibilizar ferramentas para consulta dos custos com computação em nuvem com acessos as informações online, histórica com a capacidade de alertas de consumo quando atingir 80% do consumo da subscrição além de módulos para predição de utilização com base em dados informados pelo Conglomerado.

Deve, também, atender à exigência regulamentar para que o dado armazenado esteja sempre disponível para que manipulado ou recuperado pelo Banco, atendendo desta maneira, às solicitações do Banco Central do Brasil.

2.10 Migração e Expurgo das Informações

Na situação de encerramento de contrato, independentemente da parte solicitante do distrato, o fornecedor deve garantir que todos os dados (por exemplo: arquivos, informações em banco de dados, backups e arquivos de recuperação em casos de incidentes, *on premise* ou nuvem) sejam completamente migrados para o ambiente do banco e, posteriormente expurgados de sua propriedade exclusiva, com o acompanhamento dos representantes a serem devidamente informados pelo Banco, utilizando ferramentas que garantam que as informações foram permanentemente deletadas, exemplo WIPE.

Na impossibilidade de acompanhamento do processo pelo Banco, caso seja solicitado, o fornecedor deverá apresentar um laudo sobre o processo de expurgo, emitido por uma consultoria a ser contratada por este.

2.11 Análise e Avaliação de Vulnerabilidades

O fornecedor deve possuir processo formal para a realização de testes de vulnerabilidades e intrusão em seus dispositivos de rede, telecomunicações, aplicações, estações de trabalho e servidores, de maneira periódica e manter os relatórios, assim como resultados e respectivos planos de ação para mitigação e gestão dos riscos, disponíveis para apresentação ao Banco sempre que solicitado.

Os testes de vulnerabilidades e intrusão deverão ser realizados pelo fornecedor por colaboradores competentes e capacitados, visando a proteção de todo o perímetro interno e externo, com uma análise ativa de vulnerabilidades, fraquezas e deficiências técnicas da infraestrutura física e lógica. O Banco poderá realizar esses testes, com time próprio ou terceiro contratado.

2.12 Subcontratação de Serviços pelo Fornecedor

Caso o fornecedor subcontrate outro prestador de serviço para realizar as atividades ou processamento/armazenamento de informações referentes ao contrato, deve informar ao banco e garantir que seu prestador siga todos os mesmos requisitos de segurança da informação apresentados neste documento, bem como, possibilitar avaliações do Conglomerado em seu ambiente para verificação dos controles de segurança da informação.

3. Conformidade

O fornecedor deverá assegurar que a segurança da informação seja implantada e operada em conformidade com as políticas e procedimentos da organização, de maneira a evitar quaisquer violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança que afetem ao Banco.

4. Avaliação de Segurança da Informação em Fornecedores

A Área IAM Controles e Riscos do Conglomerado estabelece o seu processo de avaliação periódica de controles e riscos nos ambientes dos fornecedores, com base nas informações obtidas com a área contratante e com o fornecedor.

Para que o Banco realize este processo de avaliação, o fornecedor deve atender às solicitações indicadas na carta comunicado, encaminhada pelo gestor responsável pela contratação ou seu representante, e cumprir os prazos estabelecidos para as etapas de:

a. Preenchimento do questionário de avaliação dos controles de segurança da informação do fornecedor;

b. Agendamento da visita técnica no local de prestação/fornecimento dos serviços, conforme aplicável.

A avaliação de controles e riscos nos ambientes e locais do fornecedor pode ser conduzida pelas seguintes Áreas do Conglomerado Votorantim: Segurança da Informação, Compliance, Controles Internos, Riscos, Tesouraria, TI e outras áreas do Banco, por auditor externo ou representante autorizado. É obrigatória a presença de colaboradores do fornecedor que conheçam os aspectos contemplados no questionário durante a visita técnica.

Em caso de identificação de melhorias ou vulnerabilidades no ambiente pelo Banco, o fornecedor deve definir o plano de ação em conjunto com os responsáveis do Banco. O acompanhamento da evolução dos planos será realizado pelo gestor responsável pela contratação com apoio da Segurança da Informação.

5 .Aspectos Gerais

O fornecedor entende e concorda que este documento pode sofrer atualizações e alterações periódicas. O Banco comunicará o fornecedor das atualizações e alterações, sendo que o fornecedor deverá se adequar a tais alterações dentro do prazo acordado com o Banco. Referidas atualizações e alterações serão acompanhadas nos fóruns de governança internos. O fornecedor deverá fornecer ao Banco evidências das adequações efetuadas, incluindo relatório detalhado e respectivos planos de ação, quando aplicável.