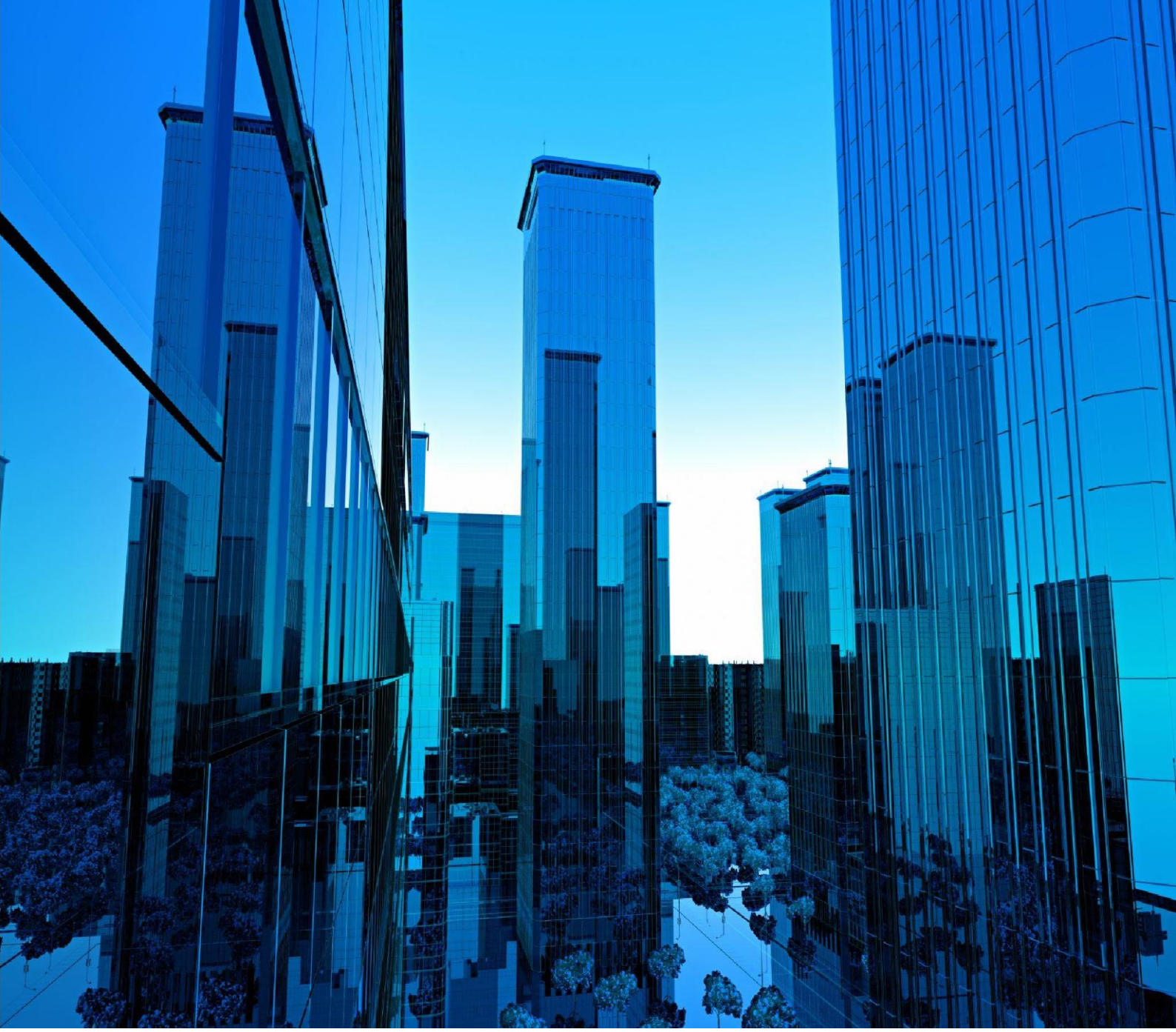

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. DEFINIÇÃO

A política de Segurança Cibernética descreve o conjunto de diretrizes que orientam o uso aceitável dos ativos de informação e tecnológicos, baseada nos princípios de confidencialidade, integridade e disponibilidade.

2. PÚBLICO-ALVO

- Banco Fibra S.A, incluindo Filial Cayman, e suas controladas (“Banco Fibra” ou “Banco”) e Terceiros Prestadores de Serviço.

3. OBJETIVO

Esta política tem por objetivo:

- Estabelecer diretrizes e normas de segurança da informação e segurança cibernética, que permitam aos colaboradores adotarem padrões de comportamento seguro, adequados às suas metas e necessidades;
- Prevenir possíveis causas de incidentes de segurança cibernética;
- Capacitar os colaboradores no que se refere à prevenção, detecção e resposta a incidentes de segurança cibernética;
- Orientar os colaboradores quanto a adoção de controles e processos para atendimento dos requisitos de segurança da informação e segurança cibernética;
- Resguardar ativos de informação e/ou tecnológicos, garantindo requisitos de confidencialidade, integridade e disponibilidade;
- Minimizar os riscos de perdas financeiras, da confiança de clientes ou de qualquer outro impacto negativo no negócio como resultado de falhas de segurança.

4. RESPONSABILIDADES

4.1. RESPONSABILIDADES DOS COLABORADORES E TERCEIROS

- Seguir as diretrizes definidas nesta política e normativos de Segurança da Informação, assim como as orientações transmitidas pela área de Segurança da Informação;
- Comunicar, imediatamente, a área de Segurança da Informação, a suspeita de Incidente de Segurança Cibernética através de telefone, e-mail, chat ou pessoalmente;
- Não divulgar informações sobre incidente de Segurança Cibernética e/ou ocorrências de segurança da informação para entidades ou pessoas internas ou externas ao Banco Fibra, Filial Cayman e suas controladas, sem aprovação expressa e formal da área de Segurança da Informação, assim como do Comitê Executivo;

- Revisar o documento de análise de impacto nos negócios (BIA), sempre que solicitado;
- Reportar, tempestivamente, à área de Segurança da Informação, mudanças significativas em processos, recursos tecnológicos e/ou pessoas críticas, para atualização do documento de análise de impacto nos negócios (BIA).

4.2. RESPONSABILIDADES DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

- Elaborar, implantar e disponibilizar as políticas, normas e procedimentos de Segurança da Informação, garantindo que os requisitos de confidencialidade, integridade e disponibilidade da informação sejam atingidos por meio de adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Conscientizar e treinar os colaboradores sobre as melhores práticas de Segurança da Informação e Segurança Cibernética;
- Tratar incidentes de segurança cibernética, garantindo que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicar as autoridades competentes;
- Melhorar, continuamente, a gestão de Segurança da Informação e Segurança Cibernética, por meio de definição e revisão sistemática de objetivos de segurança em todos os níveis do Banco Fibra;
- Atender requisitos de Segurança da Informação e Segurança Cibernética, aplicáveis ou exigidos pela regulação vigente, bem como por cláusulas contratuais;
- Garantir a continuidade dos negócios através da melhoria contínua de planos de continuidade;
- Coordenar a revisão de processos críticos e impacto em negócios em caso de interrupção no “BIA” – *Business Impact Analysis*, de forma anual ou sempre que mudanças significativas nos negócios ocorrerem;
- Coordenar exercícios periódicos anuais para avaliação dos cenários de contingência previstos no Plano de Continuidade de Negócios (PCN);
- Treinar, de forma periódica, o pessoal envolvido nos procedimentos de reposta em situações de contingência.

4.3. RESPONSABILIDADES DA ÁREA JURÍDICA

- Elaborar, quando necessário e aplicável, as notificações e os comunicados a respeito de eventual incidente de segurança para os titulares e ANPD, a ser enviado pelo Encarregado;
- Identificar obrigações contratuais e regulatórias de reportar os incidentes de Segurança Cibernética, relacionado a dados pessoais a terceiros, órgãos reguladores/governamentais (que não a ANPD), bem como elaborar e enviar as respectivas notificações, quando demandado;

- Recomendar, juntamente com o Encarregado e submeter para a aprovação da alçada competente, conforme aplicável, a adoção de medidas de conciliação e compensação de danos causados aos titulares.

4.4. RESPONSABILIDADES DA ÁREA DE COMPLIANCE

- Comunicar, tempestivamente, ao Banco Central e/ou a outros órgãos reguladores, incluindo, mas não se limitando, à Autoridade Nacional de Proteção de Dados (ANPD), com o apoio de Segurança da Informação ou Tecnologia da Informação, conforme aplicável, incidentes de segurança cibernética e/ou interrupções de serviço classificados com severidade extrema, que se configurem situações de crise na instituição ou ocorridos em empresas prestadoras de serviços. As providências para reinício das atividades da instituição devem ser informadas na mesma comunicação supracitada;
- E, anualmente, enviar, para os devidos órgãos reguladores, quando assim for exigido, o Relatório de Incidentes de Segurança Cibernética, identificados e tratados no ano anterior.

4.5. RESPONSABILIDADES DA ALTA ADMINISTRAÇÃO

- Comprometer-se com a melhoria contínua dos procedimentos relacionados à Segurança da Informação e Segurança Cibernética, assim como com a disseminação da cultura de Segurança da Informação;

- Adotar medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da instituição;

- Estar envolvida e comprometida com a disseminação da cultura e melhoria contínua dos processos relacionados à Segurança Cibernética. Conscientizar, de forma contínua, os colaboradores, sobre a importância dos exercícios de continuidade de negócio, além de apoiar a atualização tempestiva das informações relativas a processos, recursos tecnológicos e pessoas críticas. O Diretor responsável por Segurança da Informação e Cibersegurança é responsável pelo devido cumprimento desta política e pela execução do Plano de Prevenção e Resposta a Incidentes.

5. GESTÃO DE RISCOS CIBERNÉTICOS

A gestão de riscos cibernéticos é uma responsabilidade da área de Segurança da Informação. Este processo identifica os requisitos de segurança relacionados às necessidades do Banco Fibra. A gestão de riscos cibernéticos é contínua e define contextos internos e externos para avaliação, além de tratar dos riscos identificados de modo que sejam reduzidos à níveis aceitáveis.

6. USO ACEITÁVEL DE RECURSOS TECNOLÓGICOS

Os recursos de tecnologia devem ser utilizados de maneira adequada, ética e segura, visando proteger os ativos da informação, como dados, sistemas e redes, contra acessos não autorizados, mau uso, roubo de informações, entre outros, conforme definido no termo de responsabilidade denominado “Termo de responsabilidade sobre o uso de bens de tecnologia” e no normativo 01-09-17/1 NI Uso aceitável de ativos da informação.

7. CONSCIENTIZAÇÃO E TREINAMENTOS DE SEGURANÇA DA INFORMAÇÃO

O Banco Fibra define diretrizes de educação contínua para o aculturamento de boas práticas de Segurança e disseminação de conhecimento para utilização no dia a dia dos colaboradores e prestadores de serviço, seja para fins profissionais quanto para fins pessoais.

O programa de conscientização de Segurança da Informação está distribuído entre as seguintes ações, mas não limitado a:

Tipo	Observação
Adesão à política de Segurança Cibernética	No ato da contratação.
Treinamento de Integração	Realizado presencialmente após a contratação dos colaboradores como parte do programa de integração da área de Pessoas.
Treinamento Online	Realizado junto com os demais treinamentos obrigatórios, logo após a contratação do colaborador, com avaliações periódicas.
Informativos de segurança para os colaboradores	Realizados mensalmente e conforme a necessidade, para os colaboradores.
Informativos de segurança para clientes, sobre precauções na utilização de produtos e serviços do Banco Fibra	Realizados, periodicamente, através dos canais de comunicação oficial do Fibra
Informativos e treinamento de segurança para prestadores de serviço	Informativos e Treinamentos são disponibilizados mensalmente por e-mail.
Avaliações de maturidade	Realizados anualmente
Simulações de e-mails maliciosos (*phishing*)	Realizados periodicamente

Políticas, normativos e procedimentos	Divulgado por e-mail no momento da sua publicação e disponíveis na intranet para consulta.

No site institucional do Banco Fibra deve ser divulgado um resumo desta política, contendo as linhas gerais de seu conteúdo para fins de conscientização e divulgação da cultura de Segurança.

8. PROTEÇÃO E CLASSIFICAÇÃO DE DADOS

As informações do Banco Fibra devem ser classificadas utilizando-se os rótulos “Pessoal”, “Pública”, “Restrita” ou “Restrita ao Fibra” conforme manuseadas e descartadas conforme as diretrizes definidas no normativo 01-09-14/1 NI Classificação da Informação, devendo todos os colaboradores terem o conhecimento de como as informações devem ser tratadas durante o seu ciclo de vida dentro do Banco Fibra.

9. GESTÃO DE VULNERABILIDADE E CONFORMIDADE

O Banco Fibra deve possuir processos para garantir que as vulnerabilidades e não conformidades sejam identificadas e tratadas de maneira eficaz, garantindo a conformidade com regulamentações e padrões de segurança relevantes.

Dessa forma, aumentando a segurança dos sistemas e protegendo os dados e informações contra ameaças cibernéticas e violações de segurança, estes são especificados na norma 01-09-11/1 NI Gestão de Vulnerabilidades e Patches.

10. MONITORAMENTO DE SEGURANÇA

Para garantir a segurança do ambiente cibernético, o Banco Fibra deve utilizar ferramentas, processos e procedimentos bem definidos, para monitorar, continuamente, as atividades e eventos nos sistemas e redes, a fim de identificar e responder, rapidamente, a possíveis ameaças de segurança, violações de políticas ou incidentes de segurança cibernética, garantindo uma detecção precoce de atividades maliciosas.

11. GESTÃO DE IDENTIDADES E ACESSOS

A Gestão de identidade e acessos deve possuir diretrizes definidas para controlar e monitorar as permissões para acessar os sistemas e recursos. Isso inclui a definição de processos, procedimentos e tecnologias para a concessão, manutenção e revisão dos acessos, garantindo que apenas pessoas autorizadas tenham acesso aos recursos necessários para execução de suas atividades, conforme especificados na norma 01-09-12/1 NI Gestão de Identidade e Controle de Acessos.

Os parâmetros de senhas são definidos para garantir que os sistemas possuam um gerenciamento **de** senhas forma segura, conforme especificados na norma 01-09-13/1 NI Parâmetros de Senha.

12. RESPOSTAS A INCIDENTES DE SEGURANÇA CIBERNÉTICA

O Banco Fibra deve definir diretrizes para prevenir, responder e tratar adequadamente incidentes de Segurança Cibernética que estejam impactando, ou possam vir a impactar ativos/serviços de informação ou recursos tecnológicos da instituição.

12.1. DEFINIÇÕES

Para tratamento de incidentes, define-se:

- **Dados Pessoais:** Qualquer informação relativa a uma pessoa física, identificada ou identificável, independente se funcionários, clientes ou terceiros;

- **Titular**: Pessoa física a quem se referem os dados pessoais;

- **Encarregado ("DPO")**: Pessoa indicada para atuar como canal de comunicação entre o Banco Fibra, Filial Cayman e suas controladas, aos titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados (ANPD);

- **Eventos:** Quaisquer ocorrências observáveis em um sistema ou rede;

- **Ofensas:** Eventos correlacionados ou agregados, com consequências, ou possíveis consequências negativas, para o ambiente tecnológico ou de negócios. As ofensas devem ser analisadas e podem configurar falso-positivo;

- **Incidente de Segurança Cibernética:** Violações ou ameaças iminentes de violação às políticas de Segurança, políticas de uso aceitáveis ou melhores práticas de Segurança. São exemplos de incidentes, mas não limitados a:

  – Tentativas (bem-sucedidas ou não) de obter acesso não autorizado a sistemas ou aos seus dados;

  – Interrupção ou negação indesejadas de serviços por meio de ataque cibernético;

  – Vazamento ou roubo de dados;

  – Uso não autorizado de recursos tecnológicos.

- **Risco ou Dano Relevante:**
    - Sob a ótica de vazamento de dados, quando o incidente de segurança puder afetar significativamente os interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios: (i) dados pessoais sensíveis; (ii) de crianças, de adolescentes ou de idosos; (iii) dados financeiros; (iv) dados de autenticação em sistemas; (v) dados protegidos por sigilo legal, judicial ou profissional; ou (vi) dados em larga escala.
    - Sob a ótica do ambiente cibernético, quando a estrutura operacional do Banco estiver sob risco de interrupção de funcionamento decorrente de um incidente de segurança cibernética.

12.2. DIRETRIZES SOBRE PREVENÇÃO E RESPOSTA A INCIDENTES

Encarregado:

- No caso de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, o Encarregado deve comunicar à ANPD, exclusivamente, através do preenchimento do formulário eletrônico disponibilizado pela ANPD no sistema SUPER/ANPD, acompanhado de documento comprobatório de vínculo contratual, empregatício ou funcional, ou por meio de representante constituído, acompanhado de instrumento com poderes de representação junto à ANPD;
- Deve fazer a comunicação do incidente de segurança para a ANPD e para os titulares em até 3 (três) dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica, contados do conhecimento de que o incidente afetou dados pessoais. Se necessário, poderá complementar as informações fornecidas na comunicação do incidente, fundamentadamente, em até 20 (vinte) dias úteis, contados da data da comunicação inicial;
- Deve ser juntado ao processo de comunicação de incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados;
- Deve constar da comunicação do incidente, à ANPD, as seguintes informações: (i) a descrição da natureza e da categoria de dados pessoais afetados; (ii) o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos; (iii) as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial; (iv) os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares; (v) os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo; (vi) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares; (vii) a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador; (viii) os dados do encarregado ou de quem represente o controlador; (ix) a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte; (x) a identificação do operador, quando aplicável; (xi) a descrição do incidente, incluindo a causa principal,

caso seja possível identificá-la; e (xii) o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

- Deve constar da comunicação do incidente, aos titulares, as seguintes informações: (i) a descrição da natureza e da categoria de dados pessoais afetados; (ii) as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (iii) os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares; (iv) os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo; (v) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis; (vi) a data do conhecimento do incidente de segurança; e (vii) o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado;
- A comunicação do incidente aos titulares deve ser realizada com o uso de linguagem simples, de fácil entendimento e deve ocorrer de forma direta e individualizada, caso seja possível identificá-los;
- Na impossibilidade de notificar os titulares de forma individualizada, deve ser comunicado o incidente em meios de divulgação disponíveis (sítio eletrônico, aplicativos, mídias sociais, canais de atendimento ao titular), de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, 3 (três) meses.

Segurança da Informação:

- Deve registrar todos os incidentes confirmados para fins consultivos e/ou regulatórios, mesmo aqueles que não precisem ser reportados à ANPD, conforme Anexo I – Modelo de Formulário para Reporte de Resposta a Incidentes Cibernéticos, observado que: (a) o registro deve ser mantido pelo prazo mínimo de 5 anos, contados da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção; e (b) o registro do incidente deverá conter, no mínimo: (i) a data de conhecimento do incidente; (ii) a descrição geral das circunstâncias em que o incidente ocorreu; (iii) a natureza e a categoria de dados afetados; (iv) o número de titulares afetados; (v) a avaliação do risco e os possíveis danos aos titulares; (vi) as medidas de correção e mitigação dos efeitos do incidente, quando aplicável; (vii) a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e (viii) os motivos da ausência de comunicação, quando for o caso;
- Analisar em relação à causa e impacto, bem como controlar seus efeitos, inclusive aqueles que possam ocorrer em empresas prestadoras de serviços considerados críticos, contratadas pelo Banco Fibra, Filial Cayman e suas controladas;
- Deve compartilhar com os demais participantes do mercado financeiro indicadores de comprometimento relativos a incidentes de segurança cibernética relevantes observados em seu ambiente. Para tal, utilizar-se-á plataforma definida por federação ou associação representante do segmento;

- Apoiar o Encarregado nas eventuais comunicações de Incidente de Segurança Cibernética ao Banco Central e/ou a outros órgãos Reguladores, incluindo, mas não se limitando, à Autoridade Nacional de Proteção de Dados (ANPD), e aos Titulares dos Dados Pessoais;
- Deve anualmente confeccionar relatório com todos os incidentes de segurança cibernética identificados e tratados no ano anterior (“Relatório”).

O Relatório deve contemplar as seguintes informações:

– A efetividade da implementação das ações para reposta e prevenção a Incidente de Segurança Cibernética;

– Resumo dos resultados obtidos na implementação das rotinas, procedimentos, controles e tecnologias utilizadas na prevenção e resposta a incidentes;

– Incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

– Resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por Incidente de Segurança Cibernética.

O Relatório supracitado deve, conforme prazo estipulado pelos órgãos reguladores, ser:

– Submetido ao Comitê de Gestão de Riscos;
– Submetido ao Comitê de Privacidade, sempre que o Relatório contemple Incidente de Segurança Cibernética relacionado a Dados Pessoais;
– Aprovado pelo Conselho de Administração;
– Armazenado por, minimamente, 5 (cinco) anos.

Quando o Incidente de Segurança Cibernética envolver Dados Pessoais, deve:

– Identificar o nível de severidade do incidente conforme critérios definidos neste documento, a fim de determinar quando este deverá ou não ser reportado aos Titulares e/ou à ANPD;

– Recomendar a forma de posicionamento público do Banco, com auxílio do Jurídico, na hipótese de Incidente de Segurança Cibernética, quando cabível;

– Informar, obrigatoriamente, o Diretor responsável por Segurança da Informação, o Jurídico e o Encarregado sobre incidentes de segurança cibernética através dos meios de comunicação disponíveis no momento do incidente;

12.3. PRIORIZAÇÃO E SEVERIDADE

Qualquer incidente de Segurança Cibernética, confirmado ou sob suspeita, relacionado à segurança de ativos de informação, violação de política ou de dados pessoais, pode ser classificado com severidade Irrelevante, Baixa, Média, Alta ou Extrema, com base nos seguintes parâmetros técnicos utilizados na classificação de relevância dos incidentes:

Impacto	Descrição
Funcional nos Negócios	Deve-se considerar como o incidente impacta as funcionalidades existentes no sistema ou ambiente afetado. Deve-se considerar ainda, os possíveis impactos futuros caso o incidente não seja contido imediatamente.
Informação	Deve-se considerar como uma possível exfiltração de informação pode impactar a instituição, de forma geral.
Capacidade de Recuperação do Incidente	Deve-se considerar o esforço necessário para se recuperar de um incidente, considerando, cuidadosamente, o custo que o esforço da recuperação irá criar, além de outros requisitos relativos à reposta à incidentes.
Financeiro	Deve-se considerar o impacto do incidente em relação a perdas financeiras pela instituição.
Reputacional	Deve-se considerar o impacto do incidente na imagem do banco de forma local, nacional ou internacional.
Em clientes	Deve-se considerar o impacto do incidente nos clientes da instituição.
Dados Pessoais	Deve-se considerar o impacto de possível violação de dados pessoais.

Nos casos de violação de política, cabe a área de Segurança da Informação determinar a severidade do incidente com base nas observações feitas durante a investigação. Incidentes que infrinjam ou atentem contra políticas de Segurança Cibernética, que não se enquadrem nos parâmetros supracitados, devem ser classificados pela área de Segurança da Informação, conforme Anexo I – Modelo de Formulário para Reporte de Resposta a Incidentes Cibernéticos.

12.4. SEVERIDADE DOS INCIDENTES

Adicionalmente, os incidentes de Segurança Cibernética que envolvam, ou não, dados pessoais, deverão ser classificados pela área de Segurança da Informação, com o apoio do Grupo de Crise1, quando necessário, baseado nos seguintes parâmetros.

Nível de Severidade	Tipo de Impacto	Perda Financeira Potencial / Percebida

Irrelevante	Eventos sem maior impacto, com finalidade informativa.	N/A
Baixo	Indisponibilidade abaixo de 1 hora, ataque cibernético de menor impacto e perda financeira conforme coluna ao lado.	> R$ 10.000 e < R$ 50.000
Médio	Critérios de baixa severidade acrescido de: Perda financeira conforme coluna ao lado e vazamento de dados pessoais; danos a sistemas ou fraude.	> R$ 50.001 e < R$ 250.000
Alto	Critérios de média severidade acrescido de: Perda Financeira conforme coluna ao lado e vazamento de dados pessoais, fraude ou indisponibilidade entre 1 e 4 horas	< R$ 250.001 e < R$5.000.000
Extremo	Critérios de alta severidade acrescido de: Perda financeira conforme coluna ao lado e vazamento de dados pessoais, danos a sistemas, fraude, violação de legislação/regulação, indisponibilidade maior que 4 horas ou casos deliberados pelo Grupo de Crise como sendo de severidade extrema.	> R$ 5.000.001

(1) **Grupo de Crise**

*Na identificação de incidentes de segurança cibernética de severidade **extrema**, o Grupo de Crise deve ser acionado para avaliação e deliberação sobre a declaração ou não de estado de crise. Interrupções às operações que tenham duração superior a 04 horas devem ser imediatamente reportadas e avaliadas por este grupo. O Grupo de Crise é composto por pelo menos dois membros votantes do Comitê de Gestão de Riscos (CGR). As atualizações sobre quaisquer incidentes devem ser comunicadas tempestivamente ao Comitê Executivo.*

Poderá haver calibragem quanto à definição do nível de severidade (*upgrade* ou *downgrade*) sugerido por Segurança da Informação para os casos mais graves, desde que devidamente justificados. A referida calibragem deverá ser deliberada pelo Grupo de Crise, em conjunto com o Encarregado.

12.5. DEFINIÇÃO DE AUTORIDADES

Definição de Autoridades		
Atividade	**Observações**	**Autoridade**
Confiscar equipamentos	Remoção para investigação forense	Membro do Comitê Executivo
Desconectar equipamentos	Desconexão para contenção de incidentes	Área de Segurança da Informação
Monitorar atividades suspeitas		
Eventos genéricos	Navegação na internet, prevenção de vazamento de dados, correlação de eventos	Analistas de SI
Eventos com possibilidade de quebra de privacidade	Abertura de caixas de correio ou outros meios de comunicação, arquivos locais ou armazenados no Microsoft *Onedrive*	Área de Segurança da Informação Auditoria Interna
Outras situações	A depender do nível de confidencialidade do incidente	Auditoria Interna Área de Segurança da Informação Membro do Comitê Executivo

12.6. ELABORAÇÃO DE CENÁRIOS DE TESTES

Para elaboração de cenários de incidentes a serem considerados nos testes de continuidade de negócio, define-se que:

- Incidentes de Segurança Cibernética devem ser baseados nos casos de uso previstos no Plano de Prevenção e Resposta a Incidentes;

Demais incidentes devem ser testados, minimamente, os aspectos de indisponibilidade física do prédio matriz do Banco Fibra, Filial Cayman e suas controladas e indisponibilidade de zona AWS.

13. GESTÃO DE RISCOS DE SEGURANÇA DE FORNECEDORES

A gestão de riscos de segurança de fornecedores é o conjunto de práticas para identificar e reduzir os riscos de segurança da informação envolvidos na relação com fornecedores e prestadores de serviços terceirizados, garantindo que esses terceiros não representem uma ameaça à segurança das informações do Banco Fibra, Filial Cayman e suas controladas, conforme diretrizes definidas no normativo 01-09-21/1 NI Gestão de Riscos de

Segurança de Fornecedores. Serão considerados para esse processo os fornecedores relevantes, ou seja, aqueles que armazenem ou processem os seguintes tipos de dados em estrutura tecnológica, não pertencente ao Banco Fibra, Filial Cayman e suas controladas:

Atividade	Observações
Informações Cadastrais	Dados relativas à Pessoa Física ou Pessoa Jurídica, endereços de contatos, informações de número de documentos, sócios estatutários, patrimônio, ativos, produtos, tipo de relacionamento.
Dados de Recursos Humanos	Informações de pessoal, médica, e dados similares. Inclui todas as informações cobertas pela lei de privacidade tais como: salários, identificadores de usuários (ID's), perfil pessoal (informações de número de documentos, endereços comerciais e residenciais, números de telefones de contatos), histórico médico e histórico do empregado.
Informações Financeiras de Clientes	Dados que possam revelar investimentos e posições de clientes Pessoa Física ou Jurídica.
Informações de Contratos	Informações relativas aos contratos firmados entre o Banco Fibra, Filial Cayman e suas controladas e os clientes.
Informações de Carteiras de Clientes	Dados que possam revelar os instrumentos, ativos ou posições financeiras de clientes Pessoa Física ou Jurídica, em determinados produtos / período.

Outros fornecedores podem ser considerados relevantes do ponto de vista de Segurança da Informação ou Segurança Cibernética, de acordo com o nível de acesso a dados ao qual está exposto, além de critérios de disponibilidade e confidencialidade.

14. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

O Banco Fibra deve realizar a gestão de continuidade de negócios com soluções, estratégias e procedimentos a serem executados durante eventuais cenários de contingência, alinhados com o propósito e metas estratégicas da instituição. Para tal, o Banco Fibra, Filial Cayman e suas controladas devem possuir um Plano de Continuidade de Negócios (PCN) que cumpra as seguintes funções:

- Identificação de processos críticos e do impacto de interrupções destes processos;
- Visibilidade do risco ao qual a instituição está exposta;
- Resposta eficiente a eventuais incidentes ou interrupções através de planejamento das ações necessárias em situações de contingência;

- Minimização de possíveis impactos às partes interessadas e ao patrimônio da instituição;
- Preservação da reputação da instituição em casos de situações de contingência;
- Treinamento do pessoal envolvido nas respostas às ocorrências de impactos relevantes;
- Atendimento de requisitos regulatórios.

15. ACESSO FÍSICO

A gestão de acesso físico ao Banco Fibra, Filial Cayman e suas controladas é de responsabilidade da área de Suprimentos, assim como a provisão de crachás aos colaboradores. As diretrizes abaixo devem ser observadas:

- Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância é permitido o seu compartilhamento;
- O crachá é de uso obrigatório para colaboradores, terceiros e visitantes, e deve ser portado em local visível durante a permanência nas dependências do Banco Fibra, Filial Cayman e suas controladas;
- Qualquer acesso de visitantes às dependências do Banco Fibra, Filial Cayman e suas controladas deve ser previamente autorizado por um colaborador efetivo da instituição;
- As portas de acesso ao escritório devem ser sempre fechadas após utilização.

16. SANÇÕES E PUNIÇÕES

A área de Segurança da Informação deve realizar monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta política.

As violações a esta política, mesmo que por mera omissão ou tentativa não consumada, bem como às demais normas e procedimentos de Segurança da Informação, podem ser classificadas como incidente de Segurança Cibernética, a depender da gravidade, e são passíveis de penalidades. Casos desta natureza são levados ao Comitê de Ética, a quem compete a avaliação e decisão quanto a aplicação ou não das penalidades acima listadas.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em danos ao Banco Fibra, Filial Cayman e suas controladas, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes, sem prejuízo aos termos descritos nos parágrafos anteriores desta sessão