POLITICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. OBJETIVO

Em atenção à Resolução nº 4.658/18 do Banco Central do Brasil e à Lei n. 13.709/2018, este documento estabelece os princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. PÚBLICO-ALVO

Este documento é dirigido a todos os sócios, administradores, colaboradores, empregados ou não, menores aprendizes, estagiários, correspondentes, prestadores de serviços a terceiros e todas e quaisquer pessoas que tenham acesso aos dados da instituição ou por ela controlados e aos sistemas por ela utilizados.

3. DOS PRINCÍPIOS

As ações da Instituição regem-se pelos seguintes princípios:

I. Confidencialidade: limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

II. Disponibilidade: garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

III. Integridade: garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

4. RESPONSABILIDADES

As responsabilidades atribuídas pela Resolução nº 4.658 do Banco Central do Brasil são distribuídas da seguinte forma:

4.1. Política de segurança cibernética e da informação e plano de ação e de resposta a incidentes

A Política de Segurança Cibernética e da Informação, a execução do Plano de Ação e de Resposta a Incidentes e a melhoria contínua dos procedimentos relacionados com a segurança cibernética são de responsabilidade do Diretor de Risco

4.2. Registro, análise da causa e do impacto e controle dos efeitos de incidentes relevantes

O registro, a análise da causa e do impacto e o controle dos efeitos de incidentes relevantes são de responsabilidade da Gerência Operacional

4.3. Realização dos testes e varreduras periódicos para detecção de vulnerabilidade

A realização dos testes e varreduras periódicos para detecção de vulnerabilidades são responsabilidades da área de tecnologia da informação.

4.4. Manutenção de cópias de segurança dos dados e das informações

A execução dos *backups*, independentemente da plataforma computacional, bem como o descarte de mídias magnéticas oriundas do processo de *backup*, quando aplicável, são responsabilidades da área de tecnologia da informação.

4.5. Documentação da verificação de capacidade do potencial prestador de serviço, das práticas de governança corporativa e da avaliação da relevância do serviço a ser contratado

A atividade de documentação das informações de que tratam os itens 6.12.3, 7.2. e 7.3 desta política, referente à verificação de capacidade do potencial prestador de serviço, das práticas de governança corporativa e referente à avaliação da relevância do serviço a ser contratado, são responsabilidades da Área de Compliance com auxílio da Área de Tecnologia da informação

4.6. Elaboração do relatório anual sobre a implementação do plano de ação e de resposta a incidentes

A elaboração do relatório anual sobre a implementação do plano de ação e de resposta a incidentes, de que trata o item 14 desta política, é responsabilidades da Área de Tecnologia da Informação.

4.7. Comunicação de incidentes de segurança à autoridade nacional de proteção de dados

Em atenção ao Art. 48 da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), será responsabilidade da Gerência Operacional, após ser cientificada pela Área de Tecnologia da Informação, comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, em conformidade com o item 8 desta política.

4.8. Comunicação de incidentes relevantes relacionados ao ambiente cibernético ao Banco Central do Brasil

Em atenção ao Art. 20, inciso III, da Resolução nº 4.658/18 do Banco Central do Brasil, será responsabilidade da Área de Compliance, após ser cientificada pela Área de Tecnologia da Informação, comunicar ao Banco Central do Brasil a ocorrência de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma

situação de crise pela instituição financeira, bem como das providências para o reinício das atividades, em conformidade com o item 9 desta política.

4.9. Comunicação de contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem

Em atenção ao Art. 15 da Resolução nº 4.658/18 do Banco Central do Brasil, será responsabilidade da Gerência Operacional, após ser cientificada pela Área de Tecnologia da Informação, comunicar ao Banco Central do Brasil a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, em conformidade com o item 7.3 desta política.

4.10. Encarregado pelo tratamento de dados pessoais

Em atenção aos arts. 5º, inciso VIII; 23, inciso II; e 41, *caput* e parágrafos, todos da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), na qualidade de "Encarregado pelo Tratamento de Dados Pessoais", pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), são responsabilidades do Gerente Operacional, além das demais atribuições estabelecidas por normas complementares:

I. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II. receber comunicações da autoridade nacional e adotar providências;

III. orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

5. DAS DIRETRIZES DE SEGURANÇA CIBERNÉTICA

A Segurança Cibernética na Instituição segue as seguintes diretrizes:

a) As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) As informações e os dados devem ser utilizados de forma transparente e apenas para as finalidades para as quais foram coletadas.

c) Os procedimentos e os controles deverão abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

d) A identificação daqueles que têm acesso às informações da Instituição deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

e) Somente deve ter concedido acesso às informações e recursos de informação imprescindíveis para o pleno desempenho das suas atividades do indivíduo autorizado

f) A senha é utilizada como assinatura eletrônica, sendo pessoal e intransferível, e deve ser mantida secreta, sendo proibido seu compartilhamento.

g) Devem ser reportados à área de Tecnologia da Informação da Instituição os riscos às informações, bem como eventuais fatos ou ocorrências que possam colocar em risco tais informações, que será responsável pelo registro e controle dos efeitos de incidentes relevantes.

h) As responsabilidades quanto à Segurança Cibernética devem ser amplamente divulgadas a todos aqueles considerados público-alvo desta política, que devem entender e assegurar o cumprimento do aqui disposto.

5.1. Das diretrizes para tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética e da Informação da Instituição em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

5.2. Das diretrizes para classificação de dados e das informações

As informações e os dados sob responsabilidade da instituição serão classificados, conforme descrito no plano de ação, para adequação das estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética.

A referida classificação se dará, considerando a relevância, a confidencialidade e as proteções necessárias, nos seguintes níveis e subníveis:

I. Dado **NÃO** Pessoal: informação não relacionada a pessoa natural identificada ou identificável:

a. Público: aquele explicitamente aprovado por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio. Possuem caráter informativo geral e são direcionadas ao público em geral.

b. Interno: destinado ao uso interno da Instituição disponível para todos os usuários. O acesso às informações dessa natureza, ainda que não autorizado, não afetaria os negócios da Instituição, seus funcionários ou seus clientes, contudo é considerado incidente de segurança de baixa relevância e, portanto, seu responsável está sujeito às sanções cabíveis. Essas informações não exigem proteções especiais salvo aquelas entendidas como mínimas para impedir o acesso não autorizado.

c. Restrito: dado com acesso autorizado a apenas um usuário específico ou grupo de usuários. Diferem das do dado interno uma vez que não está disponível para todos os usuários e eventual divulgação poderia afetar significativamente os negócios da Instituição, funcionários, terceiros, clientes ou outros.

II. Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável:

a. Dado pessoal não sensível: dado pessoal que não seja classificado como sensível pelo art. 5º, inciso II, da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais) e que não possa ser utilizado para fins discriminatórios, ilícitos ou abusivos;

b. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, dado protegido pelo sigilo das operações ativas e passivas e serviços prestados, na forma da Lei Complementar nº 105/01, ou dado que possa ser utilizado para fins discriminatórios, ilícitos ou abusivos, quando vinculados a uma pessoa natural.

A divulgação desses dados é proibida, salvo se solicitada por órgãos fiscalizadores competentes, tais como o Banco Central do Brasil, a Receita Federal do Brasil e a Comissão de Valores Mobiliários ou por decisão judicial.

Os dados pessoais sensíveis deverão ser protegidos de forma mais rígida, incluindo inciativas de rastreabilidade da informação e controle de acesso diferenciado, devendo ser compatível com as funções desempenhadas e com a sensibilidade das informações. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Uma vez classificada a informação deve ser protegida e receber tratamento e armazenamento adequados.

5.3. Das diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios:

Deverão ser elaborados, no âmbito dos testes de continuidade de negócios, cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela instituição, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

Deverão ser consideradas para a elaboração desses cenários a ausência de

ativos, humanos ou tecnológicos, que assegurem à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados considerando as ausências de ativos causadas por:

I. vazamento de dados;

II. indisponibilidade de recursos computacionais;

III. problemas relacionados a software, banco de dados, servidor de aplicação, rede;

IV. quebra da integridade dos dados, via alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados;

V. fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da instituição;

VI. desastres ou catástrofes, naturais ou não;

VII. danos físicos relevantes a instalações ou equipamentos críticos, intencionais ou não;

VIII. falhas no fornecimento de energia elétrica;

IX. ausência de colaboradores.

5.4. Das diretrizes para a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços

Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços, considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

Uma vez identificados os possíveis cenários serão analisados os controles voltados à prevenção e ao tratamento dos incidentes já utilizados pela prestadora, e, caso necessário, deverão ser estabelecidos com a respectiva prestadora de serviços outros procedimentos e controles prevenção e ao tratamento dos incidentes a serem adotados, de forma a suprir as possíveis lacunas relativas à prevenção, detecção e redução da

vulnerabilidade a incidentes relacionados com o ambiente cibernético.

5.5. Das diretrizes para definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

6. PROCEDIMENTOS E OS CONTROLES

Para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, a instituição, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias, adotará os seguintes procedimentos e os controles:

6.1. Autenticação

Em segurança da informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um log in (acesso) em um programa ou computador. A autenticação normalmente depende de um ou mais "fatores de autenticação".

A instituição utiliza mecanismos de autenticação baseada no conhecimento (com login e senha) em vários níveis, delimitando e controlando o acesso às informações.

Todas as informações armazenadas estão protegidas por sistemas que exigem a autenticação prévia para o acesso.

Os acessos à arquivos na rede também exigem autenticação central.

A instituição adota políticas para atualização periódica de senhas, bem como adota padrões de força para as senhas.

As senhas são armazenadas de forma criptografada na base de dados.

Os seguintes acessos exigem autenticação:

- Sistema de e-mails;

- Consultas a base de dados (em todos os canais);
- Sistemas ERP;
- APIs de Integração;
- Diretórios e arquivos na rede;
- Estação de trabalho;

6.2. Criptografia

Esta instituição classifica suas informações de acordo com o seu sigilo. Assim criptografa as informações consideradas sigilosas, indiferente se estão na base de dados ou em sistemas de arquivos na rede.

Para a base de dados, a maioria dos SGBD (Sistemas Gerenciadores de Base de Dados) comercializados, possuem suporte nativo à criptografia de informações.

Para os sistemas de arquivos, é utilizado o sistema nativo da solução de endpoint, do fabricante Kaspersky.

6.3. Prevenção e detecção de intrusão

Esta instituição utiliza a solução da Fortinet. Ele monitora a atividade em tempo real dos dados e complementa o IDS/IPS. A solução não inclui apenas a detecção de ransomware baseada em assinatura, mas também reconhece as características e o comportamento de um ataque.

6.4. Prevenção de vazamento de informações

Esta instituição também utiliza a Solução de DLP, da Safetica, para prevenção e rastreabilidade de vazamento de informações.

6.5. Testes e varreduras periódicos para detecção de vulnerabilidades

Esta instituição utiliza a ferramenta Nessus e OpenWas para detecção periódica de vunerabilidades internas e externas.

Com uma frequência de 4 meses, as varreduras são feitas, identificadas as prioridades e efetuadas as correções, sendo reavaliadas quando à sua remediação no próximo ciclo de varreduras.

6.6. Proteção contra software malicioso

Esta instituição utiliza a suíte de segurança da Kaspersky, contemplando:

- Threat Intelligence – Permite o conhecimento profundo e atualizado sobre

ameaças específicas e fontes de ataque tradicionalmente difíceis de serem detectadas por engenheiros de segurança que acessam a informação apenas dentro de suas próprias redes.

- Enterprise Inspector – Ferramenta sofisticada de detecção e resposta que permite o monitoramento abrangente, contínuo e em tempo real da atividade dos endpoints, bem como a análise de processos suspeitos para fornecer uma resposta imediata.

6.7. Mecanismos de rastreabilidade para informações sensíveis

Esta instituição utiliza a solução ESET Safetica para mapeamento de dado sensível, verificando quem possui acesso aos dados, rastreando a origem e destino deste dado.

6.8. Controles de acesso

Esta Instituição utiliza mecanismos de controle de acesso por autenticação e todos os sistemas listados no item 6.1 permitem que apenas usuários autorizados possam acessar as informações, de acordo com o nível de sigilo e acesso.

6.9. Segmentação da rede de computadores

As redes da Instituição são segmentadas de acordo com o tipo de informação e local de acesso.

Atualmente dispomos de recursos e sistemas que permitem a criação e controle de políticas avançadas pela atribuição de perfis de acesso que são dissociadas do controle por endereços IP. Foram estabelecidas políticas de controle simples, baseadas nesses perfis para segmentar o acesso de forma dinâmica. Foi implementado também a segmentação virtual das redes (VLAN) permitindo um maior controle dos acessos entre usuários, visitantes e serviços.

6.10. Manutenção de cópias de segurança dos dados e das informações

Esta instituição instituiu a política de backup, na qual são registradas todas as decisões sobre armazenamento de dados. Assim são definidos:

- quais são os dados a serem copiados;

- frequência de realização do processo;
- tipo de backup a ser realizado;
- métricas de avaliação do processo;
- funcionários envolvidos no processo.

6.11. Registro, análise da causa e do impacto e controle dos efeitos de incidentes relevantes

Esta instituição registra as vulnerabilidades encontradas, analisa e mapeia o impacto dos incidentes relevantes para as atividades da instituição, sendo incluídos as informações recebidas de empresas prestadoras de serviços.

6.12. Gestão de Prestadores de Serviço

Quando da contratação de prestadores de serviço, inclusive serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a instituição adotará as seguintes práticas de governança corporativa e de gestão:

6.12.1. Abrangência

Devem ser consideradas para fins de aplicação do disposto nesta política aquelas empresas prestadoras de serviços a terceiros que tiverem acesso:

I. aos dados da instituição, ou por ela controlados; ou

II. aos sistemas por ela utilizados; ou

III. aos ambientes físicos ou tecnológicos, que possam ser utilizados para acessar aos dados e sistemas de que tratam os incisos I e II.

6.12.2. Cláusulas contratuais

Os contratos com empresas prestadoras de serviços a terceiros deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, bem como cláusulas que garantam que os profissionais das empresas prestadoras de serviços a terceiros:

I. Protejam e zelem pelo sigilo das informações da Instituição.

II. Tenham conhecimento e cumpram esta política.

III. Cumpram as leis e normas que regulamentam a propriedade intelectual e a proteção de dados, especialmente a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais) e a Resolução nº 4.658 do Banco Central do Brasil.

IV. Utilizem os dados da instituição, ou por ela controlados, os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da Instituição, apenas para as finalidades objeto do contrato de prestação de serviço.

V. Comuniquem imediatamente qualquer violação desta Política e/ou outras Normas.

6.12.3. Procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros

A instituição somente contratará prestadores de serviços que demonstrarem a adoção dos seguintes mecanismos de prevenção e tratamento de incidentes:

1. Adoção de software de proteção contra softwares maliciosos, mantendo-o sempre ativado e atualizado;

2. Adoção de Firewall, mantendo-o sempre ativado e atualizado;

3. Adoção de processo de manutenção de cópias de segurança dos dados e das informações, seja ele realizado para servidor físico ou em nuvem, a ser executado no mínimo semanalmente;

4. Adoção de mecanismos de controles de acesso e de autenticação que permitam identificar e rastrear o usuário que tiver acesso aos sistemas ou dados da instituição e seus clientes no ambiente cibernético;

5. Adoção de mecanismos de criptografia que permitam criptografar os dados pessoais de clientes e os dados pertencentes à instituição armazenados pelo prestador de serviço ou enviado por meios de comunicação;

6. Adoção de mecanismos de segmentação da rede pela qual o prestador de serviço acessa aos sistemas ou dados da instituição ou dos clientes da instituição;

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

Quando da contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, além das práticas de governança corporativa e de gestão referidas acima, a instituição adotará as seguintes práticas de governança corporativa e de gestão:

7.1. Abrangência

Além dos serviços relevantes de processamento e armazenamento de dados, para fins desta política os serviços de computação em nuvem abrangem a disponibilidade à instituição, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

I. processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;

II. implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III. execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

7.2. Avaliação da relevância do serviço a ser contratado

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem esta instituição irá avaliar os seguintes aspectos:

I. os riscos a que estará exposta;

II. a criticidade do serviço;

III. sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado;

IV. classificação da informação a ser tratada pelo prestador.

7.3. Critérios de decisão quanto à contratação

A instituição estabelece como critérios de decisão quanto à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a capacidade do potencial prestador de serviço de assegurar:

I. o cumprimento da legislação e da regulamentação em vigor;

II. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas;

IV. a sua aderência às certificações exigidas por lei para a prestação do serviço a ser contratado;

V. o acesso da instituição aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;

VI. provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados

VII. a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;

VIII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

IX. o acesso da instituição às informações a serem fornecidas pelo prestador de serviço, visando verificar o cumprimento do disposto nas cláusulas referentes à:

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

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

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

d) aderência do prestador de serviço às certificações exigidas por lei;

e) concessão de acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços aqui contratados, quando aplicável;

f) concessão de acesso às informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) confidencialidade, integridade e disponibilidade dos dados da instituição, bem como pelo cumprimento da legislação e da regulamentação em vigor;

h) prestação dos serviços, armazenamento, processamento e gerenciamento dos dados unicamente nos países e regiões previamente estabelecidos e comprometendo-se a não mudar a localização indicada sem a prévia autorização.

i) transferência dos dados recebidos para a prestação do serviço ao novo prestador de serviços ou à instituição em caso de extinção do contrato e a excluir os dados recebidos para a prestação do serviço, após a transferência dos dados e a confirmação da integridade e da disponibilidade;

j) não promoção de subcontratação de serviços sem autorização prévia.

k) concessão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação dos 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.

l) obrigação de mantê-la permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

m) obrigação de, em caso de decretação de regime de resolução da instituição pelo Banco Central do Brasil:

I. o prestador de serviço 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, bem como aos códigos de acesso códigos de acesso aos dados e às informações, que estejam em poder do prestador de serviço;

II. o prestador de serviço notificar previamente ao responsável pelo regime de resolução sobre a intenção de interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

1. o prestador de serviço obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

2. a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da instituição.

7.4. Cláusulas contratuais

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

I. 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;

II. a adoção de medidas de segurança para a transmissão e armazenamento dos dados;

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

IV. a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados ao novo prestador de serviços ou à instituição contratante; e

b) exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;

V. o acesso da instituição contratante a:

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento dessas obrigações;

b) informações relativas às certificações e aos relatórios de auditoria especializada; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VI. a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;

VII. 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;

VIII. a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e

IX. a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Os **contratos** devem prever, ainda, cláusulas específicas para o caso de decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

I. a obrigação de a empresa contratada 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, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada; e

II. a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

7.5. Comunicação da contratação ao Banco Central do Brasil

A instituição comunicará ao Banco Central do Brasil, a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem com as seguintes informações:

I - a denominação da empresa a ser contratada;

II - os serviços relevantes a serem contratados; e

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados,

A referida comunicação será realizada, no máximo, até 10 (dez) dias após a contratação dos serviços ou alterações contratuais que impliquem modificação dessas informações.

7.6. Documentação

Devem ser documentadas as práticas de governança corporativa e de gestão adotadas, proporcionais à relevância do serviço a ser contratado e aos riscos aos quais a instituição se expõe.

Da mesma forma, deve ser documentada a verificação da capacidade do potencial prestador de serviço de assegurar:

I. o cumprimento da legislação e da regulamentação em vigor;

II. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

IV. a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

V. o acesso da instituição contratante aos 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;

VI. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VII. a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

VIII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

8. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A instituição comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança, seja ele relativo ao ambiente cibernético ou não, que possa acarretar risco ou dano relevante aos titulares.

A referida comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;

II. as informações sobre os titulares envolvidos;

III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV. os riscos relacionados ao incidente;

V. a causa do incidente;

VI. o impacto do incidente;

VII. os motivos da demora, no caso de a comunicação não ter sido imediata; e

VIII. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

9. COMUNICAÇÃO DE INCIDENTES RELEVANTES RELACIONADOS AO AMBIENTE CIBERNÉTICO AO BANCO CENTRAL DO BRASIL

A instituição comunicará ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades, mencionando, no mínimo, os itens descritos no item 8 desta política.

10. MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA INSTITUIÇÃO

Para a disseminação da cultura de segurança cibernética a instituição adotará os seguintes mecanismos:

I. a instituição promoverá a disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização, capacitação e avaliação periódicas de pessoal.

II. a política e as regras de segurança da informação e segurança cibernética serão divulgadas e compartilhadas com todo o público-alvo desta política, e são disponibilizadas de maneira que seu conteúdo possa ser consultado a qualquer momento, protegidas contra alterações.

III. a prestação, na página da instituição na internet, de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros

IV. a divulgação ao público, na página da instituição na internet, de resumo

contendo as linhas gerais da política de segurança cibernética.

11. PROGRAMA DE SEGURANÇA CIBERNÉTICA

Conforme sua criticidade, o programa de segurança cibernética divide-se em:

Ações críticas: Correções emergências e imediatas para mitigar riscos iminentes.

Ações de Sustentação: Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro e permitindo que ações de longo prazo/estruturantes possam ser realizadas.

Ações Estruturantes: Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos, voltadas para o futuro da Instituição.

12. GOVERNANÇA COM AS ÁREAS DE NEGÓCIO E TECNOLOGIA

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas da Segurança Cibernética, garantindo a confidencialidade, integridade e disponibilidade das informações.

13. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE APLICAÇÃO

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da instituição e às boas práticas de segurança.

14. RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A Instituição elaborará relatório anual sobre a implementação do plano de ação e de resposta a incidentes, tendo como data-base o dia 31 de dezembro de cada ano.

O relatório deverá ser submetido ao comitê de risco, quando existente, e apresentado ao conselho de administração ou, na sua inexistência, à diretoria até 31 de março do ano seguinte ao da data-base, devendo abordar:

I. A efetividade da implementação das ações desenvolvidas pela Instituição

para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

II. O 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;

III. Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

IV. Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

15. MANUTENÇÃO DE DOCUMENTAÇÃO

Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

I. o documento relativo à política de segurança cibernética;

II. o documento relativo ao plano de ação;

III. o documento relativo ao plano de resposta a incidentes;

IV. os relatórios anuais de que trata esta política;

V. a documentação referente às práticas de governança corporativa e de gestão e a verificação da capacidade do potencial prestador de serviço;

VI. os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato.

VII. os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle da implementação e da efetividade:

a. da política de segurança cibernética, contado o prazo a partir da implementação;

b. do plano de ação, contado o prazo a partir da implementação;

c. do plano de resposta a incidentes, contado o prazo a partir da implementação;

d. dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo a partir da implementação.

16. DA DIVULGAÇÃO

A Política de Segurança Cibernética e da Informação e as demais políticas e normas complementares da Instituição aqui referenciadas devem ser divulgadas ao Público-Alvo, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, devendo estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.

Além disso, será divulgado ao público, na página da instituição na internet, resumo contendo as linhas gerais da política de segurança cibernética.

17. MEDIDAS DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas, nas normas internas da Instituição e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas, tais como: advertências (verbal e/ou escritas), suspensões e demissões com e sem justa causa.

18. REVISÃO ANUAL

Esta política será documentada e revisada anualmente.

19. REVISÕES EXCEPCIONAIS

Esta política será atualizada na data 01/06/2021 e na data 01/10/2021 para que sejam integradas as respectivas modificações a serem implementadas no curto, médio e longo prazo, conforme plano de ação da instituição.

20. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da instituição, ao aprovar esta Política de Segurança Cibernética e da Informação, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética e da informação, buscando sempre manter a instituição em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados,

permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

21. APROVAÇÃO DA POLÍTICA

Esta política foi aprovada pela Diretoria da Instituição em ..... data...., conforme ata.....

Publicado em...(local)... em xx/xx/xxxx.

ANEXO I – REGRAS DE SEGURANÇA

1. LINHAS GERAIS DE COMPORTAMENTO

1.1.1. Cuidados no ambiente externo

I. É proibido o compartilhamento oral de informações referentes à Instituição em locais públicos, áreas expostas (aviões, restaurantes, encontros sociais, etc.), ou próximo a pessoas estranhas à Instituição, sob pena de responsabilização.

II. Equipamentos que contenham, ou possam conter, informações, devem permanecer sob vigilância e responsabilidade do portador, especialmente quando, devidamente autorizado, levados para o ambiente externo da Instituição, objetivando evitar acesso de pessoas desautorizadas às informações neles constantes, sob pena de responsabilização.

1.1.2. Cuidados com o armazenamento e descarte

I. É proibido o transporte de informações da Instituição em qualquer meio (Computador, CD, DVD, pendrive, papel, etc.) sem as devidas autorizações e proteções;

II. Os documentos que contenham informações sensíveis, pessoais ou da Instituição, mas não só, os impressos, deverão ser devidamente inutilizados antes de serem descartados.

1.1.3. Gestão de Mudanças

I. A área de Infraestrutura é responsável por participar, documentar, homologar e implementar toda e qualquer alteração, seja de acesso, hardware e software ou que tenha impacto direto na infraestrutura da Instituição.

II. As solicitações devem ser encaminhadas pelo gestor responsável pela área em questão à área de Infraestrutura, e tais demandas devem ser registradas em sistema para acompanhamento histórico.

2. REGRAS DO USO DE TECNOLOGIA

I. Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções

na Instituição. Somente se houver permissão formal poderão ser utilizados tais recursos para outros fins.

II. Quando o usuário se comunicar através de recursos de tecnologia da Instituição, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da Instituição e garanta a compreensão da mensagem por parte do destinatário.

III. Os conteúdos acessados e transmitidos através dos recursos de tecnologia da instituição devem ser legais, inclusive de acordo com o Código de Ética da Instituição, e devem contribuir para as atividades profissionais do usuário.

IV. O uso dos recursos de tecnologia da Instituição pode ser examinado, auditado ou verificado pela Instituição, mediante autorização expressa do Gerente Operacional, sempre respeitando a legislação vigente.

V. Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados.

VI. Os recursos de tecnologia da Instituição, disponibilizados para os usuários, é de uso pessoal e intransferível e não podem ser repassados para outra pessoa interna ou externa à organização.

VII. Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à gerência operacional.

2.1. Gestão de Ativos da Informação:

I. Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "hardening", patch management, autenticação e autorização, por exemplo) e ter documentação e planos de manutenção atualizados periodicamente.

II. Os profissionais contratados por tempo limitado, prestadores de serviço e parceiros, não terão direito à unidade pessoal de diretório de rede, salvo solicitação à Gerência da área.

III. O funcionário é responsável por todas as informações e arquivos em sua unidade pessoal ou departamental.

IV. Não podem ser armazenados nos servidores de arquivo ou diretórios de rede arquivos tais como:

a) Jogos: Não devem ser instalados nas estações de trabalho e nem armazenados em unidades de rede individuais ou departamentais.

b) Imagens: Devem ser armazenados em unidade de rede, quando relacionadas ao desempenho de atividades profissionais na Instituição (Exemplo: Imagens ou fotos de campanha de *marketing* a ser realizada com extensão *.JPG, JPEG, BMP, GIF, dentre outras).

c) Vídeos: Exclusivamente devem ser armazenados em unidade de rede, quando condizentes com os negócios da Instituição.

d) Música: Exclusivamente devem ser armazenadas em unidades de rede, quando condizentes com os negócios da Instituição.

e) Banco de Dados: Tais programas ou arquivos devem estar instalados em infraestrutura apropriada destinado para tal finalidade, sob a gerência da TI.

V. Equipamentos de utilização pessoais, tais como tablets, notebook ou telefone celular, sejam pessoais ou cedidos a determinados funcionários para que desenvolvam suas atividades profissionais são permitidos, mediante a assinatura de um Termo de Responsabilidade pelos mesmos e pelos softwares neles instalados, sendo regulados pelas regras da Política de Segurança da Informação e outras normas específicas.

VI. A aquisição de softwares depende de planejamento orçamentário autorizado pelo órgão competente e homologação técnica da Segurança da informação, que receberá solicitações e avaliará a necessidades de uso.

VII. Somente a área de Suporte e Infraestrutura estão autorizados a realizar instalação de qualquer tipo de software nos equipamentos da Instituição seja este um sistema ou um aplicativo simples, inclusive aqueles obtidos gratuitamente e/ou baixados da internet.

VIII. Somente poderão ser instalados e utilizados softwares devidamente licenciados, não é permitido instalar softwares pessoais, emprestados, de

terceiros, que não sejam devidamente licenciados pelo fabricante do produto.

IX. O uso das impressoras destina-se às atividades profissionais da Instituição. Casos excepcionais, onde a impressão seja de caráter pessoal, deve ser autorizado pelo gestor da área e Suporte, ficando o usuário ciente de que o serviço de impressão pode ser monitorado.

X. A impressão de informações classificadas como confidenciais deve ser controlada e o usuário responsável deve imediatamente recolher o material impresso na impressora.

XI. Todos os considerados público-alvo desta política devem manter suas mesas de trabalho livres de documentos classificados. Quando não estiverem trabalhando diretamente com eles e ao final do expediente, todos documentos devem ser armazenados em locais apropriados, de acordo com sua classificação.

XII. As estações de trabalho e computadores portáteis devem permanecer bloqueados por senhas quando da ausência do usuário.

3. REGRAS DE USO DO COMPUTADOR

3.1. Disponibilização e uso

O computador disponibilizado para o usuário pela Instituição tem por objetivo o desempenho das atividades profissionais desse usuário na organização.

É necessário que o gestor do usuário o autorize a usar o computador. Deve ser feita uma solicitação à área de suporte, que autorizará tecnicamente e fará a liberação mediante a criação de um usuário com senha.

Todos os equipamentos, *softwares* e permissões de acessos devem ser testados, homologados e autorizados pela área de infraestrutura.

A Instituição pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário.

O gestor de cada setor da instituição é responsável pelos computadores do seu setor. O controle das máquinas é de responsabilidade da área de suporte.

A identificação do usuário ao computador é feita através do login e senha

disponibilizado pela área de segurança da informação, portanto ela é sua assinatura eletrônica.

Com relação aos parâmetros para criação da senha de acesso, a primeira senha será gerada pela Diretoria de TI e deverá ser alterada no primeiro acesso.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (!, @, #, $, %, etc.) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanuméricos, utilizando caracteres especiais (!, @, #, $, %, etc.) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha. O prazo máximo de duração da senha de acesso é de 90 (noventa) dias contados de sua criação/alteração, sendo que, 15 dias antes do fim do referido período o sistema notificará o usuário para acerca da expiração da senha.

É permitido apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso.

Recomenda-se para elaboração de senhas que se utilize repetir senhas de uso pessoal para acessos corporativos, de forma que duas pessoas não tenham a mesma senha.

Deve ser evitado o uso de dados pessoais, sequencias de teclado, palavras que fazem parte de listas publicamente conhecidas (times de futebol, por exemplo).

Sugere-se a substituição de caracteres semelhantes, entre letras e números, por exemplo: “Astro-rei” por “A5tr0-re1”. É aconselhada, também a formação de uma frase, por exemplo: “Eu trabalho na Instituição Tal há 2 anos e 6 mês” = EtnITh2ae6m.

3.2. Programas utilizados no computador

Os programas aplicativos, programas básicos (sistema operacional e

ferramentas) e componentes físicos são implantados e configurados somente pelas áreas de suporte e infraestrutura.

É proibido aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada das áreas de infraestrutura e suporte.

É proibido aos usuários conectar, implantar ou alterar componentes físicos no computador.

3.3. Verificação do computador e acessos

A Instituição mantém por 5 anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *softwares*, hardwares ou acessos que não sejam autorizados pela área de infraestrutura.

Os acessos a equipamentos, *softwares* e respectivas permissões serão testados pela área de Infraestrutura de Tecnologia com validação da área de Riscos e Controles Internos a cada 6 meses.

3.4. Responsabilidades do usuário

Cuidar adequadamente do equipamento. O usuário é o custodiante deste recurso.

Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de segurança da informação.

3.5. Vazamento de dados

A instituição utiliza a solução Safetica para mapeamento e rastreamento de dados sensíveis, monitorando toda e qualquer operação dos usuários, mapeando o fluxo dos arquivos com conteúdo sensível ou não, monitorando também a utilização de todos os softwares em cada equipamento de usuário.

3.6. Outras proteções

O Compliance da Instituição alerta todos os usuários que a instalação ou utilização de *software* não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena

de detenção e multa. A Instituição não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima.

Todas as práticas que representem ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

3.7. Regras do Uso da Internet

a) Responsabilidade e forma de uso

O usuário é responsável por todo acesso realizado com a sua autenticação.

O usuário é proibido de acessar endereços de internet (sites) que:

i. Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes.

ii. Possuam conteúdo pornográfico.

iii. Defendam atividades ilegais. Menosprezem, depreciem ou incitem o preconceito em razão de sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento, deficiência física, ou qualquer outro motivo.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.

3.8. Regras do Uso do Correio Eletrônico (E-Mail)

Os endereços de correio eletrônico disponibilizados pela Instituição deverão ser utilizados unicamente para desempenho das funções profissionais. O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à empresa.

É obrigatória a utilização de senha e identificação de usuário pessoal e intransferível.

A utilização desse endereço de correio eletrônico pelo usuário necessita ser autorizada pelo seu gestor da área.

A liberação do endereço de correio eletrônico será feita pela área de tecnologia da informação, de maneira controlada e segura com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço.

Quando acontecer desligamento de usuário, o Gestor deve comunicar à área de tecnologia da informação o nome e a identificação desse usuário.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, sem que haja autorização expressa do autor do trabalho e da organização.

É proibido criar, copiar , enviar ou encaminhar mensagens ou imagens que:

i. Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
ii. Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
iii. Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
iv. Menosprezem, depreciem ou incitem o preconceito em razão de sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento, deficiência física, ou qualquer outro motivo;
v. Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
vi. Utilizem de termos obscenos ou com referência à conduta sexual;
vii. De cunho político ou religioso;
viii. Conteúdos que constituam quebra, infração ou detrimento de legislação;
ix. Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
x. Defendam ou possibilitem a realização de atividades ilegais.
xi. Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
xii. Possam prejudicar a imagem da Instituição;

xiii. Sejam incoerentes com o Código de Ética da Instituição;

É proibido utilizar os recursos de correio eletrônico para:

1. assediar ou perturbar outrem seja através de linguagem inadequada, alta frequência de mensagens ou excessivo tamanho de arquivos;
2. enviar, encaminhar ou, de qualquer forma, propagar mensagens em cadeia de "correntes" ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;
3. enviar anexos contendo *software* malicioso ou quaisquer arquivos maléficos e contra a legislação vigente;
4. enviar mensagens contendo arquivos de programas de código executável (.exe, .scr, .bat, .dll, etc) que represente risco à Instituição ou à terceiros;
5. enviar mensagens de propagandas ou venda de produtos com fins particulares.

O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da Instituição. Assim, em situações autorizadas pela Diretoria, as mensagens do correio eletrônico de um usuário poderão ser acessadas pela Instituição ou por pessoas/entidades por ela indicada. Portanto, não deve ser mantida expectativa de privacidade pessoal.

O usuário que utiliza um endereço de correio eletrônico concedido pela Instituição é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.

Toda mensagem recebida pelo correio eletrônico da Instituição é um documento formal e, portanto, obedece aos regramentos sobre Geração, Manuseio, Armazenamento, Transporte e Descarte desta política.

O usuário deverá ser especialmente diligente em relação:

xiv. Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);

xv. Ao nível de sigilo da informação contida na mensagem;

xvi. Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;

xvii. Ao uso da opção Encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada e em nuvem, sob a responsabilidade da área de tecnologia da informação.