POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

SUMÁRIO

1. OBJETIVO

O objetivo desta política é promover as práticas de segurança para o trânsito das informações no âmbito do Conglomerado Prudencial Bari("Bari"), formado pelo Banco Bari de Investimentos e Financiamentos S/A, Bari Companhia Hipotecária e Bari Securitizadora S/A na forma de Diretrizes e Normas, para o trato de seus ativos e passivos, disseminando uma cultura de segurança das informações entre seus colaboradores, mantendo a segurança dos sistemas, a integridade e disponibilidade de dados, a confidencialidade das informações, a continuidade dos negócios e a aderência às leis e normas que regulamentam os negócios da indústria de serviços financeiros. A política sob referência visa, ainda, mitigar riscos que possam resultar em perda ou prejuízo, seja de ordem financeira ou de imagem para o Bari.

Na busca constante pela excelência de nossos serviços, esta Política é uma declaração formal do Bari em relação ao seu comprometimento em proteger todas as suas informações sensíveis, apoiando metas e princípios de Segurança da Informação e Segurança Cibernética, a fim de garantir o cumprimento do objetivo acima, alinhado com estratégias de negócio.

Esta política e os demais procedimentos que suportam sua implementação estão em conformidade com as demais políticas do Bari.

2. ABRANGÊNCIA

Esta Política é aplicável a todos os colaboradores, em todos os níveis, parceiros e prestadores de serviços terceirizados que atuam em nome do Bari, incluindo trabalhos executados externa e internamente, que utilizem o ambiente de sistemas e dados do Bari, ou que, de qualquer forma, tenham acesso a estas informações.

3. DEFINIÇÕES

A informação é um ativo de alto valor para o Bari e, assim, deve ser preservada e protegida, independentemente da forma de apresentação e armazenamento.

Na elaboração das normas de segurança específicas a cada ambiente e processo, o Bari seguiu diretrizes determinadas por seu Conselho de Administração, de acordo com as boas práticas de segurança das informações e segurança cibernética, garantindo a confidencialidade, integridade e

disponibilidade das informações e dados processados nas suas operações e negócios.

Para a elaboração desta Política foram consideras as seguintes diretrizes como principais:

- Garantir que esta Política de Segurança da Informação e Cibernética e os procedimentos operacionais relativos ao cumprimento das normas aqui definidas estejam compatíveis com os requisitos legais e regulamentares aplicáveis ao Bari e também ao porte, perfil de risco, modelo de negócio, natureza das operações e complexidade dos produtos e serviços do Bari;

- Classificar as informações pelo grau de confidencialidade, adotando medidas de proteção para as informações classificadas como de acesso restrito e confidenciais;

- Manter processos de avaliação de risco, identificando ameaças e vulnerabilidades, gerando relatórios com os resultados conclusivos sobre as avaliações de risco;

- Gerenciar e controlar os acessos às contas de usuários, incluindo adições, exclusões e modificações. Os acessos a informações do Bari devem ser formalmente autorizados;

- Manter, instalar e testar recursos e planos de contingência e continuidade dos negócios, mantendo também backups dos dados e sistemas críticos;

- Armazenar e proteger de acordo com sua classificação as mídias que contenham dados classificados como confidenciais;

- Treinar e conscientizar os responsáveis e também os usuários, quanto às suas responsabilidades pela segurança das informações e pelas respostas a uma quebra de segurança;

- Prevenir a intrusão e alertar caso seja detectada alguma anomalia na integridade dos dados;

- Revisar periodicamente os logs dos componentes críticos para a segurança dos dados do Bari, tais como Firewalls, Aplicações, Sistemas Operacionais, Equipamentos de Rede, para: Autenticação, Autorização e Monitoramento de Acesso e das ações executadas;

- Conservar as trilhas e os registros de auditoria referentes aos processos e recursos de segurança por um período mínimo de um ano ou conforme determina a regulamentação vigente;

- Garantir que todos os colaboradores, parceiros e prestadores de serviço conheçam e cumpram com as diretrizes desta Política.

3.1. Classificação das Informações

Todos os ativos de informação devem ser identificados, inventariados, ter classificações definidas e seus gestores responsáveis designados.

Deve ser definido e estabelecido um processo para a classificação das informações do Bari, de forma que estas possam ser mantidas protegidas de acordo com sua relevância e grau de confidencialidade para os processos de negócios do Bari.

É de responsabilidade do Gerente/Supervisor/Coordenador de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (cadastros, dados de transações, logs, relatórios e/ou mídias) gerada por sua área, de acordo com os níveis abaixo:

1 – Informação Pública

Toda informação que pode ser acessada por todos os usuários da organização, clientes, fornecedores, prestadores de serviços, podendo e/ou devendo ser divulgada para o público em geral. Geralmente este tipo de informação refere-se a Marketing, Dados Legais Públicos, Relações com Investidores, Ouvidoria, conteúdo disponibilizado no website do Bari e etc.

2 – Informação de Acesso Restrito

Toda informação que pode ser acessada por determinado grupo de usuários/colaboradores da organização, e em alguns casos, somente mediante aprovação submetida a alçadas de poderes. Geralmente, a divulgação não autorizada dessa informação pode causar impactos financeiros, de imagem ou operacionais ao negócio da organização ou do parceiro;

3 – Informação Confidencial

Toda informação que pode ser acessada somente por usuários da organização explicitamente indicados pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia negocial da organização. Estes tipos de acessos devem ter a ciência e/ou reconhecimento da Diretoria, Controladoria e Compliance do Bari.

Informações de terceiros sob responsabilidade ou custódia do Bari devem também ser, se não classificadas formalmente, submetidas a medidas e critérios estabelecidos entre as partes, alinhadas com o processo de classificação interno, com as cláusulas contratuais e os termos de sigilo estabelecidos.

4. REGRAS E DIRETRIZES

4.1. Diretrizes para o Comportamento Seguro

É importante que todos os colaboradores e prestadores de serviços adotem comportamento seguro com o objetivo de proteger as informações pertencentes ao Bari, com destaque para os seguintes itens:

- Diretores, gerentes, coordenadores, funcionários, parceiros e prestadores de serviços devem assumir atitude proativa no que diz respeito à proteção das informações do Bari.
- Os colaboradores e prestadores de serviços devem compreender as ameaças internas e externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, uso de dispositivos não autorizados e homologados ao ambiente, uso de webmail, acesso a conteúdo suspeito e malicioso, bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Informações confidenciais ou de acesso restrito do Bari não devem ser transportadas em qualquer tipo de mídia sem as devidas proteções e autorizações.
- As senhas de usuários devem ser pessoais e intransferíveis, não podendo ser reveladas, compartilhadas, registradas em locais vulneráveis, como papel, etiquetas e dispositivos eletrônicos.
- Assuntos confidenciais só podem ser falados/comentados em áreas restritas do Bari, não podendo ser reveladas em ambientes públicos, como elevadores, serviços de transporte, restaurantes, etc.
- Dúvidas sobre a Política e Normas de Segurança da Informação devem ser imediatamente esclarecidas com a área de Governança de TI/Segurança Da Informação ou Gestor de área.

4.2. Diretrizes para Propriedade Intelectual

Todos os documentos produzidos por intermédio de recurso de processamentos do Bari são de sua propriedade, assim como todo e qualquer registro de dados, voz e/ou imagem armazenados em meio magnético, óptico, eletrônico, impresso ou qualquer outro veículo de exibição, produzidos com o fim de publicitar ou operacionalizar, interna ou externamente, as atividades do Bari.

Toda informação de propriedade do Bari, deve ser tratada de acordo com a sua classificação, conforme item 3.1 desta política.

4.3. Diretrizes para Privacidade e Proteção de Dados Pessoais

Informações armazenadas, tratadas ou enviadas por meio de recursos do Bari são consideradas informações profissionais.

Os dados pessoais de funcionários, colaboradores, parceiros e clientes deverão ser tratados conforme a finalidade de uso autorizada pelo titular, e pelo tempo informado e necessário para este uso, conforme definido na Lei nº 13.709 – Lei Geral de Proteção de Dados.

Todos os dados pessoais de colaboradores, parceiros e clientes serão considerados dados confidenciais. O Bari se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores, parceiros e clientes além daqueles relevantes na condução do seu negócio.

Adicionalmente, os dados pessoais de colaboradores, parceiros e clientes sob a responsabilidade do Bari não serão usados para fins diferentes daqueles para os quais foram coletados e não serão compartilhados com terceiros, exceto quando exigido pelo negócio, e desde que o proprietário dos dados autorize formalmente a compartilhar tais informações ou através de legislação que autorize o compartilhamento.

Todos os dados trafegados nos ambientes físicos e sistêmicos do Bari estão sujeitos a monitoramento. Assim, ao utilizar qualquer recurso do Bari, os usuários automaticamente consentem este monitoramento.

4.4. Diretrizes para Gerenciamento de Incidentes e Problemas

Procedimentos operacionais para o atendimento, registro, resposta, correção, monitoramento e prevenção de incidentes e problemas relacionados com segurança da informação devem ser definidos e devidamente documentados pelo Departamento de TI e pela área de Segurança da Informação, a fim de garantir a segurança dos dados e a continuidade dos serviços.

Os incidentes podem ser classificados como alto, médio ou baixo, a depender de alguns parâmetros como: impedimento total ou parcial do desenvolvimento das atividades de negócio, do desempenho de uma área ou de um usuário do Conglomerado; tentativa ou vazamento de informações confidenciais ou identificação de informações desprotegidas; utilização de informações ou sistemas de forma fraudulenta.

Os procedimentos de resposta a incidentes de segurança devem também prever escalonamento, quando necessário, assegurando a administração

oportuna e eficiente de todas as situações. Para este fim, devem ser definidos níveis de responsabilidade para respostas aos alertas e incidentes de segurança.

Um incidente de segurança que identifique um possível vazamento de informações da empresa deve ser imediatamente reportado a direção e ter ação corretiva contínua e priorizada até a sua conclusão.
O detalhamento do processo de gestão de incidentes deve estar formalizado em documento específico contendo a descrição de todo o procedimento a ser realizado.

4.5. Diretrizes de Atendimento ao PCI-DSS

Toda documentação de segurança da informação desenvolvida pelo Bari, além de garantir a confidencialidade, integridade e disponibilidade da informação, deve também atender a todos os requisitos do padrão global de segurança de dados do setor de cartões, o PCI-DSS, garantindo assim a segurança dos dados do portador do cartão dos clientes do Bari.

Todos os funcionários e/ou terceiros que forem ter acesso ao ambiente escopo de avaliação do PCI-DSS, ou seja, que forem trabalhar no ambiente que possua dados do portador do cartão devem ter verificações referentes ao histórico do emprego anterior e verificação das referências curriculares. Esta verificação deve ser feita de acordo com o que a legislação permite e requer.

Deve haver documentação formalizando a confirmação de que os prestadores de serviço são também responsáveis pela segurança dos dados dos portadores de cartões.

Anualmente, deve-se realizar o programa de conscientização da segurança da informação, composto de treinamentos e/ou palestras sobre o tema. O programa, deve ser aplicado a todos os colaboradores do Bari, bem como a coleta do reconhecimento dos colaboradores quanto a participação e compreensão do programa, podendo ser por meio manual ou eletrônico.

4.6. Normas de Segurança das Informações

4.6.1 Plano de Continuidade de Negócios

Cabe ao Departamento de Tecnologia da Informação e à área de Segurança da Informação definirem, em conjunto com as demais áreas das empresas do Bari o desenvolvimento, manutenção e testes de um Plano de Continuidade dos Negócios (PCN), que determine, no mínimo:

1. Os principais serviços ou mais relevantes, que não podem ser interrompidos por um curto período de tempo;
2. Os cenários identificados e que serão contemplados no Plano de Continuidade;
3. Os riscos e eventos possíveis de ocorrer, que podem impactar na perda de continuidade destes serviços. Por exemplo: falhas técnicas (internas, externas e de parceiros ou prestadores de serviço) ou eventos de força maior (catástrofes ou intervenção externa como ação sindical, por exemplo);
4. O tempo máximo de recuperação (RTO – Recovery Time Objective) de cada um dos serviços críticos definidos;
5. Os responsáveis pelo diagnóstico da situação e acionamento do Plano;
6. Os procedimentos a serem executados para a recuperação de cada um dos serviços críticos impactados e os respectivos responsáveis por sua execução;
7. O plano de comunicação para crise, contendo informações sobre o incidente, providências tomadas, prazos estabelecidos, os responsáveis pela comunicação e os destinatários autorizados internos e externos (ex. Banco Central).

O PCN deverá prover a rápida retomada das atividades e garantir a segurança de todas as pessoas que porventura estejam nas dependências do Bari.

Sempre que houver a necessidade de alteração do PCN, a nova redação deverá ser revisada e aprovada pela Diretoria e pelo Conselho de Administração. A área de Governança de TI/Segurança da Informação deve atualizar o documento e submeter para Compliance solicitar as aprovações da Diretoria e Conselho e informar a nova versão a todos os colaboradores envolvidos.

Os incidentes de Segurança que possam gerar indisponibilidade e, consequentemente, acionar o Plano de Contingência devem ser alvo de testes periódicos.

O treinamento específico e os testes do PCN devem ser programados de acordo com o calendário a ser definido pela área de Governança de TI/Segurança da Informação, com aprovação da Diretoria.

Os resultados dos testes de execução do PCN devem demonstrar o atendimento aos tempos de recuperação definidos (RTO). Tais testes devem ser sempre documentados, gerando evidências que possam ser consultadas, sempre que requerido e necessário, inclusive, para melhorias/correções para o PCN.

4.6.2 Gestão da Disponibilidade de Sistemas e Informações

Cabe à área de Governança de TI/Segurança da Informação a responsabilidade de definir os procedimentos operacionais para o planejamento, controle, resposta e monitoramento de riscos que possam impactar na disponibilidade dos sistemas e dados, bem como dos serviços de TI do Bari.

Para isso, Governança de TI deverá atuar em conjunto com a área de Compliance e Controles Internos, inserindo e atualizando os riscos relacionados com disponibilidade na Matriz de Riscos do Bari, com o apoio das demais áreas, com o objetivo de:

- Monitorar se as respostas definidas para cada um dos riscos identificados estão sendo efetivas para a adequada mitigação;
- Avaliar se não há riscos que não mais se aplicam aos negócios e ao ambiente do Bari. Neste caso, estes riscos podem ser eliminados da matriz de riscos.
- Avaliar se não há outros riscos que possam impactar na disponibilidade dos sistemas e serviços de TI do Bari. Neste caso, estes novos riscos devem ser adicionados à matriz, bem como as demais informações relacionadas, incluindo as respostas para mitigação e seus responsáveis.

Por questões de confidencialidade das informações, a Matriz de Riscos deverá ser armazenada em local seguro, com acesso somente à área de Compliance e Controles Internos e Diretoria.

Caberá também à área de Governança de TI/Segurança da Informação a responsabilidade de informar Compliance e Controles Internos os fatos apurados no tocante aos riscos listados na matriz de riscos do Bari. Em havendo a materialização de impactos relativos à disponibilidade dos sistemas, informações e serviços de TI, deve a área de Governança de TI/Segurança da Informação esclarecer as ocorrências e os planos de ação para mitigação daqueles riscos.

Merece realce o fato de que novos riscos podem ser identificados, ocorrência que deverá gerar pronta comunicação a área de Compliance e Controles

Internos para inserção na Matriz de Riscos, informando as áreas e/ou serviços impactados.

4.6.3 Gestão de Problemas e Incidentes de Segurança

O Departamento de TI deve desenvolver e manter um procedimento operacional, detalhando as atividades do processo de Gerenciamento de Incidentes e Problemas relacionados com segurança das informações e demais aspectos de TI.

O escopo deste processo de Gerenciamento de Incidentes e Problemas deve incluir qualquer evento que interrompa ou que possa interromper um serviço de TI, ou que impacte em perda da confidencialidade, integridade e disponibilidade de qualquer informação importante para os negócios.

O processo de Gerenciamento de Incidentes e Problemas deve abranger eventos que podem ser:

- Identificados pelas áreas de TI, incluindo Governança de TI/Segurança da Informação;
- Comunicados diretamente pelos usuários, usando os seguintes canais: telefone, e-mail, ou pela ferramenta GLPI (ferramenta específica para o registro e controle de chamados).
- Por ferramentas de Monitoramento, Rastreamento e Detecção de anomalias no ambiente informatizado.

O escopo do processo de Gerenciamento de Incidentes e Problemas, bem como a ferramenta GLPI, devem abranger todas as informações e registros de incidentes e problemas, tanto para Tecnologia da Informação como para desenvolvimento e manutenção de sistemas aplicativos.

Com base nas definições a seguir, uma lista de prioridades de atendimento deve ser elaborada sob a responsabilidade do Departamento de Tecnologia da Informação, bem como as evidências que deverão ser documentadas sobre cada atendimento:

- Incidente: refere-se qualquer evento que cause um desvio na operação normal de um serviço e que cause, ou possa causar, uma interrupção ou redução na qualidade deste serviço.
- Problema: refere-se a qualquer falha ininterrupta e ainda não corrigida, ou um evento que não seja parte da operação normal de um serviço e que esteja causando uma suspensão na disponibilidade daquele serviço.
- Categorização do chamado: os chamados serão categorizados de acordo com o atendimento a ser realizado, sendo categorizados como

incidentes, problemas ou requisições de serviço e solicitações de melhoria.

- Priorização do chamado: a priorização do chamado deve ser realizada em conjunto com o usuário envolvido, e, avaliada sua relevância, com a Diretoria, com base no incidente identificado, para estabelecer sua prioridade e urgência de resolução.
- Vazamento de Informação: refere-se a um incidente de segurança que produziu uma falha que expôs dados sensíveis ou informações confidenciais.

Caso o incidente seja relacionado com indícios ou fatos de perda de confidencialidade ou violação de documentos sigilosos, o Gestor da Informação deve informar, formal e imediatamente, seu superior hierárquico, a Diretoria, o departamento de TI e a área de Governança de TI/Segurança da Informação, que devem adotar medidas imediatas para remediação e para mitigar a vulnerabilidade causadora do ocorrido.

4.6.4 Gerenciamento de Mudanças

O Departamento de TI desenvolve e mantém um procedimento operacional, detalhando as atividades do processo de Gerenciamento de Mudanças na Infraestrutura e nos Sistemas, de forma a garantir a disponibilidade, integridade e confidencialidade das informações, sistemas e infraestrutura.

O processo de Gerenciamento de Mudanças tem como objetivo atender demandas relacionadas com mudanças na Infraestrutura de TI e sistemas informatizados do Bari. Tais mudanças podem ser necessárias para garantir a segurança das informações.

O processo prevê três categorias de mudanças – normal, padrão e emergencial - e garante que todas as atividades de mudança são documentadas, testadas, evidenciadas e aprovadas conforme as alçadas definidas.

4.6.5 Segurança Física

Todos os ativos de informação devem ser protegidos de acordo com a criticidade e importância para o Bari.

Os ativos classificados como confidenciais e de acesso restrito devem contar com recursos que restrinjam e controlem o acesso físico.

A área de Infraestrutura de TI é responsável pelo controle e monitoramento dos acessos físicos aos ativos de tecnologia e também pela definição de processos e indicadores necessários para a efetiva gestão destes acessos.

Todas as áreas que armazenam dados e informações classificadas como confidenciais e de acesso restrito devem contar com câmeras de monitoramento, bem como também áreas comuns, que dão acesso a estas áreas de proteção.

Adicionalmente, deve haver controles de acesso através de mecanismos de autenticação (biometria e/ou Magikey – sistema de autenticação via bluetooth ou NFC de aparelho móvel) nas principais entradas para colaboradores do Bari, e para acesso a sala de Data Center e Tesouraria. Somente colaboradores autorizados poderão acessar tais áreas. Pessoal de outros departamentos e terceiros somente poderão ter acesso a estas áreas por meio de requisição previamente aprovada pelo responsável do departamento.

O acesso de visitantes às dependências do Bari, deverá sempre ocorrer após a autorização de um funcionário e que sempre o acompanhará durante sua passagem pelo Bari.

4.6.6 Segurança Lógica e Gestão de Acessos Lógicos

A rede local utilizada para o acesso dos colaboradores aos sistemas de gestão das operações de negócios de todas as empresas que compõem o Bari deve ser segregada logicamente de qualquer outra rede que permita acesso público.

Fornecedores e prestadores de serviços devem usar conexão independente e segregada para acesso à Internet, não podendo utilizar a rede dos sistemas de produção do Bari.

Para garantir a segurança dos acessos lógicos às redes, sistemas, dados e demais serviços que fornecem informações, o Bari conta com um processo de gerenciamento de acessos, que garante a autenticação de cada acesso e que visa assegurar que as concessões e alterações em direitos de acesso sejam realizadas de forma controlada (avaliadas, registradas e aprovadas), reduzindo o risco e impacto de perda de confidencialidade, disponibilidade e integridade das informações.

O processo de Gerenciamento de Acessos Lógicos tem como objetivo atender demandas relacionadas aos diferentes níveis de acessos lógicos à Rede, aos Sistemas e aos Bancos de Dados do Bari, e deve garantir a opção de restrição de acesso aos dados, sistemas e demais recursos que armazenam e processam informações.

O Departamento de TI e a área de Governança de TI/Segurança da Informação são responsáveis por definir e disponibilizar o processo e ferramentas que permitam:

- Concessão de acessos à rede e sistemas (acesso somente ao que o usuário necessita);
- Alteração de acessos na rede e sistemas;
- Revogação de acessos;
- Revisão periódica de perfis de acessos sistêmicos (acesso e autoridade para execução das atividades);
- Administração da rede, sistemas e Bancos de Dados (incluindo acessos de terceiros);
- Gestão de usuários não nominais (genéricos).

Procedimentos de revisões periódicas são implementados com prazo máximo de 06 meses e devem ser devidamente formalizados e evidenciados. Alterações sistêmicas que demandem revisões de acessos e autoridades mais complexas devem ser planejadas antes de implementação em ambiente de produção.

Acessos privilegiados - aqueles concedidos para atualização, manutenção e administração dos sistemas, serviços e fluxos de trabalho que possam comprometer os controles de segurança existentes - deverão ser tratados com extrema cautela e controles, a fim de prevenir o seu uso indevido, por exemplo, contas e logins de administração de equipamentos, sistemas operacionais, bancos de dados e sistemas aplicativos.

A concessão de acesso privilegiado deve ser solicitada formalmente, através de abertura de chamado na ferramenta GLPI. Todos chamados referente a concessão de acessos privilegiados devem ser submetidos à aprovação do responsável pelo sistema/ferramenta solicitado acesso e/ou pelo responsável da área de Segurança da Informação.

Todo e qualquer acesso privilegiado concedido deverá possuir, no mínimo:

- Registro de controle e acompanhamento destes acessos, sob a responsabilidade da área de Segurança da Informação.
- Geração de logs para os logins que possuírem tais acessos.

Para o gerenciamento de usuário, as senhas devem ser criadas e compostas de acordo com os privilégios atribuídos às suas contas, devendo, portanto, ser tratadas como senhas administrativas e senhas não administrativas. As primeiras são aquelas associadas às tarefas de manutenção e administração de sistemas e ambientes computacionais, enquanto as últimas são aquelas senhas cujas contas são utilizadas para as atividades rotineiras e sem os privilégios de acesso concedidos às tarefas de manutenção e administração de sistemas.

Os técnicos do Departamento de TI deverão configurar os sistemas do Bari (sistemas operacionais, banco de dados, etc.) para que as senhas expirem a cada 90 dias, tanto para as administrativas quanto para as não administrativas.

As senhas devem ser criadas evitando o uso de combinações de fácil dedução, considerando, também, os aspectos a seguir para a sua composição:

- As senhas devem ter um tamanho mínimo de oito caracteres;
- Devem ser formadas a partir da combinação de caracteres alfabéticos, maiúsculos e minúsculos, numéricos e especiais (%, #, $, @, &, entre outros);
- Não é recomendado usar:
    - Palavras encontradas em dicionários de qualquer idioma;
    - dados pessoais, tais como: datas, placas de carro, nomes próprios e de pessoas conhecidas;
    - números ou letras repetidos, em sequência ou formando séries óbvias, como, por exemplo, “senhasenha”, “aaaabbbb“, “12345678”, “Ana0000”;
- Não deve ser permitida a reutilização das últimas 5 (cinco) senhas.

Quando for solicitada alteração de senha, deverão ser criados procedimentos de identificação que possam assegurar que o solicitante é o proprietário da senha a ser alterada.

As bases que contêm as senhas dos usuários devem ser protegidas contra acesso não autorizado, bem como separadas das outras informações do Bari.

Quando houver suspeita de vazamento das senhas dos usuários, deverão ser alteradas imediatamente pelo Departamento de Tecnologia da Informação e os usuários e seus gestores diretos deverão ser notificados, conforme o caso e extensão do incidente.

Devem ser disponibilizados mecanismos que permitam ao usuário a troca da senha quando o mesmo considerar necessário.

4.6.7 Uso de Dispositivos Móveis

O uso de dispositivos móveis de propriedade dos funcionários e prestadores de serviços dentro do ambiente do Bari é permitido, porém tais dispositivos somente podem ser conectados a redes públicas, segregadas das redes dos sistemas de produção do Bari.

Os dispositivos móveis fornecidos pelo Bari para uso de seus colaboradores poderão ser conectados às redes dos sistemas de produção, inclusive redes WI-FI. Equipamentos ligados à rede de produção não podem compartilhar ou abrir novas redes WI-FI.

4.6.8 Uso de Softwares e Aplicativos

Apenas os aplicativos e softwares disponibilizados, homologados e aprovados pelo Departamento de TI são permitidos para uso nos equipamentos do Bari.

É proibida a instalação de qualquer software ou aplicativo pelo próprio usuário. Todo e qualquer software somente poderá ser instalado pelo Departamento de TI. As instalações levarão em conta a licença existente e a presença do sistema na lista de softwares homologados para uso na empresa.

É obrigatório o uso de sistemas de proteção contra vírus e malwares, que para os equipamentos do Bari serão disponibilizados pelo Departamento de TI. Em equipamentos de terceiros ou prestadores de serviços será exigida a comprovação da existência de tais ferramentas, sendo o uso também obrigatório. A remoção ou paralização da ação destas ferramentas é considerada uma violação a esta política de segurança da informação e cibernética.

A instalação ou uso de software não autorizado pelo Departamento de Tecnologia da Informação pode ocasionar riscos graves para a segurança das informações do Bari, ficando o seu responsável sujeito às sansões cabíveis.

4.6.9 Transporte de Informações

As informações classificadas como confidenciais e de acesso restrito devem ser transportadas, ou seja, transferidas de seu local habitual de armazenamento, somente com autorização prévia e formal do Gestor da informação, em conjunto com a área de Segurança da Informação.

As informações confidenciais devem ser transportadas somente de forma controlada e registrada. Independentemente da forma adotada no transporte, o processo deve conter uma mensagem ao portador ou transportador, identificando o grau de sigilo daquela informação, bem como uma advertência para que o responsável pelo transporte redobre a atenção durante o processo, evitando descuidos que possam diminuir o grau de segurança do processo.

Todo arquivo de origem desconhecida ou conhecidamente de procedência externa, transportados por meios não seguros, como Pen-drive, USB Drive, Flash Memory, discos rígidos ou SSDs externos, CD/DVD/Blue Ray, celulares, máquinas fotográficas, Internet, ou qualquer outro meio de armazenamento e

transporte de dados deve ter o seu conteúdo verificado pela Área de Segurança da Informação antes de ser copiado para qualquer equipamento do Bari.

4.6.10Uso de E-mail e Outras Formas de Mensagens Eletrônicas

Os e-mails corporativos e as demais formas de comunicação e trocas de mensagens eletrônicas disponibilizadas aos colaboradores pelo Bari devem ser exclusivamente utilizadas para mensagens profissionais, relacionadas com os negócios do Bari.

Vale relembrar que, ao redigir qualquer tipo de mensagem escrita, incluindo e-mails, os colaboradores devem redobrar sua atenção, a fim de garantir que sejam corretamente interpretadas por seus destinatários finais, sem que haja a possibilidade de gerar qualquer desentendimento ou má publicidade, risco à imagem ou constrangimento público para o Bari, seus clientes, prestadores de serviços, parceiros ou acionistas.

É importante destacar a todos os colaboradores e prestadores de serviços que o e-mail é uma forma de comunicação extremamente vulnerável e passível de leitura e interceptação por terceiros. Assim, deve-se evitar a utilização do e-mail para troca de mensagens com informações confidenciais e/ou estratégicas para os negócios do Bari. Quando necessário, deve-se adotar criptografia nos arquivos anexados ou o uso de canais mais seguros, tais como: transferência eletrônica com protocolos seguros (por exemplo, SFTP) ou cópias gravadas em pastas seguras nos servidores de rede.

Adicionalmente, é terminantemente proibido o envio de documentos e informações classificadas como confidenciais ou de acesso restrito para e-mails pessoais ou em provedores públicos, tais como Gmail, Hotmail, Outlook, Yahoo e outros.

O Bari reserva-se ao direito de monitorar o conteúdo e armazenar todas as mensagens de e-mail e de outras formas de comunicação eletrônica que trafeguem pelos meios por ele disponibilizados, com o objetivo de se resguardar e assegurar as boas práticas de segurança, conforme determinado nesta Política.

Destaca-se também que o emitente das mensagens é considerado o único responsável pela segurança das informações contidas nestas mensagens.

4.6.11 Impressão de Documentos

Os equipamentos de impressão deverão ser configurados para somente imprimir documentos quando os usuários digitarem uma senha (PIN) presencialmente no equipamento.

Os colaboradores deverão recolher o material impresso imediatamente.

Todo o funcionário que constatar a presença de documentos impressos nos equipamentos sem a devida atenção do responsável, deverá comunicar o fato ao Gestor daquelas informações, ao responsável pela área de Governança de TI/Segurança da Informação e à área de Compliance e Controles Internos, que têm autonomia para destruir o que foi encontrado e não retirado da impressora, além de informar ao superior hierárquico do infrator.

Todo e qualquer documento somente deverá ser impresso se for estritamente necessário, observando princípios de preservação ambiental.

4.6.12 Mesa Limpa

O colaborador deve sempre bloquear seu computador ao deixá-lo desassistido, ainda que momentaneamente e não deve deixar informações sensíveis ou confidenciais disponíveis ao alcance de outras pessoas.

Ao final do expediente, todo colaborador deverá guardar todos os documentos, caso houver, em local fechado com chave e desligar sua estação de trabalho, a fim de deixar a sua mesa limpa e sem nenhum tipo de informação disponível.

Deve-se, ainda, manter os armários e gaveteiros devidamente trancados, evitando assim o acesso indevido a informações do Bari.

4.6.13 Segurança Cibernética

O Departamento de Tecnologia da Informação deve descrever as atividades de planejamento, controle, resposta e monitoramento dos mecanismos de Segurança Cibernética, ou seja, de proteção e segurança para prevenir, detectar e reduzir vulnerabilidades a ataques digitais à Infraestrutura de TI que suporta os principais sistemas e dados de operação dos negócios do Bari, incluindo os dados sensíveis aos negócios, classificados como “Confidenciais” e de “Acesso restrito” na Classificação das Informações do Bari.

Os objetivos dos procedimentos de gerenciamento de segurança e proteção contra-ataques digitais são:

- Identificar e conhecer as principais vulnerabilidades que podem permitir que um atacante, ou seja, uma pessoa não autorizada, seja ela interna ou externa, acesse informações, dados ou sistemas de negócios do Bari ou de seus clientes;

- Monitorar a eficácia dos processos e recursos de proteção contra os ataques digitais (Cyber Security), além de planejar e executar ações preventivas, sempre que necessário;

- Definir e executar ações corretivas de novas vulnerabilidades identificadas;

- Definir e executar ações de resposta a incidentes e problemas relacionados com ataques digitais.

4.6.14 Integração e Interfaces Sistêmicas

Os sistemas do Bari possuem rotinas automatizadas e interfaces com outros sistemas e instituições externas (regulatórias ou não), de forma que devem estar disponíveis para atender às demandas requeridas.

Os principais sistemas financeiros do Bari são o Lydians, Sicred, Prognum e ERSystems. Considerando a criticidade das interfaces e integrações entre estes sistemas, assim como das integrações de dados entre estes sistemas e outros sistemas externos, o Departamento de TI deverá garantir a existência de controles de integridade dos dados trafegados e pelo monitoramento das rotinas de troca de dados nestas interfaces sistêmicas, considerando as seguintes atividades:

- Desenvolvimento de rotinas de integração utilizando controles de prevenção contra perda de integridade dos dados. Por exemplo: adoção de controles automáticos utilizando recontagem da quantidade de registros, conciliação de valores totalizadores de campos, etc.

- Configuração das rotinas e interfaces para o envio automático de mensagens de alerta ao Departamento de Tecnologia da informação, no caso de falhas na execução;

- Tratativa de todos os erros (por exemplo: reexecução da rotina);

- Coleta e armazenamento de evidência da execução destas tratativas;

- Registro formal, em chamado, da tratativa do erro de execução.

Somente as áreas de TI (e os respectivos fornecedores dos sistemas, mediante aprovação do Gestor da Informação) poderão alterar as rotinas e os códigos executados nas interfaces entre os sistemas do Bari.

4.6.15 Telecomunicações e Conectividade

Os servidores contendo sistemas e dados críticos do Bari estão protegidos por soluções de "Firewall" nas conexões externas, soluções estas administradas pelo Departamento de TI.

A utilização de sistemas de detecção e prevenção de intrusos deve ser avaliada pelo Departamento de TI e aprovada pelos Diretores e pelo Conselho de Administração. Tais ferramentas inibem e/ou minimizam os riscos de tentativas de acesso tanto pela internet como entre redes.

O controle, a concessão de permissões e a aplicação de restrições em relação ao uso dos links de comunicação de dados e dos ramais telefônicos do Bari, assim como o uso de eventuais outras formas de comunicação utilizando tais recursos, como os ramais virtuais instalados nos computadores, é de responsabilidade do Departamento de Tecnologia da Informação e da área de Governança de TI/Segurança da Informação do Bari, de acordo com as definições da Diretoria.

Todas as formas de comunicação, incluindo ramais telefônicos, são monitorados e podem ter suas atividades gravadas e armazenadas em mídias internas do Bari. Estas gravações são armazenadas por um período de 5 (cinco) anos conforme regulamentos do CMN e do Banco Central do Brasil.

Para recuperação de um registro de ligações realizadas nas dependências do Bari, deverá ser aberto um chamado para o Departamento de TI, com aprovação prévia do Diretor responsável por aquele ramal.

4.6.16 Banco de Dados

As regras de segurança para as informações armazenadas e processadas por sistemas gerenciadores de bancos de dados são definidas pelo Departamento de Tecnologia da Informação e pela área de Governança de TI/Segurança da Informação do Bari.

Já a disponibilização, manutenção, atualização e proteção dos bancos de dados dos sistemas aplicativos contendo informações classificadas como confidenciais e de acesso restrito, bem como dos servidores que contém estes bancos de dados, são de responsabilidade do Departamento de TI.

4.6.17 Contratação de Terceiros

A fim de garantir o integral cumprimento das diretrizes legais e regulatórias, o Bari, ao contratar prestadores de serviços terceirizados, adota critérios estritos para selecionar os melhores profissionais do mercado. Isso é necessário para, além de manter seu padrão de qualidade oferecido ao cliente final, zelar pela adoção das melhores práticas corporativas.

Os principais critérios considerados no momento da contratação são a garantia, por parte do prestador, de que está apto a garantir os controles para prevenção e impedimento de lavagem de dinheiro e financiamento ao terrorismo, garantir

a segurança das informações, a proteção de dados e a continuidade dos negócios, de forma a atender aos mesmos padrões de segurança e qualidade.

No que tange especificamente às contratações de terceiros, pelo Bari, que processam e armazenam dados de seus clientes, são adotadas medidas e procedimentos exigidos pelo Banco Central do Brasil, nos termos da Resolução do CMN nº 4.893/2021. Além disso, atenção especial é despendida aos serviços relevantes e que tenham participação direta no trato com clientes e no manuseio de informações ou processamento de dados e de negócios, incluindo desenvolvimento e manutenção de sistemas, além de processamento e armazenamento de dados e de computação em nuvem.

Adicionalmente, as contratações de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelo Bari para o Banco Central em até dez dias após a contratação dos serviços. A área de Compliance e Controles Internos é responsável pela comunicação após receber os subsídios da área de Governança de TI/Segurança da Informação.

Assim, previamente à contratação de serviços de terceiros, o Bari adota procedimentos que contemplam as práticas de governança e gestão proporcionais à relevância do serviço a ser contratado e aos riscos relacionados, podendo realizar avaliações e *Due Diligence*s, verificando a capacidade do potencial prestador de serviço de assegurar:

- o cumprimento da legislação e das políticas do Bari e da regulamentação em vigor;
- o acesso completo do Bari aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- a confidencialidade, a integridade, a disponibilidade e a capacidade de recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- a sua aderência a certificações exigidas pelos órgãos reguladores para a prestação do serviço;
- o acesso do Bari a realizar diligencias próprias e também aos relatórios elaborados por empresa de auditoria especializada e independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços;
- o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços prestados;
- a identificação e a segregação dos dados dos clientes do Bari, por meio de controles físicos e lógicos;

- controles de acesso voltados à proteção dos dados e das informações dos clientes do Bari;
- a aderências às regras da Lei Geral de Proteção de Dados (LGPD).

Na avaliação da relevância do serviço a ser contratado, mencionada acima, consideramos os riscos da falta de aderência dos serviços contratados para os negócios, além do grau de criticidade do serviço e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo contratado e/ou pelos sistemas desenvolvidos e/ou mantidos pelo contratado, nos casos de serviços de processamento ou fornecimento de sistemas.

Para o cumprimento destes termos, o fornecedor a ser contratado deverá, antes da contratação, apresentar uma declaração relacionando todos os processos e controles de segurança de informações que adota em seu ambiente interno e também os que adotará na execução dos serviços ao Bari, para atendimento dos aspectos relacionados acima.

O Bari analisará a suficiência de tais controles para a execução dos serviços objeto do contrato e poderá avaliar ou auditar estes controles antes de aprovar a contratação do fornecedor.

Os procedimentos desta avaliação serão documentados.

4.6.18Monitoramento e Rastreabilidade

O Departamento de TI deve prover o monitoramento e a rastreabilidade das ações executadas nos ambientes computacionais, tanto aplicações quanto servidores e equipamentos de comunicação, com o objetivo de apoiar na avaliação dos incidentes. Sistemas de Prevenção e Detecção de Invasão devem ser avaliados e instalados no ambiente para monitoramento de ações adversas ao ambiente como possíveis ações intrusivas.

A equipe de Segurança da Informação deve ter acesso às informações de rastreabilidade quando necessário, contudo, informações dos últimos 02 meses devem estar disponíveis imediatamente. As informações reportadas pelos sistemas de detecção devem ser registradas para análise e resposta se necessário. Havendo confirmação de um incidente de segurança, este deve seguir o fluxo de tratamento e Comunicação.

Em consonância com a Resolução CMN nº 4.557/2017, a estrutura de gerenciamento de riscos do Bari deve prever, entre outros controles: "sistemas, processos e infraestrutura de TI que incluam mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais".

4.6.19 Backups e Cópias de Segurança

As áreas de Infraestrutura de TI e Segurança Cibernética devem assegurar a execução das cópias de segurança dos dados, informações, sistema e ambientes do Bari. As cópias de segurança são armazenadas em ambiente de nuvem e devem estar protegidas contra acesso indevido às informações, devem ser testadas periodicamente e disponíveis para recuperação tanto em ambiente de contingência quanto em produção regular. Os dados a serem guardados, sua periodicidade de cópia, retenção e validade devem estar descritos e validados pela Diretoria.

A guarda dos instaladores de sistemas, aplicações, configuração de equipamentos, regras de ambientes tecnológicos, etc., também devem ser protegidos contra perda e estarem disponíveis para uso quando necessário.

4.6.20 Guarda e Uso de Chaves de Criptografia Privadas

O Departamento de TI e a área de Governança de TI/Segurança da Informação devem garantir que cada chave privada de criptografia, incluindo os arquivos e dispositivos contendo os certificados digitais do Bari, possuam pelo menos uma cópia de segurança, guardada em local seguro, preferencialmente em cofre trancado.

A área de Governança de TI/Segurança da Informação será a responsável por definir o custodiante de cada chave privada, bem como será o responsável pela guarda segura da cópia daquela chave.

Os custodiantes devem ser escolhidos levando em consideração critérios éticos, além de seu histórico e reputação. Devem também ter, ao menos, conhecimentos mínimos de computação e de como manipular arquivos digitais de forma segura.

A área de Governança de TI/Segurança da Informação deve orientar os custodiantes acerca de sua responsabilidade, das práticas corretas de manuseio com segurança das chaves privadas e do prazo de custódia. Deve também exigir que os custodiantes assinem um Termo de Compromisso e Responsabilidade conforme Anexo II desta política.

O Termo de Compromisso e Responsabilidade deve possuir, pelo menos, os seguintes termos:

- que o custodiante se compromete a manter em sigilo que está custodiando chaves privadas;

- que o custodiante se compromete a manter em sigilo o local de guarda da chave privada;
- que o custodiante não irá entregar a chave privada para qualquer pessoa, salvo quando solicitado formalmente pela área de Tecnologia e Segurança da Informação e após aprovado pela Diretoria do Bari;
- que o custodiante deve manter a chave privada em local seguro, não identificado e protegido por senha; e
- o prazo de custódia será de, no máximo, 05 anos.

A área de Governança de TI/Segurança da Informação deve garantir que os custodiantes das chaves privadas não tenham acesso ao ambiente de produção das bases de dados criptografados.

A área de Governança de TI/Segurança da Informação deve solicitar a chave privada ao custodiante quando:

- O método de criptografia se tornar obsoleto. Neste caso, a chave será usada para refazer os dados usando os métodos mais recentes e seguros;
- Houver comprometimento ou suspeita de comprometimento da chave privada ou dos dados; ou
- O tempo máximo de armazenamento estiver expirado.

A solicitação da chave privada deve ser feita via abertura de chamado na ferramenta GLPI e deve ser aprovada pela Diretoria do Bari.

O custodiante, mediante a entrega da CHAVE PRIVADA, deve assinar o termo específico para este fim, onde se encerra sua responsabilidade.

A área de Governança de TI/Segurança da Informação deve garantir que os Termo de Responsabilidade e Compromisso, os nomes e os dados dos custodiantes estejam armazenados dentro de um ambiente seguro no Bari, sob a classificação CONFIDENCIAL.

A área de Segurança da Informação deve manter uma lista dos "hash" das chaves que já foram utilizadas e descartadas, para que elas não sejam reaproveitadas no futuro.

4.6.21 Gestão de Vulnerabilidade e Testes de Invasão

A execução de análise de vulnerabilidade periódica nos ambientes computacionais visa identificar falhas existentes. A necessidade de correção das vulnerabilidades identificadas deve acontecer conforme listado em relatório do nível mais alto de criticidade para o mais baixo.

A exposição de vulnerabilidade através de um Teste de penetração demonstra ao Bari o quanto a informação pode estar ameaçada pela falta de controles e de implementações de segurança. A realização de Testes de Penetração Internos e Externos nos serviços mais críticos promovem o aumento da segurança pela identificação e correção dos riscos sistêmicos apontados.

Tanto o resultado das análises de vulnerabilidades, quanto dos Testes de penetração devem ser documentados e acompanhados no plano de ação.

4.6.22 Normas Relacionadas com PCI-DSS

Esta Política, Normas e Procedimentos de Segurança da Informação desenvolvidos no Bari devem atender a todos os requisitos do PCI/DSS. Os principais pontos são:

- Documentação para Classificação da Informação, assim como toda mídia deve ser classificada e rotulada;

- Todos os componentes de sistema devem ser configurados de forma adequada e segura. De acordo com as suas características e utilização, os equipamentos devem ter aplicados procedimentos de *hardening* (mapeamento de ameaças), proteção contra *malwares* e agentes intrusivos, atualização de *patches*, geração, captura e análise das trilhas de auditorias e correlação de eventos em sistema centralizado;

- Deve haver documentação e procedimentos para gestão de mudança (GMUD). Os procedimentos de GMUD devem ser aplicados para todos os componentes do sistema;

- Todos os acessos físicos aos diversos ambientes que contenham dados do portador do cartão devem ser registrados e armazenados por três meses. Também, deve haver monitoração por câmeras em todos os principais ambientes que possuam dados do portador do cartão;

- Deve haver utilização de crachás para funcionários, fornecedores e prestadores de serviços e visitantes, onde os crachás de funcionários devem ser diferentes dos demais crachás;

- Deve haver Plano e Procedimentos para resposta a incidente de segurança da informação; e

- Devem ser realizados testes de invasão, varredura de vulnerabilidades, e aplicação de análise de riscos de acordo com os períodos especificados pelo PCI/DSS.

4.6.23 Plano de Resposta a Incidentes

Estabelece um conjunto de atividades necessárias para acompanhamento interno e externo de ações inesperadas que promovam falhas em ambientes computacionais que possam levar prejuízos financeiros ou de imagem ao Bari:

- Time de Resposta: Designar equipe especializada para preparação do ambiente, monitoração, análise, execução e resolução dos Incidentes.
- Liderança: Gestor Responsável pela tomada de decisão ou encaminhamento da tomada de decisão por outras lideranças.
- Registro: Local ou ferramenta para controle e acompanhamento dos incidentes de Segurança
- Comunicação: canais estabelecidos interna e externamente para envio e recebimento de informações
- Detecção: Ferramentas para análise de comportamento de rede e/ou aplicação e identificação de anomalias.
- Classificação: Dimensionar os incidentes por critérios objetivos de exposição (Riscos Ocorridos).
- Identificação: Confirmação das informações necessárias para execução das ações de correção
- Contenção: Separação do evento evitando contaminação de outros ambientes, a continuação de perda de informações ou acessos dos indevidos.
- Evidenciação: Preservação de informações para perícia/ação judicial e backup dos dados contaminados para análise detalhada do ataque e dos vazamentos.
- Recuperação: Restabelecimento do ambiente a produção com as devidas correções e com as mitigações para não ocorrência de novo incidente.
- Reporte: Comunicação Interna e Externa sobre informações do Incidente (conforme regulamentação)
- Lições Aprendidas: Análise para melhorias continua no processo e na capacitação da equipe de Resposta a Incidentes.

4.6.24 Plano de Ação

O objetivo é o controle e o acompanhamento das melhorias propostas para a Organização no âmbito da Segurança da Cibernética.

Um plano de ação pode ser descrito como uma atividade específica ou um projeto com muitas atividades, o importante é conter informações que resumam o acompanhamento e respondendo as seguintes perguntas:

- What (O que?) - Descreve o problema ou o motivo da existência de um projeto
- Why (Por quê?) - Listar as possíveis causas do problema a ser resolvido ou as vantagens que a empresa pode ter ao investir em determinado projeto.
- Where (Onde?) - Delimite os departamentos sobre os quais o projeto terá impacto.
- When (Quando?) - Definir o prazo para começar e terminar a execução de todas as tarefas.
- Who (Quem?) - Listar os responsáveis, os executores, quem irá avaliar resultados.
- How (Como?) - Listar os métodos utilizados para colocar o projeto em prática e os indicadores de performance escolhidos para acompanhar seu andamento.
- How Much (Quanto?) - Estimar os custos que as soluções propostas terão para a empresa, isso ajudará a avaliar a viabilidade de cada ideia.

4.6.25 Relatório de Conformidade e Melhoria Contínua e Plano de Ação e de Resposta a Incidentes

O Diretor responsável por esta Política deve entregar um relatório anual contendo resultados obtidos nas seguintes implementações:

- Efetividade das ações propostas no Plano de Ação para cumprimento desta Política.
- Resumo dos resultados obtidos com implementação de ações de prevenção e resposta a incidentes.
- Incidentes de Segurança relevantes ocorridos no período.
- Resultado dos Testes de continuidade de Negócio.

Este relatório deve ser submetido ao Comitê de Gestão de Riscos, quando existir, e apresentado à Diretoria e ao Conselho de Administração até 31 de março do ano subsequente.

4.7 Divulgação

A Política de Segurança da Informação e Cibernética, bem como os procedimentos operacionais relacionados, serão divulgados por meio de:

- Campanhas de conscientização
- Treinamentos
- Comunicados internos
- Área de Governança de TI/Segurança da Informação
- Alta Direção de Organização
- Intranet, mensagens instantâneas e outros meios de divulgação interna
- Avaliação periódica do conhecimento de segurança dos funcionários

Deve ser divulgado ao público, resumo contendo as linhas gerais desta política, mediante linguagem clara e acessível.

Os prestadores de serviço e os parceiros devem ter acesso à capacitação de segurança da informação e segurança cibernética em suas organizações. Caso não seja possível, deverá ser disponibilizado pelo próprio Bari, antes da prestação dos serviços.

Clientes e usuários devem ser informados sempre que possível sobre melhores práticas na utilização dos serviços e sistemas disponibilizados pelo Bari, bem como das ações de segurança implementadas para este fim. Uma linguagem adequada deve ser utilizada para o público externo, ressaltando as linhas gerais da segurança.

4.8 Penalidades

O não cumprimento de qualquer um dos itens presentes nesta Política e em Procedimentos associados poderá implicar em sanções disciplinares, sanções administrativas, legais e/ou penais, dependendo do grau e natureza da infração.

Ao observar uma violação da Política de Segurança da Informação e Cibernética, o usuário observante deve comunicar a infração aos responsáveis pela Segurança da Informação do Bari. Caso seja detectado que o colaborador não comunicou a infração, mesmo sabendo da sua existência, pode ser considerado conivente com a sua ocorrência e, assim, também estar sujeito a sansões.

Em nenhuma hipótese será admitida a alegação de desconhecimento para o não cumprimento desta Política de Segurança da Informação e Cibernética.

5. GLOSSÁRIO

- Ativos - Tudo aquilo que manipule direta ou indiretamente uma informação. Em termos de segurança da informação, um ativo pode ser um computador, uma impressora, um fichário na recepção, o próprio usuário etc. Não deve ser confundido com o ativo patrimonial.
- Autenticidade - Declaração de que o dado ou informação são verdadeiros e confiáveis tanto na origem quanto no destino.
- Certificado Digital - Documento eletrônico que contém informações necessárias para correta identificação do portador, o mesmo deve prover mecanismos para garantir autenticidade, confidencialidade e integridades de informações.
- Chave privada – (ou chave criptográfica privada) é um arquivo usado em vários métodos de criptografia para cifrar ou decifrar mensagens ou qualquer conteúdo digital. Em métodos de criptografia que usam chaves assimétricas, há duas chaves diferentes, uma para cifrar e outra para decifrar. Quando uma chave é usada para cifrar, a outra é usada para decifrar, não sendo possível usar a mesma chave para cifrar e decifrar ou vice-versa. A chave privada, neste contexto é a chave capaz de decifrar um conteúdo previamente cifrado com a chave pública.
- Ciclo de Vida - Criação ou aquisição, utilização, transporte, guarda e descarte de uma informação.
- Ciclo de Vida da Informação - Desde o momento em que informação ela é gerada, rotulada, manipulada, armazenada, transmitida até a sua destruição.
- Classificação - Atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação.
- Código Fonte - É qualquer sequência ou declaração escrita em alguma linguagem de programação. Estas linguagens são a ponte de comunicação entre o programador e o computador. Quando o programa está finalizado, é feita uma compilação do código fonte, que o transforma em linguagem de máquina para que o computador consiga interpretar.
- Confidenciais - Informações que pertencem à empresa e informações de clientes, que foram geradas ou adquiridas e que se reveladas, podem trazer impactos negativos aos negócios ou repercussões para a imagem da mesma, embaraços administrativos com colaboradores ou vantagens a concorrentes e terceiros.
- Custodiante - Colaborador responsável pela guarda adequada da informação.

- **Desclassificação** - Cancelamento, pelo gestor competente, da classificação, tornando públicos dados ou informação.
- **Gestor da Informação** - Colaborador responsável pelas informações e recursos sob sua gestão, o qual os classifica conforme seu grau de sigilo.
- **GLPI** – Ferramenta gestora de chamados (Abertura, acompanhamento, encerramento e registro de chamados).
- **Grau de Sigilo** - Gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo.
- **Guarda Permanente** - Consideram-se de guarda permanente os dados ou informações de valor histórico, probatório e informativo que devam ser definitivamente preservados.
- **Hash** – Código gerado por um método criptográfico, de forma a identificar unicamente um conteúdo digital;
- **Internas** - Todas as informações geradas, possuídas ou custodiadas pela empresa, que podem ser acessadas por todos os colaboradores, mediante autorização do respectivo proprietário.
- **Legitimidade** - Asseveração de que o emissor e o receptor de dados ou informações são legítimos e confiáveis tanto na origem quanto no destino.
- **Malwares** - Código malicioso de computador ou programa malicioso – uma parte de um código executável – com capacidade de auto replicação podendo destruir arquivos, formatar a unidade de disco rígido, roubar informações sensíveis ou causar outros danos.
- **PCI/DSS (Payment Card Industry/Data Security Standards)** - É uma organização que dita os padrões de Segurança da Informação para ambientes que armazenem, transmitam ou processem dados do portador do cartão.
- **Prestador de Serviço** - Todo profissional terceirizado executando atividades pontuais.
- **Público** - Informações de caráter informativo, profissional ou que, em função da legislação vigente, podem ser divulgadas ao público externo à empresa, mediante a avaliação e aprovação da área responsável pela comunicação da empresa.
- **Reclassificação** - Alteração, pelo gestor competente, da classificação de dados, informação, área ou instalação sigilosas.
- **Segurança da Informação** – Conceito que abrange a garantia da confidencialidade, da integridade e da disponibilidade das informações.

- **Terceiro** - Todo profissional terceirizado executando atividades profissionais com jornada de trabalho fixa e regular.
- **Vulnerabilidade** - Fragilidade ou fraqueza que podem ser exploradas por ameaças e tornar-se um incidente.

6. VIGÊNCIA

Esta Política entra em vigor na data de sua publicação e permanece vigente até sua atualização.

7. BASE REGULATÓRIA

- **Resolução nº 2.554** do Conselho Monetário Nacional, de 24.09.1998 - Dispõe sobre a implantação e implementação de sistema de controles internos;
- **Resolução nº 4.893/2021** do Banco Central do Brasil, de 26.02.2021 - Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução nº 4.557/2017** do Conselho Monetário Nacional, de 23.02.2017 – Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital;
- **Circular nº 3.467/2009** do Banco Central do Brasil – Estabelece critérios para elaboração dos relatórios de avaliação da qualidade e adequação do sistema de controles internos e de descumprimento de dispositivos legais e regulamentares e dá outras providências;
- **Lei nº 13.709/2018 do Planalto, de 14.08.2018 – Lei Geral de Proteção de Dados;**
- **COBIT - Control Objectives For Information and Related Technology** – "Framework" de boas práticas para Governança e Gestão de TI.
- **ABNT NBR ISO/IEC 27001:2013** – Sistema de Gestão de Segurança da Informação.
- **ABNT NBR ISO/IEC 27002:2013** – Código de Prática para Gestão da Segurança da Informação
- Payment Card Industry/Data Security Standards (PCI/DSS) v.3.2

8. CONTROLE DE ALTERAÇÕES

VERSÃO	MOTIVO	DATA
v001	Criação do Documento e substituição do POP STI 01 – Tecnologia da Informação	01/04/2019
v002	Atualização da Política e junção dos temas Segurança Cibernética e Segurança da Informação em uma única Política	10/12/2021

9. ANEXOS

Anexo I – Termo de Ciência e Aceite quanto à Política de Segurança da Informação e Cibernética;

Anexo II – Termo de Compromisso e Responsabilidade do Custodiante de Chaves Privadas.

ANEXO I

TERMO DE CIÊNCIA E ACEITE QUANTO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Por este instrumento, eu, _____,

colaborador do(a) _____,

portador do RG nº _____, declaro que:

a) Tive acesso ao documento PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA;
b) Li o documento e tenho plena compreensão de seu conteúdo, estando ciente das condições descritas e da minha responsabilidade em cumprir com as suas determinações;
c) Estou ciente de que todas as minhas atividades, utilizando recursos do Bari, podem ser monitoradas e auditadas, sem aviso prévio;
d) Estou ciente de que a não conformidade para com o disposto na Política de Segurança da Informação e Cibernética pode acarretar em medidas disciplinares e outras medidas aplicáveis; e
e) Comprometo-me a seguir integralmente todas as diretrizes do documento recebido, zelando plenamente pela segurança de todas as informações sensíveis com as quais poderei ter contato.

Tipo de contrato do colaborador:

[ ] Funcionário [ ] Estagiário [ ] Terceiro [ ] Outro

_____

Área de atuação do colaborador: _____.

Líder imediato: _____.

Local e Data : _____, _____/_____/_____

_____

Assinatura do COLABORADOR

ANEXO II

TERMO DE COMPROMISSO E RESPONSABILIDADE DOS CUSTODIANTES DE CHAVES PRIVADAS

COMO CUSTODIANTE DA CHAVE PRIVADA(Descrição)_____
DO(A) _____.

EU,_____,
RG_____,

ESTOU CIENTE DAS NORMAS DEFINIDAS NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA, EM RELAÇÃO À SEGURANÇA DAS CHAVES PRIVADAS DE CRIPTOGRAFIA, COMPROMENTENDO-ME A:

- Manter a chave privada em local seguro, não identificado e protegido contra acessos indevidos, durante o prazo de vigência da chave;
- Manter em sigilo que estou custodiando chave privada;
- Não entregar a chave privada para ninguém, salvo quando solicitado formalmente pela DIREÇÃO do Bari;
- Se houver indícios de comprometimento da chave privada, avisar formal e imediatamente à Diretoria Bari.

_____ _____ / _____ /_____

Custodiante da Chave Privada Data