POLÍTICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

1. OBJETIVO

O objetivo desta política é promover as práticas de segurança para o trânsito das informações no âmbito do Conglomerado Financeiro Bari (Conglomerado), formado pelo Banco Bari de Investimentos e Financiamentos S/A ("Banco") e a Bari Companhia Hipotecária ("Hipotecária"), na forma de Diretrizes e Normas, para o trato de seus ativos e passivos, disseminando uma cultura de segurança das informações, 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 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 as empresas do Conglomerado.

Na busca constante pela excelência de nossos serviços, esta Política é uma declaração formal do Conglomerado em relação ao seu comprometimento em proteger todas as suas informações sensíveis, apoiando metas e princípios de Segurança da Informação, 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 Conglomerado.

2. ABRANGÊNCIA

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

3. REGRAS E DIRETRIZES

A informação é um ativo de alto valor para o Conglomerado 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 Conglomerado seguiu diretrizes determinadas por seu Conselho de Administração, de acordo com as boas práticas de segurança das

informações, 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 Cibernética e os procedimentos operacionais relativos ao cumprimento das normas aqui definidas estejam compatíveis com os requisitos legais e regulamentares aplicáveis ao Conglomerado.
- 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 Conglomerado 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.
- 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 das Instituições, 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.
- Garantir que todos os colaboradores, parceiros e prestadores de serviço conheçam e cumpram com as exigências desta Política.

3.1. 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 Conglomerado, 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 Conglomerado.

- 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 Conglomerado 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 Conglomerado, não podendo ser reveladas em ambientes públicos, como elevadores, taxis, restaurantes, etc.

- Dúvidas sobre a Política e Normas de Segurança da Informação devem ser imediatamente esclarecidas com os Gestores ou o responsável da área de SEGURANÇA DA INFORMAÇÃO.

3.2. Diretrizes para Propriedade Intelectual

Todos os documentos produzidos por intermédio de recurso de processamentos do Conglomerado 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 Conglomerado.

3.3. Diretrizes para Privacidade e Proteção de Dados Pessoais

Informações armazenadas, tratadas ou enviadas por meio de recursos do Conglomerado 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 Geral de Proteção de Dados.

Todos os dados pessoais de colaboradores, parceiros e clientes serão considerados dados confidenciais. O Conglomerado 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 Conglomerado 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 Conglomerado estão sujeitos a monitoramento. Assim, ao utilizar qualquer recurso do Conglomerado, os usuários automaticamente consentem este monitoramento.

3.4. 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 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 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.

3.5. 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 Conglomerado, de forma que estas possam ser mantidas protegidas de acordo com sua relevância e grau de confidencialidade para os processos de negócios do Conglomerado.

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, 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 ao negócio 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 reconhecimento da Diretoria, Controladoria e Compliance deste Conglomerado Financeiro.

Informações de terceiros sob responsabilidade ou custódia do Conglomerado 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.

3.6. Normas de Segurança das Informações

3.6.1 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 Conglomerado 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 Banco.

Sempre que houver a necessidade de alteração do PCN, a nova redação deverá ser revisada e aprovada pela Diretoria e pelo Conselho de Administração. O Departamento de Tecnologia e área de Segurança da Informação devem atualizar o documento e informar a nova versão a todos os colaboradores envolvidos, bem como submeter para nova aprovação pela Diretoria e Conselho.

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 pelo Departamento de Tecnologia 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 e alimentando melhorias/correções para o PCN.

3.6.2 Gestão da Disponibilidade de Sistemas e Informações

Cabe à área de 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 Conglomerado.

Para isso, a área deverá atuar em conjunto com o Departamento de Governança, inserindo e atualizando os riscos relacionados com disponibilidade na Matriz de Riscos do Conglomerado, 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 Conglomerado. 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 da instituição. 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 equipe do Departamento de Governança e da Diretoria.

Caberá também à área de Segurança da Informação a responsabilidade de informar ao Departamento de Governança os fatos apurados no tocante aos riscos listados na matriz de riscos do Conglomerado. Em havendo a materialização de impactos relativos à disponibilidade dos sistemas, informações e serviços de TI, deve a área de 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 ao Departamento de Governança para inserção na Matriz de Riscos, informando as áreas e/ou serviços impactados.

3.6.3 Gestão de Problemas e Incidentes de Segurança

O Departamento de TI deverá desenvolver e manter o 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 Segurança da Informação;
- Identificados pelo Departamento de Governança; e
- Comunicados diretamente pelos usuários, usando os seguintes canais: telefone, e-mail, ou por sistema de gestão de help desk (ferramenta específica para o registro e controle de chamados definidos pelo Conglomerado).
- Por ferramentas de Monitoramento, Rastreamento e Detecção de anomalias no ambiente.

O escopo do processo de Gerenciamento de Incidentes e Problemas, bem como as ferramentas de registro de chamados de help-desk, 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 a qualquer falha pontual ou um evento que não seja parte da operação normal de um serviço, que pode causar uma redução na qualidade, acesso indevido ou indisponibilidade temporária daquele 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, sopesada 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 Segurança da Informação, que devem adotar medidas imediatas para remediação e para mitigar a vulnerabilidade causadora do ocorrido.

3.6.4 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 Conglomerado. Tais mudanças podem ser necessárias para garantir a segurança das informações.

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

3.6.5 Segurança Física

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

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

O Departamento de TI e a área de Segurança da Informação são responsáveis pelo controle e monitoramento dos acessos físicos aos ativos de tecnologia e também pela definição de procedimentos 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 liberação biométrica na entrada para colaboradores do Conglomerado, para acessos aos Departamentos de Tecnologia da informação e Tesouraria. Somente colaboradores destes departamentos 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 Conglomerado deverá sempre ocorrer após a autorização de um funcionário e que sempre o acompanhará.

3.6.6 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 Conglomerado 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 Conglomerado.

Para garantir a segurança dos acessos lógicos às redes, sistemas, dados e demais serviços que fornecem informações, deve haver um processo de gerenciamento de acessos, que garanta a autenticação de cada acesso e que vise 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 Conglomerado, 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 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 devem ser 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, por escrita ou por ferramenta de solicitação, pelo gestor do colaborador ao gestor da informação, assim como à 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 Conglomerado (sistemas operacionais, banco de dados, etc.) para que as senhas expirem a cada 90 dias, tanto para as senhas administrativas quanto para as senhas 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, mas combinações esparsas de letras;
    - 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 4 (quatro) 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.

Quando da necessidade de impressão das senhas, devem ser criados procedimentos para que não sejam reveladas a pessoas não autorizadas.

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

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.

3.6.7 Uso de Dispositivos Móveis

O uso de dispositivos móveis de propriedade dos funcionários e prestadores de serviços dentro do ambiente do Conglomerado é permitido, porém tais dispositivos somente podem ser conectados a nossa rede wifi que está segregada das redes dos sistemas de produção do Conglomerado.

Em casos excepcionais, em que seja necessário o uso na rede dos sistemas de negócios, em decorrência de atividade ou situação específica, o colaborador deverá enviar solicitação formal a área de Segurança da Informação, contendo aprovação prévia da Diretoria. A área de Segurança da Informação avaliará o cenário e concederá acesso temporário e específico, desde que o grau de risco esteja dentro de parâmetros aceitáveis.

Os dispositivos móveis fornecidos pelo Conglomerado 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.

3.6.8 Uso de Softwares e Aplicativos

Apenas os aplicativos e softwares disponibilizados, homologados e aprovados pelo Conglomerado são permitidos para uso nos equipamentos do Banco.

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 Conglomerado serão disponibilizados pelo Departamento de TI. Em equipamentos de terceiros ou prestadores de serviços será exigida a comprovação da existência de tais sistemas, sendo o uso também obrigatório. A remoção ou paralização destes sistemas é considerada uma violação a esta política de segurança.

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

3.6.9 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 Banco.

3.6.10 Uso 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 Conglomerado devem ser exclusivamente utilizadas para mensagens profissionais, relacionadas com os negócios do Banco.

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 Conglomerado, 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 Conglomerado. Quando necessário, recomenda-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 Conglomerado 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.

3.6.11 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 Segurança da Informação e à área de Compliance, 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.

3.6.12 Mesa Limpa

O colaborador deverá sempre bloquear seu computador ao deixar a estação de trabalho, ainda que momentaneamente e não deverá deixar informações sensíveis ou confidenciais disponíveis ao alcance de outras pessoas.

Ao final do expediente, todo colaborador deverá guardar todos os documentos 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 Conglomerado.

3.6.13 Integração e Interfaces Sistêmicas

Os sistemas do Conglomerado 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 Conglomerado 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: re-execução 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 Conglomerado.

3.6.14 Telecomunicações e Conectividade

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

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 Conglomerado, 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 Segurança da Informação deste Conglomerado, de acordo com as definições da Diretoria.

Todos as formas de comunicação, incluindo ramais telefônicos, são monitorados e podem ter suas atividades gravadas e armazenadas em mídias internas do Conglomerado. 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 deste Conglomerado, deverá ser aberto um chamado para o Departamento de TI, com aprovação prévia do Diretor responsável por aquele ramal.

3.6.15 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 Segurança da Informação do Conglomerado.

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 do Grupo Bari, sendo estes serviços contratualmente acordados entre as partes.

Cabe ao Departamento de Tecnologia da Informação do Conglomerado monitorar o funcionamento das operacionalidades transacionais ocorridas nos bancos de dados do Conglomerado. Este Departamento deverá ainda reportar formalmente ao Departamento de TI do Grupo Bari qualquer alerta, evidências e/ou suspeita de mau funcionamento, inoperância ou vulnerabilidades de segurança nestes serviços.

Em caso de catástrofes ou falhas nos servidores de banco de dados, é também de responsabilidade do Departamento de TI do Grupo Bari a recuperação do hardware e dos respectivos softwares afetados, ficando somente ao Departamento de Tecnologia da Informação do Conglomerado a responsabilidade pela reconfiguração lógica destes serviços.

3.6.16 Contratação de Terceiros

A fim de garantir o integral cumprimento das diretrizes legais e regulatórias, o Conglomerado, 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, e 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 Conglomerado, 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 4.658/2018. 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.

Assim, previamente à contratação de serviços de terceiros, o Conglomerado Financeiro 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 Diligences*, verificando a capacidade do potencial prestador de serviço de assegurar:

- o cumprimento da legislação e das políticas do Conglomerado e da regulamentação em vigor;
- o acesso completo do Conglomerado 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 Conglomerado 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 Banco, por meio de controles físicos e lógicos;
- controles de acesso voltados à proteção dos dados e das informações dos clientes do Banco.

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 Conglomerado, para atendimento dos aspectos relacionados acima.

O Conglomerado 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.

3.6.17 Monitoramento e Rastreabilidade

O Departamento de TI deve prover o monitoramento e a rastreabilidade das ações executadas nos ambientes computacionais, tanto aplicações quando 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 Conglomerado 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".

3.6.18 Backups e Cópias de Segurança

O Departamento de TI deve prover a guarda de cópias de segurança dos dados, informações, sistema e ambientes do Conglomerado. As cópias de segurança devem estar protegidas, testadas e disponíveis para recuperação tanto em ambiente de contingência quanto em produção regular. Os dados a serem guardados, sua periodicidade de cópia, e validade deve 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.

3.6.19 Guarda e Uso de Chaves de Criptografia Privadas

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

A área de 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 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.

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 direção do Conglomerado;
- 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 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 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 por escrito e aprovada pela direção do Conglomerado.

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

A área de 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 Conglomerado, 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.

3.6.20 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 Conglomerado 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.

3.6.21Plano 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 Conglomerado:

- 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.

3.6.22 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.

3.6.23 Relatório de Conformidade e Melhoria Contínua

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.

3.7 Divulgação

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

- Campanhas de conscientização
- Treinamentos
- Comunicados internos
- Equipe de Segurança Cibernética

- Alta Direção de Organização
- Intranet, mensagens instantâneas e outros meios de divulgação interna
- Avaliação periódica do conhecimento de segurança dos funcionários

Os prestadores de serviço e os parceiros devem ter acesso à capacitação de segurança cibernética em suas organizações. Caso não seja possível, deverá ser disponibilizado pelo próprio Conglomerado, 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 Conglomerados, 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.

3.8 Penalidades

O não cumprimento de qualquer um dos itens presentes nesta Política de Segurança Cibernética e Normas associadas 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 Cibernética, o usuário observante deve comunicar a infração aos responsáveis pela Segurança da Informação do Conglomerado. 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 Cibernética.

4. 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.
- 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.

5. RESPONSABILIDADES

5.1. Conselho de Administração

- Aprovar a Política de Segurança Cibernética, o Plano de Resposta a Incidentes e os Planos de Ação.

5.2. Diretoria

- Revisar, aprovar, implementar e garantir o cumprimento desta Política;
- Indicar as principais diretrizes, referendando e adotando procedimentos, bem como delegando as demais responsabilidades;
- Apoiar todos os esforços para que esta Política e seus anexos cheguem a todos os colaboradores, parceiros e prestadores de serviço terceirizados;
- Indicar um Diretor, que ficará responsável por esta Política e também pelo Plano de Ação e o Plano de Resposta a Incidentes.

5.3. Área de Tecnologia da Informação

- Fornecer todos os recursos de tecnologia, incluindo ferramentas, hardware, software, serviços de TI e executar os processos necessários para o cumprimento das diretrizes e normas definidas neste documento;
- Garantir o funcionamento adequado e contínuo de todos os ativos de tecnologia sob sua responsabilidade;
- Desenvolver, implementar e executar os devidos procedimentos operacionais dos processos de segurança determinados nesta política;
- Realizar processos de avaliação de riscos para a segurança das informações, identificando ameaças e vulnerabilidades, gerando relatórios com os resultados conclusivos sobre tais avaliações de risco;
- Apoiar na contratação dos serviços com os fornecedores de TI e dos fornecedores de sistemas aplicativos, acompanhando e dando suporte às solicitações de alterações na infraestrutura e nos sistemas, quer sejam por demanda interna (solicitação de alteração ou desenvolvimento de nova funcionalidade) quanto por solicitação do próprio fornecedor (nova versão do pacote, por exemplo);
- Registrar, criar, manter e distribuir os planos de ação e de resposta a incidentes de segurança e os devidos procedimentos de escalonamento, quando necessário, incluindo:
  a) As estratégias de comunicação e definição de responsabilidades; e
  b) Informações detalhadas sobre a incidentes, problemas relacionados e seus efeitos no Conglomerado.

- A comunicação com outras instituições sobre informações de incidentes deve ser planejada e aprovada, objetivando sempre a melhoria nos processos, o amadurecimento das equipes de resposta a incidentes, a redução de perdas ou dos custos e a agilidade na solução. O

Conglomerado entende que a troca de informações é importante, porém é necessária a observância de termos de confidencialidade e sigilo dos dados destas informações.

5.4. Área de Segurança da Informação

- Sugerir, definir, monitorar e garantir o cumprimento das Diretrizes, Normas e Procedimentos de segurança estabelecidas nesta Política e também nos respectivos procedimentos operacionais de TI, relacionados com as normas de segurança aqui estabelecidas;
- Garantir que os procedimentos de contingenciamento e continuidade dos negócios do Conglomerado estejam atualizados e testados conforme definido no PCN – Plano de Continuidade dos Negócios.

5.5. Área de Pessoas e Cultura

- Garantir que todos os colaboradores do Conglomerado tenham ciência das diretrizes de segurança da informação;
- Manter atualizados os termos assinados por todos os colaboradores, desde o momento de suas contratações. Tais termos devem estar anexos ao "Código de Conduta", que declara a ciência das informações contidas neste documento.
- Comunicar o desligamento de funcionários à área de Tecnologia da Informação, para que desabilite/remova todos os acessos do colaborador desligado.

5.6. Áreas de Negócios

- Manter termos e acordos (Anexos I e II) por escrito, que incluam o reconhecimento dos eventuais prestadores de serviços terceirizados, incluindo serviços de armazenamento, transmissão e processamento de dados, pela segurança dos dados dos usuários e clientes do Conglomerado.

5.7. Todos os Colaboradores

- Atender e disseminar todas as diretrizes e normas determinadas nesta Política e reportar situações que configurem descumprimento intencional ou não desta Política, assim como eventos de incidentes de segurança.

5.8. Parceiros e Prestadores de Serviços Terceirizados

- Atender e disseminar, para os seus colaboradores envolvidos na prestação de serviços contratados pelo Conglomerado, todas as diretrizes e normas determinadas nesta Política, bem como reportar

situações que configurem descumprimento intencional ou não desta política, assim como eventos de incidentes de segurança que envolvam o Conglomerado.

5.9. Compliance e Controles Internos

- Revisar esta política afim de garantir o cumprimento às normas regulatórias;
- Providenciar a formalização da aprovação deste documento;
- Manter a guarda deste documento atualizada.

6. DISPOSIÇÕES FINAIS

Em caso de dúvidas relacionadas ao tema relacionado neste documento, contactar a área de Governança de TI, através do e-mail: governança.ti@bancobari.com.br

7. VIGÊNCIA

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

8. 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 4.658/2018** do Conselho Monetário Nacional, de 26.04.2018 - 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.
- **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

9. CONTROLE DE ALTERAÇÕES

VERSÃO	MOTIVO	DATA
001	Criação do Documento	01.04.2019

10. APROVAÇÕES

ÁREA	NOME	CARGO
Conselho de Administração	Conselho de Administração	Conselho de Administração

11. ANEXOS

Anexo I – Termo de Ciência e Aceite quanto à Política de Segurança 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 CIBERNÉTICA

Por este instrumento, eu, _____, colaborador do Conglomerado Financeiro Bari, portador do RG nº _____, declaro que:

a) Tive acesso ao documento PSC – POLÍTICA DE SEGURANÇA 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 Conglomerado e demais empresas do Conglomerado Financeiro, 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 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 Conglomerado Financeiro Bari.

EU,_____,
RG_____,

ESTOU CIENTE DAS NORMAS DEFINIDAS NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, 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 Conglomerado;
- Se houver indícios de comprometimento da chave privada, avisar formal e imediatamente à Diretoria do Conglomerado.

_____ _____ / _____ /_____

Custodiante da Chave Privada Data