BANCO RNX

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Resolução BCB nº 4.893, de 26 de fevereiro de 2021.

Dezembro de 2025

SUMÁRIO

1. PROPÓSITO

O objetivo desta política é estabelecer regras e orientar quanto aos processos de Segurança da Informação do Banco RNX S.A. (denominado nesse documento como “instituição” ou “banco”), observando a resolução CMN nº 4.893/2021, a fim de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação, ambiente cibernético e o sigilo das informações, determinando os princípios, conceitos, valores e práticas que devem ser seguidos pelos administradores, funcionários e/ou outros colaboradores do banco na sua interação interna e com o mercado, abrangendo todos os ambientes, sistemas, processos e colaboradores.

O Banco incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus Colaboradores. Na constante busca do seu desenvolvimento e da satisfação dos clientes, o Banco busca transparência e cumprimento da legislação aplicável às atividades de banco múltiplo. A publicação desta Política representa o compromisso de todos os que trabalham no Banco com os valores e as práticas fundamentadas na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento do Banco e a defesa dos interesses dos clientes estarão sempre pautadas nas diretrizes aqui expostas. (Para atender ao §1º do art. 3º)

2. APLICAÇÃO

A presente política aplica-se a todos os processos, operações, sistemas, colaboradores, terceiros, parceiros e prestadores de serviços do Banco, independente do seu vínculo com a instituição, de forma a manter a segurança das informações.

3. DIRETRIZES

Os princípios básicos da segurança da informação são confidencialidade, integridade e disponibilidade das informações. Os benefícios são evidentes ao minimizar os riscos com divulgação indevida, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos:

- Confidencialidade: Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostos voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários;
- Integridade: Garantia da veracidade da informação, sendo que não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação; e
- Disponibilidade: Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das

funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

3.1. CONCEITOS E DEFINIÇÕES

Segurança Cibernética e da Informação: tem como objetivo a proteção dos ativos de informação, a redução dos riscos de acessos não autorizados ou uso indevido da rede e sistemas, redução dos riscos de fraude ou roubo, além da capacidade de identificar, proteger, detectar, responder e recuperar rapidamente de uma ameaça cibernética, a fim de proteger os ativos tecnológicos e informações.

Incidente Relevante: Eventos confirmados que impactaram de forma significativa a continuidade dos negócios (Alta, Média ou Baixa), selecionados após avaliação da Equipe de Avaliação a Incidentes (EAI).

Colaboradores: Pessoas contratadas para integrar o quadro do Banco, incluindo executivos, conselheiros, diretores, estagiários, aprendizes e prestadores de serviços.

Acesso controlado: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

4. OBJETIVOS DE SEGURANÇA CIBERNÉTICA

A instituição, através de sua política de segurança cibernética, tem por objetivos proteger sistemas, aplicações, computadores, dados sensíveis e ativos financeiros individuais e empresariais de ameaças provenientes de dentro ou de fora da instituição.

A instituição, a partir dos procedimentos e controles descritos no item 5 desta política declara, através de tais procedimentos a capacidade para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados a ambiente cibernéticos.

5. PROCEDIMENTOS E CONTROLES

O banco, a fim de atender os objetivos de segurança cibernética, adota procedimentos para reduzir a vulnerabilidade da instituição a incidentes, sendo os principais elencados a seguir.

5.1. AUTENTICAÇÃO

Em segurança da informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema, geralmente, quando ele requisita um login (acesso) em um programa ou computador. A autenticação normalmente depende de um ou mais "fatores de autenticação". A instituição utiliza mecanismos de autenticação baseada no conhecimento (com login e senha) em vários níveis, delimitando e controlando o acesso às informações. Todas as informações

armazenadas estão protegidas por sistemas que exigem a autenticação prévia para o acesso. Os acessos à arquivos na rede também exigem autenticação central. A instituição adota políticas para atualização periódica de senhas, bem como adota padrões de força para as senhas. As senhas são armazenadas de forma criptografada na base de dados. Os seguintes acessos exigem autenticação:

- Estação de trabalho.
- Sistema de e-mails;
- Consultas a base de dados (em todos os canais);
- Sistemas internos; e
- Acessos a pastas de rede.

5.2. CRIPTOGRAFIA

A criptografia é um conjunto de técnicas que transformam dados em códigos que só podem ser decifrados por quem tem a chave de acesso. Desta forma, a criptografia garante a proteção dessas informações e permite que apenas quem tem direito cedido de acesso (autenticação) consiga visualizar seu conteúdo. Sendo aplicada, pela instituição, para todas as senhas voltadas a banco de dados.

5.3. PREVENÇÃO E DETECÇÃO DE INTRUSÃO

Para prevenção e detecção de intrusão, o banco, conta com solução fornecida pelo software Acronis Cyber Protect, que possui proteção anti-malware completa e gestão abrangente de terminais, combate ataques cibernéticos avançados com tecnologias de proteção, analisando o tráfego da rede em busca de assinaturas que correspondam a ciberataques conhecidos. Dispõe também de solução fornecida pelo Firewall PfSense, com geolocalização ativada, que mitiga efeitos de ciberataques, originados em regiões distintos daqueles em que o banco efetivamente opera.

5.4. PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

A instituição utiliza o Firewall PfSense como medida de proteção a acesso não autorizado de informações, sendo que todos os dados e informações, estão em uma estrutura de pastas, com níveis de acesso, gerenciados pelo AD (Active Directory), o que limita e inibe acessos indevidos.

5.5. TESTES PARA DETECÇÃO DE VULNERABILIDADES

A instituição está em processo de desenvolvimento para aplicação de testes periódicos para detecção de vulnerabilidades.

5.6. PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

Esta instituição utiliza o software de segurança da ESET (Endpoint Security), onde a ferramenta de detecção e resposta permite o monitoramento abrangente, contínuo e em tempo real da atividade dos endpoints, bem como a análise de processos suspeitos para fornecer uma resposta imediata.

A instituição utiliza o Firewall PfSense como medida de proteção a acesso não autorizado de informações, no Firewall regras específicas são estabelecidas para permissão de acesso. Para maior segurança essas regras ficam em sigilo, delimitado ao responsável do setor de tecnologia. Ainda, todos os dados e informações, estão em uma estrutura de pastas, com níveis de acesso, gerenciados pelo AD (Active Directory), o que limita e inibe acessos indevidos.

5.7. GESTÃO DE CERTIFICADO DIGITAL

A Instituição adota procedimentos formais para a gestão do ciclo de vida dos certificados digitais utilizados em seus sistemas e comunicações, abrangendo emissão, armazenamento, utilização, renovação e controle de acesso, de forma a garantir a confidencialidade, integridade, autenticidade e não repúdio das informações.

Certificados utilizados no SPB (Sistema de Pagamentos Brasileiro):

Os certificados digitais utilizados para assinatura e autenticação das mensagens no âmbito do SPB não são compartilhados com o PSTI (Provedor de Serviços de Tecnologia da Informação), permanecendo exclusivamente sob posse e controle da Instituição.

A renovação desses certificados ocorre anualmente, mediante os procedimentos exigidos pela Autoridade Certificadora responsável. O SPB disponibiliza dois ambientes distintos – homologação e produção – e a Instituição utiliza certificados digitais distintos e independentes para cada um desses ambientes, assegurando segregação adequada entre testes e operação produtiva.

Certificado Digital A1 – CNPJ da Instituição:

A Instituição utiliza certificado digital do tipo A1 vinculado ao seu CNPJ, empregado em processos que exigem identificação institucional, assinatura digital e autenticação junto a órgãos e sistemas externos.

Esse certificado possui validade anual e sua renovação é acompanhada de forma proativa, com notificações automáticas da Autoridade Certificadora com antecedência mínima de 90, 60 e 30 dias do vencimento.

Existe controle interno por meio de planilha de gestão, na qual são registradas as datas de emissão, vencimento, instalação e os responsáveis ou sistemas que utilizam o certificado, assegurando rastreabilidade e mitigação de riscos de indisponibilidade.

Certificados de comunicação com a Núclea:

A Instituição também utiliza certificados digitais específicos para comunicação segura com a Núclea, empregados exclusivamente nos sistemas responsáveis pelo Cadastro Positivo e pelos processos de Portabilidade.

Esses certificados possuem validade anual e seguem o mesmo processo de renovação, com avisos prévios da Autoridade Certificadora e acompanhamento interno. A instalação e o uso são restritos

apenas aos servidores responsáveis pela comunicação com a Núclea, respeitando o princípio do menor privilégio e evitando uso indevido ou exposição desnecessária.

Controles e responsabilidades:

A gestão dos certificados digitais é de responsabilidade da área de Tecnologia da Informação, que assegura:

Que os certificados sejam utilizados apenas para as finalidades previstas;

Que o acesso seja restrito a sistemas e profissionais autorizados;

Que as renovações sejam realizadas dentro dos prazos estabelecidos;

Que haja controle documental e rastreabilidade dos certificados ativos.

5.8. MECANISMOS DE RASTREABILIDADE

Através da padronização de recebimento dos dados, a rastreabilidade das informações sensíveis é garantida através do acesso controlado dos usuários ao sistema de informação, sendo que as senhas ficam armazenadas de forma criptografada na base de dados. Através do controle de acesso individual, as consultas na base de dados permitem o registro e rastreio das informações.

5.9. CONTROLES DE ACESSO

A instituição utiliza mecanismos de controle de acesso por autenticação, permitindo que apenas usuários autorizados possam acessar as informações, de acordo com o nível de sigilo e acesso. O controle de acesso às informações/dados é gerenciado por um servidor de autenticação (AD - Active Directory). Em paralelo o banco, relativamente a seus principais sistemas, aplica critérios e procedimentos para criação de usuários e concessão de acessos, com a finalidade de monitoramento e controle quanto a disponibilização de dados e informações.

5.10. SEGMENTAÇÃO DA REDE DE COMPUTADORES

A segmentação de rede divide uma rede em seções menores (diretórios), às quais são aplicados controles e políticas de segurança diferentes. A instituição aplica este conceito especialmente quando a gestão do servidor de dados, onde são armazenados, principalmente, arquivos relativos a textos e planilhas de cálculos. Para efetivar a segurança dos dados e informações, a partição é efetuada por áreas e por permissões de acesso (leitura, gravação e exclusão).

5.11. MANUTENÇÃO DE CÓPIAS DE SEGURANÇA DOS DADOS E DAS INFORMAÇÕES

A instituição possui procedimentos de backups de todo banco de dados e servidores, efetuados diariamente. Com critérios de manutenção de cópias com diferente tempestividade, sendo que ao menos o backup do último dia de cada mês deve ser armazenado por não menos que cinco anos.

6. CONTROLES PARA GARANTIR A SEGURANÇA DE INFORMAÇÕES SENSÍVEIS

O banco, a fim de aprimorar sua postura em relação prevenção a acessos não autorizados às informações sensíveis dos clientes e usuários, adota as principais soluções de segurança de dados:

- Firewall - é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.;
- Backup e recuperação de dados - é o processo de fazer backup de seus dados para o caso de uma perda e configurar sistemas seguros que permitem que você recupere seus dados como resultado;
- Antivírus - software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e códigos, usados para proteção e prevenção, a fim de dar mais segurança ao usuário;
- Controle de acessos - é elemento essencial de segurança que determina quem tem permissão para acessar determinados dados, aplicativos e recursos e em que circunstâncias.;
- Auditoria - é o processo de analisar a área de forma minuciosa, buscando entender como são realizadas as tarefas a ela delegadas, neste caos em especial quanto aos procedimentos de segurança da informação da instituição;
- Criptografia de dados - é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados; e
- Segurança física - a segurança física tem como objetivo proteger as pessoas, bens e ativos físicos de qualquer ação ou evento que possa levar a perda ou danos.

7. REGISTRO, ANÁLISE E CONTROLE SOBRE INCIDENTES RELEVANTES

Para que seja possível a melhoria contínua dos procedimentos relacionados à segurança cibernética, permitindo que sejam realizadas as adequações necessárias à correção de vulnerabilidades nas medidas e procedimentos relativos à segurança cibernética, deve ser realizado o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, abrangendo, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros, sendo elaborado relatório próprio pela área responsável.

7.1. PREMISSAS BÁSICAS

A Instituição deve garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, até o retorno à situação de normalidade no funcionamento das operações dentro do contexto dos seus negócios, para tanto são observadas as seguintes premissas:

- Foram elaborados cenários de incidentes, considerados nos testes de continuidade de negócios, baseado em interrupções de energia; indisponibilidade de rede/circuitos; falha de climatização do ambiente; falha humana; incêndio; desastres naturais; falha de hardware/software e ataques cibernéticos;
- Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços, considerando as características dos serviços prestados, níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados;
- Para a classificação dos dados e das informações quanto a relevância, deve ser observada a seguinte classificação, de acordo com o disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD):

  - Dados públicos: podem ser acessados por qualquer pessoa;
  - Dados internos: podem ser acessados apenas por colaboradores da empresa;
  - Dados confidenciais: podem ser acessados apenas por um grupo de pessoas ou cargos específicos; e
  - Dados restritos: podem ser acessados apenas por algumas pessoas.

- Para efeito de avaliação da relevância de incidentes, com base no impacto nos negócios e em sua urgência, a instituição definiu a severidade dos incidentes em três níveis:

  - Alta - Paralisação da instituição, paralisação de um ou mais departamentos e paralisação de atividades de um ou mais funcionários;
  - Média - Lentidão de sistemas e processos; e
  - Baixa - Demandas que não envolvem interrupção ou lentidão na execução das atividades ou processos.

8.DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

A instituição, através da divulgação tempestiva, disponibiliza material a seus colaboradores com o intuito de reforçar a Cultura de Segurança Cibernética, assim como, alertar quanto a precauções e cuidados na gestão e tratamento de dados.

O banco disponibiliza informações em seu site sobre precauções a serem tomadas em relação a contratação de produtos e serviços financeiros, como, contatos comerciais confiáveis e alertas sobre envio de recursos financeiros a instituição, além de utilização de cookies e direcionamento à política de privacidade e proteção de dados.

Como uma de suas responsabilidades, a diretoria da instituição apoia ações relativas à conscientização, em sua estrutura funcional e propor ações de forma a demonstrar aos colaboradores o compromisso necessário para atingir os objetivos relacionados com a segurança cibernética, sempre mantendo a instituição em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com

o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético

9.COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

A troca de informações entre pares de mercado, via grupos de compartilhamento, é umas das iniciativas de destaque no enfrentamento de ameaças cibernéticas – e requisito regulatório disposto às instituições financeiras pela Resolução 4.893 do CMN. A prática envolve basicamente duas questões: (a) onde compartilhar; e (b) o que compartilhar. A primeira trata das plataformas de compartilhamento e a segunda, que é abordada de maneira principiológica neste documento, diz respeito ao conteúdo das informações.

a) Onde compartilhar

O compartilhamento de informações acerca das ameaças cibernéticas entre pares do mercado pode ser realizado via plataformas de compartilhamento especializadas. Esses locais podem contar com requisitos mínimos de segurança que auxiliam a formação da comunidade e a construção da confiança necessária para a sustentação da prática de compartilhamento de dados entres as instituições. Como exemplos de plataformas de compartilhamento, é possível citar MISP, FS-ISAC, entre outros.

b) O que compartilhar

A padronização de informações é apontada como boa prática para a ampliação e o fortalecimento das atividades de compartilhamento. Um conjunto de atributos mínimos a serem compartilhados de acordo com o tipo/classificação do incidente cibernético. Além de promover a estruturação e aumentar a agilidade no compartilhamento. Assim, tomamos como exemplo o rol de atributos elencados pela ANBIMA, como referência para o desenvolvimento pelo Banco de modelo de compartilhamento.

PHISHING	
DEFINIÇÃO	ATRÍBUTOS MÍNIMOS
Links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais.	• Data da ocorrência • Data e hora da identificação • Status da análise • Segmento da entidade • Atributos (ex.: URL, remetente)

RANSOMWARE	
DEFINIÇÃO	ATRÍBUTOS MÍNIMOS
Software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.	• Data da ocorrência • Data e hora da identificação • Status da análise • Segmento da entidade • Atributos (ex.: IP, remetente)

DDoS	
DEFINIÇÃO	ATRÍBUTOS MÍNIMOS
Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.	• Data da ocorrência • Data e hora da identificação • Status da análise • Segmento da entidade • Atributos (ex.: URL)

Neste item cabe esclarecer que a instituição está em processo de análise para futuro desenvolvimento de solução para compartilhamento, salientando que em virtude do volume e complexidade das suas operações, não é alvo de eventos de ciberataques, mas que procura estar preparada e monitorando constantemente seus ambientes a fim de evitar quaisquer incidentes relevantes.

10. DIVULGAÇÃO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética e da Informação e as demais políticas e normas complementares da instituição aqui referenciadas devem ser divulgadas ao Público-Alvo, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, devendo estar disponíveis em local acessível aos colaboradores e protegidas contra alterações. Além disso, é divulgado ao público, na página da instituição na internet, resumo contendo as linhas gerais da política de segurança cibernética.

11. DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A Instituição elabora relatório anual sobre a implementação do plano de ação e de resposta a incidentes, tendo como data-base o dia 31 de dezembro de cada ano. O relatório deverá ser submetido à diretoria até 31 de março do ano seguinte ao da data-base, devendo abordar:

- A efetividade da implementação das ações desenvolvidas pela Instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

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

Destacando que a instituição contratante destes serviços é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor, sendo responsável pela comunicação ao BCB até 10 dias após a contratação dos serviços, de no mínimo:

I - A denominação da empresa contratada;

II - Os serviços relevantes contratados; e

III - A indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, definida nos termos do inciso III do art. 16, no caso de contratação no exterior.

Além disso, para contratação de serviços de processamento ou armazenamento em nuvem, deve observar os preceitos de funcionamento e operacionalidade conforme descritos abaixo:

- A terceirizada contratada deverá garantir o correto funcionamento técnico dos módulos licenciados dos sistemas, mantendo todas suas funções em plena operacionalidade e provendo as soluções aos eventuais problemas técnicos registrados pela instituição;
- A contratada irá implementar e manter controles de segurança incluindo, sem limitação, segurança de hardware e software, firewall, filtros e outras ferramentas de segurança;
- A contratada deverá armazenar e transmitir as credenciais de acesso e demais informações confidenciais de maneira criptografada;
- Será garantida a segregação de acesso entre os ambientes de diferentes clientes, impedindo o acesso não autorizado às informações da instituição, bem como que os acessos sigam a diretriz do privilégio mínimo, onde os acessos aos ambientes devem ser concedidos baseando-se somente na real necessidade;
- Será disponibilizada informações para auditorias (internas e externas) e investigações judiciais quando solicitadas. Caso sejam encontradas desconformidades, a responsável deverá prover um plano de ação para correção;
- A contratada disponibilizará para a instituição, informações quanto aos procedimentos e controles utilizados na prestação de serviços, assegurando o acesso a informações e recursos de gestão adequados ao monitoramento dos serviços;

- No caso de eventuais desastres, deverão ser seguidos os procedimentos preconizados pela própria fornecedora de ambiente em nuvem, em seu processo interno;
- A contratada deverá manter completo sigilo e confidencialidade sobre os dados pessoais e informações que tiver acesso, bem como não divulgá-los;
- Todos os implementos necessários para a adequação à legislação exclusivamente federal nos módulos licenciados do sistema deverão ser efetuados, tempestivamente;
- O suporte técnico deverá ser realizado pela contratada, solucionando ou oferecendo previsão para solução de problemas quanto ao bom funcionamento dos serviços;
- As interrupções necessárias para ajustes técnicos ou manutenção do sistema, deverão ser comunicadas à instituição, com 2 (dois) dias úteis de antecedência;
- Caso haja urgência que coloquem em risco o regular funcionamento do servidor e aqueles determinados por motivo de segurança decorrente de vulnerabilidades detectadas, as interrupções serão imediatas e sem prévio aviso;
- Caso a interrupção interfira ou cause prejuízo à operacionalidade do ambiente em nuvem, onde hospedado o sistema, e seja necessária para a manutenção dos serviços, a mesma será realizada, sempre que possível, entre as 21h e 6h ou nos finais de semana;
- A interrupção para a manutenção na prestação de serviços acessórios, que não impliquem em prejuízo para a operacionalidade do servidor, perdurará pelo tempo necessário à supressão das irregularidades detectadas;

Sempre que houver a necessidade de subcontratar serviços relevantes a empresa contratada deverá notificar, de imediato, a instituição.

13. NORMAS PARA GESTÃO DE SENHAS (Política de Gestão de Senha)

A identificação do usuário e sua respectiva senha são individuais e intransferíveis. O usuário é responsável pela confidencialidade de sua senha e não deve revelá-la em circunstância alguma. O compartilhamento de senhas entre usuários constitui falta grave, podendo sujeitar os colaboradores às sanções dispostas no Código de Conduta Ética da instituição.

As senhas devem ser renovadas trimestralmente pelos colaboradores ou serão bloqueadas.

As senhas terão validade de 120 dias, os colaboradores serão comunicados, pelos sistemas, sobre a necessidade de troca de senha, com 30 dias de antecedência.

Com o objetivo de evitar o uso de senhas fracas, está implementado uma regra de complexidade de senhas. Dessa forma, ao criar ou alterar uma senha, os seguintes requisitos devem ser atendidos:

- A senha não pode conter palavras que façam parte do login do usuário nem de seu nome;
- A senha não deverá ser igual a uma das últimas duas senhas utilizadas;
- A senha deve ter pelo menos seis caracteres;
- A senha deve conter ao menos uma letra maiúscula;
- A senha deve conter ao menos uma letra minúscula;
- A senha deve conter ao menos um número; e

- A senha deve conter ao menos um símbolo ou caractere especial, como: ~!@#$%^&*-+='|\(){}[]:;'"<>,?/.

14. GESTÃO DE MUDANÇAS (Política de Gestão de Mudanças)

A área de Infraestrutura de TI é responsável por participar, documentar, homologar e implementar toda e qualquer alteração seja de hardware e software ou que tenha impacto direto na infraestrutura de negócio ou operacional do Banco.

O processo de gestão de mudança tem como objetivo geral gerenciar grandes alterações/adequações, relacionadas a introdução de novos sistemas e/ou mudanças que possam causar impacto na área de TI em entregar serviços, através de um processo para assegurar que os recursos permaneçam alinhados aos requisitos do negócio com o menor risco possível.

Consideramos como grandes alterações/adequações atividades que possam impactar na continuidade de negócios.

Descrevemos abaixo modelo próprio para implementação de mudanças:

- Preparação: É a fase em que se identifica uma oportunidade ou necessidade de mudança, sendo responsável o gestor da área que demanda a mudança;
- Aprovação: Quando é levado o plano para aprovação das áreas envolvidas e diretoria responsável;
- Programação: Idealização de toda a gestão da mudança, verificando quais serão as alterações necessárias, os principais envolvidos, para, então, gerar um planejamento entre a área demandante e o fornecedor;
- Formalização para área de TI: Abertura de chamado junto ao suporte, para acompanhamento da programação e posterior execução do projeto, assim como a sustentação após implantação;
- Execução: Quando o plano é posto em prática e acompanhado até sua implantação (homologação e produção);
- Sustentação: Após finalizar o processo de implantação, é preciso manter um controle acerca das mudanças para garantir a adaptação de todos os envolvidos;

Nesse sentido, este processo tem os seguintes objetivos específicos:

- Assegurar a conformidade com os requisitos estatutários, regulamentares e contratuais; e
- Garantir que as mudanças sejam registradas e avaliadas e que as mudanças autorizadas sejam priorizadas, planejadas, testadas, implementadas, documentadas e revisadas de maneira controlada, observando a integração com os demais sistemas e/ou processos, com o mínimo de impacto nos negócios da instituição.

A partir do processo de gestão de mudanças, espera-se obter os seguintes benefícios:

- Redução de incidentes e indisponibilidades relacionados com mudanças nos serviços de TI;
- Atendimento eficiente das necessidades de mudanças dos usuários;
- Planejamento adequado das mudanças, reduzindo seus custos, riscos e impactos;
- Redução do trabalho de manutenção e documentação de todos os processos de gerenciamento;

- Maior visibilidade, alinhamento e comunicação de alterações, tanto de negócio quanto de TI; e
- Aumentar a capacidade de absorver grandes mudanças.

Todo processo de mudanças deve ter seu início via solicitações, que devem ser encaminhadas do gestor responsável pela solicitação para área de infraestrutura de TI, e tais demandas devem ser registradas em sistema para acompanhamento histórico.

15. REVISÕES DE ACESSOS

A área de Riscos/Controles Internos e Infraestrutura de Tecnologia da Informação são responsáveis por liderar anualmente os processos de revisões de acessos físicos ou lógicos de todos os colaboradores do Banco e propor a alteração e sua respectiva implementação.

16. REGULAMENTO DE USO DA INFORMÁTICA E REDE

O Banco regulamenta os procedimentos e normas para utilização dos recursos de informática e segurança de informações através do “Regulamento de Uso de Informática e Rede do Banco RNX S/A” que é divulgado e formalizado no momento da contratação de cada colaborador, sendo que um termo de compromisso deverá ser assinado e arquivado na pasta funcional sob os cuidados da área de Recursos Humanos da empresa. Da mesma forma, quando da contratação de terceiros que terão acesso à rede de dados e sistemas do banco, o mesmo termo deverá ser formalizado e arquivado na pasta do fornecedor. A íntegra do regulamento, contendo o termo de compromisso, está disponível na rede interna BC-PDADOS/MANUAL_BM.

17. VIOLAÇÃO E SANÇÕES

Todos os colaboradores, terceiros e prestadores de serviço devem estar cientes de que o não cumprimento das diretrizes desta política implicará em sanções, sejam internas, administrativas, legais e/ou penais, dependendo do grau da infração. Para terceiros e prestadores de serviços, inclui-se a rescisão de contratos e penas de responsabilidade civil e criminal na extensão que a lei permitir. Além disso, cabe observar o disposto no Código de Conduta Ética da instituição, em especial quanto às medidas disciplinares nele disposto. Ao detectar uma violação, o usuário deve comunicar aos responsáveis pela Segurança da Informação imediatamente. Caso seja verificado que o colaborador não comunicou a infração, mesmo sabendo da sua existência, o mesmo pode ser considerado coautor da mesma e assim ser indiciado e sofrer sanções.