Política de Segurança Cibernética e da Informação

1. PROPÓSITO

O objetivo desta política é estabelecer regras e orientar quanto aos processos de Segurança da Informação do Banco RNX S.A., observando a resolução CMN nº 4.658/2018, a fim de garantir a segurança e sigilo das informações, determinar os princípios, conceitos, valores e práticas que devem ser seguidos pelos administradores, funcionários e / ou outros colaboradores do Banco RNX S/A (Banco) na sua interação interna e com o Mercado, abrangendo todos os ambientes, sistemas, processos e colaboradores.

2. APLICAÇÃO

A presente política aplica-se a todos os processos, operações, sistemas, funcionários, terceiros e prestadores de serviços do Banco, de forma a manter a segurança das informações.

3. POLÍTICA

A Política de Segurança Cibernética e da Informação, tratada neste documento, tem como objetivo estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos relacionados as informações acessadas pelos administradores, funcionários e/ou outros colaboradores do Banco na sua atuação interna e com o mercado. 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.

3.1 CONCEITOS E PRINCÍPIOS

O Banco define Segurança Cibernética e da Informação como a proteção contra o uso ou acesso não – autorizado à informação, preservando sua integridade e a confidencialidade.

Atualmente, o conceito de Segurança Cibernética e da Informação refere-se à proteção existente sobre as informações de uma determinada instituição financeira, empresa ou pessoa, e aplica-se tanto a informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Os princípios da segurança da informação nos dão subsídios para proteger as informações do Banco. Portanto, quando mencionamos "segurança da informação" estamos nos referindo sobre proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa.

Os princípios básicos da segurança da informação são confidencialidade, integridade e disponibilidade das informações, além de características como irrefutabilidade, autenticação e o controle de acesso. 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 expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários;

− Integridade: Garantia da veracidade da informação, pois a mesma 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;

− 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; e

− 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.

3.2. DIRETRIZES

Toda informação ou sistema de informação possui um determinado valor, sendo assim, pode ser considerado como um ativo do Banco, devendo ser protegido de forma adequada.

O Sistema de Segurança da Informação visa assegurar a:

- Confidencialidade: Garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados;

- Integridade: Garantir que todas as informações estejam íntegras e precisas durante todo o ciclo (criação, processamento, destruição);

- Disponibilidade: Garantir que os usuários, quando devidamente autorizados, tenham acesso às informações sempre que necessitarem.

O Banco não autoriza cópia das informações para uso pessoal ou de terceiros, ou envio por correio eletrônico para que sejam utilizadas para qualquer fim que não seja de interesse da empresa, bem como não tenha sido autorizado formalmente pela instituição.
Também não é permitida alteração ou exclusão de dados ou informações dos sistemas operacionais da empresa, banco de dados ou de qualquer outro dado de propriedade do Banco, que venha prejudicar a empresa, ou para benefício do próprio usuário, sendo tal procedimento caracterizado como falta grave sujeita a sanções legais.

3.3. CONTROLE DAS INFORMAÇÕES

O acesso aos recursos de informática da rede são disponibilizados aos usuários devidamente cadastrados no Sistema de Controle Administrativo e que tenham assinado o termo de Compromisso anexo I do Regulamento de Uso da Informática e Rede do Banco.
O Administrador da rede deverá proporcionar o acesso aos sistemas de rede mediante senha pessoal e intransferível, sendo o usuário responsável pela utilização e guarda desta informação.

3.4. 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 do grupo sendo que um termo de compromisso é assinado e arquivado na pasta funcional sob os cuidados da área de Recursos Humanos da empresa.
A íntegra do regulamento, assim como do termo de compromisso fazem parte do anexo desta política.

3.5. LINHAS GERAIS DE COMPORTAMENTO

O controle de acesso é parte central da segurança de uma empresa do ponto de vista da segurança da informação. Por isso, é fundamental que ao entrar nas dependências do Banco passe a portar seu crachá. No ambiente externo, é melhor ficar atento, falar sobre informações restritas ou segredos profissionais em um lugar público ou por telefone merecem cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa. Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa da empresa. Qualquer pen-drive ou conexão de rede pode conter dados valiosos. Cuidado com o lixo que você produz. O lixo pode ser uma fonte de informações para pessoas mal-intencionadas. Destrua os documentos que

contenham informações sensíveis, pessoais ou do Banco antes de descartá-los. Se o papel que vai ser jogado no lixo contém informações que não devem ser lidas por estranhos, rasgue-o antes de jogá-lo fora. Cuidados com senhas e acessos no sistema cada tarefa desenvolvida no Banco precisa ter um responsável. A única forma de saber o responsável por cada atividade é através da identificação do usuário. Tudo que é feito com a sua identificação (assinatura ou senha) é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está usando esse acesso. Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua.

Alguns exemplos de ações que podem ser atribuídas a você, são:

▪ Liberação de ações indevidas;

▪ E-mails com informações inadequadas;

▪ Acesso a páginas da internet proibidas;

COMPARTILHAR SUA SENHA É COMO ASSINAR UM CHEQUE EM BRANCO!

Adote um comportamento seguro

▪ Não compartilhe nem divulgue sua senha a terceiros;

▪ Não transporte informações confidenciais do Banco em qualquer meio (CD, DVD, pendrive, papel, etc.) sem as devidas autorizações e proteções;

▪ Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);

▪ Não abra mensagens de origem desconhecida;

▪ Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contêm informações confidenciais; e

▪ Siga corretamente a política para uso de internet e correio eletrônico estabelecida pelo Banco.

3.6. GESTÃO DE MUDANÇAS

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

3.7. Revisões de acessos

A área de Riscos/Controles Internos e Infraestrutura de TI 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.

3.8. Duvidas

Quaisquer dúvidas relacionadas com a presente política devem ser esclarecidas com a Diretoria do Banco ou com a área de Risco e Controles Internos.

4. ANEXOS

- Regulamento de uso de Informática e Rede do Banco RNX S/A;
- Termo de Compromisso.

5. ELABORAÇÃO

Tiago Alexandre Santos Ribeiro Área de Tecnologia da Informação (MR Informática)	**Assinatura**

6. APROVAÇÃO

João Mauricio Archer Wanderley Diretor	**Assinatura**

Luiz Albari Veiga Aschembrener Diretor	**Assinatura**

Marcelo Renaux Diretor	**Assinatura**

REGULAMENTO DE USO DA INFORMÁTICA E REDE DO BANCO

O presente regulamento tem por objetivo estabelecer normas e procedimentos para utilização dos recursos de computação e rede do Banco RNX S/A (Banco). Sua aplicação se destina a todos os usuários do sistema de informática, funcionários e/ou colaboradores, conforme segue:

1. Regras do Uso de Tecnologia

Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções no Banco ou para outras situações formalmente permitidas, observando os ditames abaixo:

a) Quando o usuário se comunicar através de recursos de tecnologia do Banco, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa;
b) Os conteúdos acessados e transmitidos através dos recursos de tecnologia do Banco devem ser legais, de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário;
c) O uso dos recursos de tecnologia do Banco pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente;
d) Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados;
e) Os recursos de tecnologia do Banco, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização; e
f) Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de **Riscos e Controles Internos**.

2. Regras do Uso do Computador

A fim de atender o bom uso dos recursos de tecnologia as regras abaixo devem ser observadas:

a) Propriedade do computador:

− O recurso computador disponibilizado para o usuário é de propriedade do Banco.

b) Disponibilização e uso:

− O recurso computador disponibilizado para o usuário pelo Banco tem por objetivo o desempenho das atividades profissionais desse usuário na organização;
− Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área de infraestrutura para uso no Banco;
– O Banco pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário;
− Cada computador tem o seu gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área de infraestrutura;
− A identificação do usuário ao computador é feita através do login e senha disponibilizado pela área de Infraestrutura, portanto ela é sua assinatura eletrônica;
− Será apenas permitido senha forte com 4 a 8 caracteres alfanuméricos, maiúsculos e minúsculos.
− É permitido apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso;
− A senha possui validade de 90 dias e sua troca será solicitada automaticamente quando da sua expiração;

c) Programas utilizados no computador

− Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura;
− É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura; e
− É desabilitado ao usuário implantar ou alterar componentes físicos no computador.

d) Verificação do computador e acessos

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

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

e) Responsabilidades do usuário
− Cuidar adequadamente do equipamento. O usuário é o custodiante deste recurso.
− Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de infraestrutura.

f) Outras proteções
− É implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);
− É implantado o "log-off" automático por inatividade durante o período de 24 horas;
− É implantado o bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;
− É implantado o bloqueio do acesso à sites de armazenamento de dados em nuvem (cloud); e
− É implantado o bloqueio de sistemas de gerenciamento de computador a distância.

3. Regras do uso da Internet
a) Responsabilidade e forma de uso
− O usuário é responsável por todo acesso realizado com a sua autenticação;
− O usuário é proibido de acessar endereços de internet (sites) que:
▪ Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes;
▪ Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
▪ Contenham informações que não colaborem para o alcance dos objetivos do Banco;
▪ Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
− O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.
b) Uso de serviço de mensagem instantânea.
− É proibido o uso de serviços de mensagem instantânea (MSN, etc), através dos computadores do Banco, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pelo Compliance.
c) Uso de serviço de rádio, TV, download de vídeos, filmes e músicas.
− É proibido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores do Banco, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pela área de infraestrutura.
d) Bloqueio de endereços de Internet
− Periodicamente a área de infraestrutura revisará e bloqueará o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Empresa.
e) Uso de Correio Eletrônico particular tipo Webmail
- É proibido o acesso aos serviços de correio eletrônico particular, tipo Webmail, através dos recursos de tecnologia do Banco.

4. Regras do Uso do Correio Eletrônico (E-mail)
a) Endereço eletrônico do usuário
– O Banco disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@bancoRNX.com.br);
− O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à empresa;
− O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com o Banco; e
− Se houver necessidade de troca de endereço, a alteração deverá ser autorizada pela área de infraestrutura e registrada para possibilitar uma posterior verificação de autoria.
b) Criação, manutenção e exclusão do endereço de correio eletrônico
− A utilização desse endereço de correio eletrônico pelo usuário necessita ser autorizada pelo seu Gestor;
− A liberação do endereço de correio eletrônico será feita pela área de infraestrutura de maneira controlada e segura com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço;
− Quando acontecer desligamento de usuário, o Gestor deve comunicar à área de infraestrutura o nome e a identificação desse usuário; e

− As caixas postais de contas de correio eletrônico do Banco tem limite de tamanho de 3.2GB e as mensagens enviadas/recebidas poderão conter arquivos anexos com até 4MB por mensagem.
c) Endereço eletrônico de programas ou de comunicação corporativa
− É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da área de infraestrutura responsável por acompanhar as mensagens emitidas e recebidas por esse endereço; e
− É permitido a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna do Banco, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.
d) Propriedades do endereço
− O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade do Banco; e
− Em situações autorizadas pela Diretoria, as mensagens do correio eletrônico de um usuário poderão ser acessadas pelo Banco ou por pessoas/entidades por ela indicada. Não deve ser mantida portando, expectativa de privacidade pessoal.

e) Responsabilidades e forma de uso
O usuário que utiliza um endereço de correio eletrônico:
− É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.
− Pode enviar mensagens necessárias para o seu desempenho profissional na Empresa.
− É proibido criar, copiar ou encaminhar mensagens ou imagens que:
▪ Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.
▪ Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais.
▪ Repassem propagandas ou mensagens de alerta sobre qualquer assunto.

Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Controles Internos, que definirá a sua publicação ou não.

− É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.
− Deve estar ciente que uma mensagem de correio eletrônico do Banco é um instrumento formal e, portanto, possui as mesmas responsabilidades de um instrumento convencional em papel timbrado da entidade.
− Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome do Banco.
− Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.
− Deve ser diligente em relação:
▪ Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
▪ Ao nível de sigilo da informação contida na mensagem;
▪ Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
▪ Ao uso da opção Encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.
− Deve deixar mensagem de ausência quando for passar um período maior do que 48 horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

g) Cópias de segurança
Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:
− A cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de infraestrutura.
− A área de infraestrutura fornecerá o serviço de recuperação de mensagens de correio eletrônico, a partir de arquivos de cópia de segurança, cumprindo parâmetros de nível de serviço previamente estabelecido.

5. Regras do Uso de Telefone
a) Número do telefone do usuário
– O Banco disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais.
− Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela área de infraestrutura e registrada para possibilitar uma posterior verificação de autoria.

b) Propriedades do número do telefone
− O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade do Banco; e
− Todos os telefones são gravados e monitorados regularmente, e em situações especiais autorizadas pelo Comitê Gestor, as conversas de um usuário poderão ser acessadas pelo Banco ou por pessoas/entidades por ela indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal.

c) Responsabilidades e forma de uso - O usuário que utiliza um telefone:
− É responsável por todo conteúdo da conversa;
− Pode utilizar o telefone para o seu desempenho profissional na empresa;
− É proibido utilizar o telefone para conversas que:
▪ Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.
▪ Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física.
▪ Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional.
▪ Defendam ou possibilitem a realização de atividades ilegais.
▪ Possam prejudicar a imagem do Banco.
▪ Sejam incoerentes com o nosso Código de Ética.

d) Cópias de segurança - Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:
− A cópia de segurança dos telefonemas é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de infraestrutura; e
− A área de infraestrutura apenas fornecerá a recuperação de telefonemas, a partir de arquivos de cópia de segurança, em situações autorizadas pelo Comitê Gestor.

Anexo I - TERMO DE COMPROMISSO

Este termo se aplica ao credenciamento do usuário de rede do Banco.

Declaro ser conhecedor(a) dos procedimentos para utilização dos recursos de computação e da rede do Banco especialmente as relativas à utilização de computadores e redes, assim como os princípios, conceitos, valores e práticas que devem ser adotados, em relação a segurança cibernética e da informação", na utilização dos recursos relacionados as informações acessadas pelos administradores, funcionários e/ou outros colaboradores do Banco na sua atuação interna e com o mercado.

Declaro também estar ciente dos princípios da segurança da informação que dão subsídios para proteger as informações do Banco. Portanto, quando mencionamos "segurança cibernética e da informação" estamos nos referindo sobre proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa.

Bem como declaro ter recebido uma via deste Regulamento, declaro também ser responsável pela conta (usuário de rede) _____, e pela conta(s) de e-mail(s)_____ _____comprometendo-me a:

- Cumprir as orientações e procedimentos contidos nas normas em vigor;

- Assumir as responsabilidades administrativas, cíveis e penais decorrentes do desvio no uso e finalidade da rede do Banco;

- Acatar as orientações e procedimentos normativos, assim como comunicar meu desligamento do Banco sob qualquer motivo, para a regularização da conta acima referida.

Por ser verdade, firmo a presente.

Nome completo: _____

Ciente:

Assinatura: _____

Local/Cidade_____ Data: _____/_____/_____