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 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 desta política e estão disponíveis na sede do Banco.

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 as áreas de Infraestrutura de TI ou Riscos e Controles Internos.

Banco RNX S/A
Diretoria