Tipo de documento:	**NORMA**		
Título do Documento:	**Segurança de Terceiros**		
Área Responsável:	**IT OPERATIONS AND SECURITY**	Classificação da Informação:	**PÚBLICO**

Índice

1. Introdução e Objetivos

O objetivo deste documento é estabelecer diretrizes e requisitos mínimos de Segurança da Informação e Privacidade para os terceiros que têm acesso aos dados e informações do EBANX.

2. Escopo e Usuários

Este documento aplica-se a todos os terceiros com potencial de acessar e afetar a confidencialidade, integridade, privacidade ou disponibilidade das informações e ativos do EBANX.

3. Termos e Definições

Ameaça: É a possibilidade de um evento indesejável, interno ou externo, explorar acidentalmente ou propositalmente as fraquezas de segurança da empresa, e potencialmente remover, desabilitar ou destruir os ativos de informação (recursos), resultando em um impacto danoso para o EBANX.

Ativo de Informação: É qualquer componente (seja humano, tecnológico, software, documento, sistema ou equipamento, etc.) que sustenta informações de um ou mais processos de negócio essenciais para as operações do EBANX.

Autenticidade: Princípio que garante a veracidade e a origem de uma informação ou da identidade de uma entidade (usuário, sistema, processo).

Confidencialidade: Proteção de informações confidenciais para que não sejam divulgadas a indivíduos, entidades ou processos não autorizados.

Disponibilidade: Garantia de que a informação e os recursos associados estão disponíveis e acessíveis quando necessário pelos usuários autorizados.

ebanker: Termo utilizado para se referir aos funcionários, funcionários temporários, sócios, estagiários e menores aprendizes do EBANX.

EBANX: Todas as empresas do grupo econômico do EBANX, incluindo o EBANX Instituição de Pagamento Ltda. (EBANX IP).

Incidente de Segurança da Informação e Incidente de Privacidade: Violação de confidencialidade, integridade ou disponibilidade de informações institucionais de forma material ou relatável, seja causado por ação não autorizada ou acidental. No caso de Incidentes de Privacidade, representa também tratamento inadequado ou ilícito de Dados Pessoais.

Integridade: Proteção da precisão e completude dos dados e informações. Em um contexto de segurança da informação, significa garantir que os dados não sejam corrompidos, alterados ou destruídos de maneira não autorizada.

Não repúdio: Garantia em segurança da informação de que a origem de uma ação ou a integridade de uma informação não pode ser negada posteriormente por nenhuma das partes. Ele estabelece uma prova irrefutável do evento, geralmente por meio de assinaturas digitais e logs.

NDA (Acordo de Não Divulgação): Um contrato legal que estabelece um relacionamento de confidencialidade entre partes, proibindo a divulgação de informações sensíveis a terceiros não autorizados. Seu objetivo principal é proteger segredos comerciais e dados confidenciais.

Risco: Risco é a expectativa de perda expressada como a probabilidade de que uma ameaça possa explorar o ativo de informação em particular, com um resultado danoso para a organização.

Sistema de Gestão de Segurança da Informação e Privacidade – SGSIP: Metodologia baseada nas normas ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 27002 que tem como propósito estabelecer um processo de gestão e melhoria contínua de Segurança da Informação e Privacidade.

Vulnerabilidade: Fraqueza de um ativo ou controle que pode ser explorada e então pode ocorrer um evento com uma consequência negativa.

4. Diretrizes

Todos os terceiros que têm acesso às informações ou aos sistemas de informação do EBANX devem cumprir as políticas de Segurança da Informação e Governança de Privacidade e Proteção de Dados Pessoais do EBANX, bem como a documentação associada, quando apropriado.

Os terceiros devem proteger as informações do EBANX contra qualquer acesso não autorizado, modificação, destruição ou disseminação, assegurando que os recursos tecnológicos postos à sua disposição pelo EBANX, sejam utilizados somente para os fins informados e aprovados. Em qualquer operação que demande acesso às informações do EBANX, o terceiro deve estar em conformidade com os princípios de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

Em casos de dúvidas relacionadas à Segurança da Informação e Privacidade e Proteção de Dados Pessoais, os terceiros devem buscar orientação de seus superiores ou do time de Information Security e Privacy do EBANX. Está disponibilizado publicamente o Aviso de Privacidade e Proteção de Dados Pessoais no site, além de outros documentos, que orientam o manuseio seguro das informações e práticas aceitas e esperadas pelo EBANX.

4.1 Privacidade e Proteção de Dados Pessoais

As leis e regulamentações de privacidade e proteção de dados pessoais estabelecem requisitos e obrigações para atividades de tratamento de dados. Muitos desses requisitos e obrigações, visam diminuir o risco de vazamento ou falhas internas que possam causar danos aos titulares de dados. Há diversas medidas que podem ser adotadas pelos agentes de tratamento para demonstrar que as atividades são realizadas considerando as melhores práticas e com foco na proteção do titular.

O EBANX respeita os direitos de qualquer titular de dados e também cumpre as leis e regulamentos aplicáveis, como a LGPD no Brasil. Para mais detalhes, o Aviso de Privacidade, disponível no site, explica os princípios relevantes e como realizamos a coleta de dados pessoais e demais tipos de tratamentos de dados pessoais.

Os dados do EBANX, processados por terceiros, devem ser tratados de acordo com os regulamentos de proteção de dados vigentes e as práticas aceitas pelo EBANX.

4.2 Classificação da Informação

O EBANX estabeleceu quatro níveis de classificação da informação: Pública, Uso Interno, Restrito e Confidencial. As informações de propriedade ou tratadas pelo EBANX devem ser classificadas e manuseadas de acordo com os níveis de sigilo estabelecidos na norma *"Classificação da Informação*".

Nível de Confidencialidade	Marcação	Critérios de classificação	Restrição de acesso
Pública	PÚBLICO	As informações públicas não devem prejudicar a organização de forma alguma e nem violar quaisquer leis ou regulamentos aplicáveis, como regras de privacidade.	A informação está disponível ao público.
Uso interno	USO INTERNO	O acesso não autorizado às informações pode causar danos menores e/ou inconvenientes para a organização.	As informações estão disponíveis para todos os funcionários e terceiros autorizados sob NDAs ou contrato contendo cláusulas específicas a respeito da confidencialidade das informações.
Restrito	RESTRITO	O acesso não autorizado às informações pode prejudicar consideravelmente os negócios e/ou a reputação da organização.	As informações estão disponíveis apenas para um grupo específico de funcionários e terceiros autorizados sob NDAs ou contrato contendo cláusulas específicas a respeito da confidencialidade das informações.
Confidencial	CONFIDENCIAL	O acesso não autorizado às informações pode causar danos catastróficos (irreparáveis) aos negócios e/ou à reputação da organização. Dados Pessoais Sensíveis e dados de pagamento enquadram-se nesta categoria.	A informação está disponível apenas para indivíduos selecionados dentro da organização e terceiros autorizados sob NDAs ou contrato contendo cláusulas específicas a respeito da confidencialidade das informações.

Qualquer tipo de informação em qualquer formato (por exemplo escrito, impresso, vídeo, imagem, mídia, verbal, armazenada digitalmente, transmitida pelo correio eletrônico), que não possui uma Classificação identificada, é considerada de USO INTERNO.

Os Terceiros devem estar atentos ao falar ou compartilhar informações confidenciais do EBANX em espaços públicos, mídias sociais ou durante teletrabalho. Devem, ainda, evitar a nomeação de outras entidades em conversas, considerando que o EBANX pode estar vinculado a Acordos de Não Divulgação (NDA) com essas partes.

4.3 Propriedade Intelectual

As informações (como aplicativos, documentos e cursos) produzidas por terceiros ou partes externas, no desempenho de suas funções contratadas, pertencem ao EBANX, a menos que o contrato especifique o contrário.

O terceiro deve cumprir os aspectos legais e regulamentares de propriedade intelectual e notificar imediatamente o time de Information Security ou o Departamento Jurídico do EBANX em caso de violação desta norma ou das leis de propriedade intelectual.

4.4 Funções e Responsabilidades

Esta norma estabelece as responsabilidades de todos os indivíduos envolvidos nos tópicos a seguir:

4.4.1 Monitoramento

- Os terceiros devem estar cientes de que qualquer informação que seja acessada, recebida ou transmitida na rede local e na Internet está sujeita a monitoramento, inspeção e registro, a fim de garantir a integridade dos dados e das informações e para fins de auditoria, incluindo a prevenção de ameaças cibernéticas;
- Os terceiros devem cooperar plenamente com qualquer atividade de auditoria iniciada pelo EBANX, incluindo auditorias conduzidas por terceiros em nome do EBANX.
- Os terceiros independentes podem realizar varreduras de vulnerabilidades e testes de penetração na infraestrutura de TI que processa informações confidenciais do EBANX,

adotando uma abordagem baseada em risco. Os resultados desses testes e os planos de remediação devem ser comunicados ao time de Information Security do EBANX;

- Todas as investigações de segurança serão gerenciadas ou coordenadas pelo time de Information Security. O EBANX e as empresas do seu grupo econômico monitoram muitos aspectos do comportamento do usuário, incluindo servidores, estações de trabalho e outros dispositivos de acesso à rede. Quando aplicável, e não se limitando a estes, os seguintes registros serão verificados em busca de problemas de segurança e exploração de vulnerabilidades:"
    - Eventos do sistema de detecção de intrusões;
    - Eventos de firewall;
    - Eventos de conta de usuário;
    - Eventos de varredura em rede;
    - Eventos de erro do sistema;
    - Eventos de aplicativos;
    - Eventos de navegação na internet;
    - Eventos de backup e recuperação de dados;
    - Ocorrências de problemas do Service Desk;
    - Atividade telefônica - relatórios detalhados de chamadas;
    - Atividades de câmera de vigilância;
    - Eventos da impressora de rede.

4.4.2 Direitos de Acesso

O acesso de terceiros aos recursos de rede, aplicativos web e instalações físicas é limitado e determinado pela necessidade de suas atividades. Devem, ainda, respeitar os níveis de acesso a sistemas, redes, equipamentos, instalações e informações do EBANX, conforme estabelecido pelo time de Information Security.

4.4.3 Segurança Física

Para acessar as instalações do EBANX, os terceiros devem respeitar as medidas de segurança a seguir:

- Os terceiros devem se identificar e se registrar na recepção. Informar a pessoa que acompanhará e o objetivo da visita antes da concessão de um crachá de identificação para a entrada em uma instalação do EBANX;
- Utilizar o crachá de identificação que lhe for concedido, enquanto estiver dentro das dependências do EBANX;
- Os terceiros que necessitam de acesso em áreas restritas, devem ser acompanhados por um ebanker, que deve acompanhá-lo durante toda a permanência. Os terceiros não devem utilizar o crachá fora das instalações e dependências do EBANX, deve manter o crachá em local seguro e confidencial;
- Terceiros podem manter o crachá em sua posse enquanto a prestação de serviços ao EBANX estiver ativa. Ao término do contrato/serviço, a devolução do crachá deve ser feita imediatamente.
- Em casos de perda, roubo, furto ou extravio do crachá de identificação deve ser relatado imediatamente ao time de Information Security, a Recepção e ebanker responsável pela contratação do serviço.

As seguintes atividades são proibidas, salvo se especificamente autorizadas:

- Qualquer tipo de gravação de vídeo, fotografia ou áudio nas áreas restritas, que envolva outros ebankers sem consentimento ou capture informacões do EBANX;
- Conectar qualquer dispositivo elétrico em uma fonte de alimentação nas áreas seguras;
- Tocar ou, de qualquer outra forma, adulterar qualquer equipamento instalado em áreas seguras;
- Conectar qualquer dispositivo a uma rede;
- Armazenar materiais ou equipamentos inflamáveis;
- Usar qualquer tipo de dispositivo de aquecimento.

4.4.4 Senhas

Os usuários devem empregar boas práticas de segurança ao criar e utilizar senhas, de acordo com as diretrizes a seguir:

- As senhas não devem ser divulgadas a outras pessoas, incluindo gerência e administradores de sistemas;
- As senhas não devem ser anotadas em quaisquer meios físicos, sendo o único armazenamento possível o aplicativo de gerenciamento de senhas fornecido e autorizado pelo time de Information Security;
- Cada usuário deve ativar a autenticação multifatorial (MFA) em todos os sistemas que fornecem esse recurso;
- Senhas geradas pelos usuários não devem ser compartilhadas através de qualquer canal (verbalmente, por escrito ou eletronicamente, etc.). Devem ser alteradas se houver qualquer indicação de que as senhas ou o sistema possam estar comprometidos, nesse caso, um incidente de segurança deve ser reportado;
- Senhas fortes devem ser criadas ou alteradas da seguinte maneira:
    - Utilizando pelo menos doze caracteres;
    - Utilizando pelo menos um caractere numérico;
    - Utilizando pelo menos um maiúsculo e pelo menos um caractere alfabético minúsculo;
    - Utilizando pelo menos um caractere especial;
    - As senhas não devem ser baseadas em dados pessoais (por exemplo, data de nascimento, endereço, nome do membro da família, etc.);
- As senhas devem ser trocadas a cada 3 meses;
- As senhas não devem ser compostas por palavras de dialeto ou jargão de qualquer idioma ou quaisquer palavras escritas de trás para frente;
- As senhas devem ser alteradas no primeiro login em um sistema;
- As senhas não devem ser armazenadas em um sistema de login automatizado (por exemplo, scripts, automações ou navegador);
- As senhas criadas e utilizadas para fins pessoais não devem ser as mesmas utilizadas para fins comerciais;

- Caso um sistema seja compartilhado entre usuários, com a devida autorização do time de Information Security, o acesso deverá ser realizado exclusivamente através do cofre de senhas. É fundamental que a senha compartilhada seja única e não seja reutilizada de contas pessoais ou de outros sistemas.

4.4.5 Uso Aceitável

Os ativos de informação devem ser utilizados apenas para necessidades de negócios com o objetivo de executar tarefas relacionadas à organização, e o uso destes ativos estão sujeitos às seguintes regras:

- Para garantir a segurança e a integridade dos dados da empresa, é proibido usar equipamentos do EBANX para fins pessoais. O EBANX não é responsável pelo backup de informações pessoais de terceiros.
- Os Terceiros devem estar cientes do uso dos recursos tecnológicos do EBANX e de quaisquer outros recursos que lhes sejam alocados. Portanto, não devem baixar softwares em computadores ou contratar soluções de software sem a homologação do EBANX, independentemente da área de atuação do funcionário terceiro;
- Os terceiros devem estar cientes do uso da conta de e-mail do EBANX, utilizando apenas para fins relacionados aos negócios do EBANX;
- As solicitações para contratação de softwares devem ser realizadas pela área de negócio do EBANX responsável pela contratação do Terceiro, e deve seguir as diretrizes da *Norma de Contratação de Terceiros* do EBANX;
- O terceiro não deve instalar ou usar dispositivos periféricos ou outros dispositivos para armazenar e ler dados (por exemplo, unidades flash USB) sem a permissão expressa do time de Information Security do EBANX.

4.4.6 Acesso Remoto

Os terceiros que atuarem remotamente devem assegurar a segurança dos dados e informações do EBANX e de seus clientes. Para isso, devem seguir estas orientações:

- O acesso remoto deve ser feito apenas por meio de dispositivos autorizados e protegidos por senhas fortes, com a autenticação de dois fatores habilitada e utilizando as ferramentas de acesso disponibilizadas pelo EBANX;
- Proteger as informações contra acesso não autorizado no seu local de trabalho remoto, que precisa ser adequado para as atividades;
- Ao utilizar dispositivos móveis em locais públicos, o usuário deve tomar cuidado para que os dados não possam ser lidos por pessoas não autorizadas.

4.4.7 Mesa, Tela e Lousa Limpa

- Ao trabalhar com dados e informações do EBANX, o terceiro deve assegurar que nenhuma informação confidencial ou sensível esteja visível para qualquer pessoa não autorizada (seja outro funcionário ou terceiro).
- Para evitar acesso não autorizado, documentos em papel e mídias de armazenamento confidenciais devem ser retirados de mesas, impressoras, fotocopiadoras e outros locais sempre que a pessoa autorizada se ausentar da estação de trabalho.
- Ao se ausentar da estação de trabalho, ebankers e terceiros devem sempre bloquear a tela do computador. Além disso, o sistema conta com um bloqueio automático que é ativado após dois minutos de inatividade.
- Quadros brancos e de vidro contendo informações internas, restritas e/ou confidenciais devem ter seu conteúdo apagado após a utilização.

4.4.8 Dados de Cartão de Crédito

Os terceiros não estão autorizados a solicitar dados de cartão de crédito, seja por e-mail, telefone ou qualquer outro meio. Se essas informações forem recebidas acidentalmente, o time de Information Security deve ser comunicado imediatamente.

4.4.9 Criptografia

As Informações devem ser criptografadas ao serem transmitidas externamente e, sempre que possível, em comunicações internas. Evite a transmissão verbal de dados e informações do EBANX em espaços públicos ou compartilhados.

4.4.10 Desenvolvimento Seguro

A certificação em Desenvolvimento Seguro é um pré-requisito obrigatório para todos os desenvolvedores que contribuem para o repositório de desenvolvimento. Esta certificação deve ser atualizada anualmente.

Existem ambientes preparados para executar validações de código, testes e provas de conceito que são gerenciados pelo time de CloudOPS, que são os administradores do ambiente. O acesso ao código-fonte de qualquer programa deve ser restrito e estritamente controlado.

4.4.11 Controles de Segurança

Os terceiros devem colocar em prática controles para prevenir, detectar, erradicar e recuperar-se de ameaças de malware;

Quaisquer alterações nos sistemas ou aplicativos que processam as informações confidenciais do EBANX devem ser revisadas e testadas para garantir que não haja impacto nas operações comerciais ou na segurança das informações.

4.4.12 Retenção e Descarte de Dados

Os terceiros devem devolver ou descartar informações ou dados (incluindo dados pessoais) do EBANX em sua posse, custódia ou controle nas seguintes situações:

- i) Quando não forem mais necessários para a finalidade original ii) se não houver exigência legal que determine o armazenamento iii) após a rescisão do Contrato. Vale o prazo que for mais longo entre essas condições;

Além disso, a devolução ou descarte deve ocorrer imediatamente, mediante solicitação do EBANX, a qualquer momento;

Os dados sensíveis ou informações confidenciais do EBANX devem ser armazenados de acordo com os períodos de armazenamento estabelecidos e somente pelo tempo que for necessário para os propósitos para os quais foram coletados de acordo com a Norma de *Retenção, Descarte e Destruição de Dados Pessoais*.

4.4.13 Transferência e Compartilhamento de Informações

Algumas práticas que devem ser seguidas ao transferir e/ou compartilhar interna ou externamente informações do EBANX:

- É proibido enviar materiais com conteúdo perturbador, desagradável, sexualmente explícito, rude, calunioso ou contendo qualquer outro conteúdo inaceitável ou ilegal;
- Se um terceiro receber um e-mail suspeito, especialmente se houver indícios de uma tentativa de phishing, deve reportar o conteúdo imediatamente através do "Phish Alert Button (PAB)" e comunicar ao time de Information Security através do e-mail infosec@ebanx.com;
- Ao enviar mensagens, documentações, apresentações ou qualquer informação classificada como Interna, Restrita e Confidencial, o terceiro deve protegê-la, conforme estabelecido na *Norma de Classificação da Informação*;
- Ao enviar informações do EBANX a qualquer destinatário, interno ou externo, considere o impacto de um acesso indevido e implemente as medidas de segurança necessárias para mitigar esse risco.
- Ao compartilhar informações relevantes, internas, restritas ou confidenciais, verifique se o destinatário possui um Termo de Confidencialidade (NDA) assinado ou um contrato contendo cláusulas de confidencialidade que protejam os dados do EBANX.
- Evite o envio de arquivos com Dados Pessoais ou confidenciais, caso necessário, proteja com senha;
- Não é permitido postar publicamente materiais considerados internos, restritos e/ou confidenciais;
- É proibido acessar arquivos corporativos em equipamentos desconhecidos, não homologados ou sem proteção adequada.
- Não realizar download, instalar ou acessar sites de software não homologados;

- Os terceiros devem estar atentos ao seu entorno ao se comunicar em espaços públicos e mídias sociais. Evite falar sobre informações internas, restritas ou confidenciais e não mencione terceiros (empresas ou indivíduos) relacionados ao EBANX.

4.5 Penalidades

Em caso de violação das diretrizes estabelecidas neste documento e em outros documentos relacionados às atividades prestadas, o terceiro estará sujeito à rescisão contratual imediata, sem prejuízo de outras sanções previstas em contrato e nas leis aplicáveis. O EBANX reserva-se o direito de tomar todas as medidas legais cabíveis para proteger seus dados, informações e ativos em caso de não conformidade com as normas estabelecidas.

4.6 Reporte de Incidentes

Um Incidente de Segurança refere-se a qualquer evento que comprometa ou possa comprometer a Confidencialidade, Integridade ou Disponibilidade dos dados em um sistema de informação. Isso pode incluir atividades maliciosas, como ataques de hackers, vírus, Malware, Phishing, acesso não autorizado, entre outros. Quando houver Dados Pessoais envolvidos, será chamado de Incidente de Privacidade.

O terceiro que suspeitar ou identificar um Incidente de Segurança (incluindo violações às Políticas e/ou vulnerabilidades observadas na segurança) ou um Incidente de Privacidade, deve reportá-lo imediatamente através do MyEBANXLife ou do e-mail infosec@ebanx.com. Essa ação rápida permite ao EBANX responder o incidente com agilidade e eficácia, minimizando danos e protegendo as informações.

O time de Information Security poderá solicitar mais informações, conforme necessário.

4.7 Treinamento e Conscientização

Todos os terceiros que têm acesso a dados e informações restritos e confidenciais devem receber conscientização e treinamento de Segurança da Informação e Privacidade.

O time de Information Security é responsável por promover treinamento e conscientização para garantir que terceiros compreendam suas responsabilidades em relação aos pilares de Segurança

da Informação confidencialidade, integridade e disponibilidade dos dados e informações do EBANX.

5. Referências Normativas

- **ISO/IEC 27000:2018** – Princípios e Vocabulários de Segurança da Informação.
- **ISO/IEC 27001:2022** – Requisitos para Sistemas de Gestão de Segurança da Informação (SGSI).
- **ISO/IEC 27002:2022** – Controles de Segurança da Informação.
- **ISO/IEC 27018:2019** – Práticas para Proteção de Dados Pessoais em Serviços de Nuvem.
- **ISO/IEC 27701:2019** – Sistema de Gestão da Privacidade da Informação (SGPI).

6. Documentação Relacionada ou de Apoio

- Norma de Segurança de Senhas;
- Norma de Classificação da Informação;
- Norma de Criptografia de Dados;
- Norma de Acesso Remoto;
- Norma de Desenvolvimento Seguro;
- Norma de Retenção, Descarte e Destruição de Dados Pessoais;
- Norma Programa de Conscientização de Segurança da Informação e Privacidade de Dados;
- Norma de Gestão de Incidentes de Segurança da Informação e Privacidade;
- Norma de Segurança Física;
- Norma de Contratação de Terceiros;
- Política de Segurança da Informação;
- Política de Governança de Privacidade e de Proteção de Dados.