Urbano Bank

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Esta política tem como objetivo definir critérios e diretrizes de controles a riscos de Segurança da Informação, como é identificado e classificado e prevenido este risco em termos de acesso e utilização, além do monitoramento dos riscos e gestão de continuidade na URBANO INSTITUICAO DE PAGAMENTOS S.A. ("URBANO BANK") e demais empresas do grupo.

Para fins desta política, são considerados riscos diretos à Segurança da Informação: malwares, Engenharia Social, ataques DDoS e qualquer tipo de invasão externa ou interna aos sistemas da empresa.

As políticas e procedimentos descritos nesta Política baseiam-se principalmente na ISSO 27001 e frameworks como COBIT e ITIL.

2. PÚBLICO ALVO

Todos os colaboradores da URBANO BANK e demais empresas do grupo, considerados usuários de dispositivos, softwares ou plataformas digitais da empresa e principalmente aos profissionais dos departamentos de Tecnologia da Informação, Segurança da Informação e Compliance que deverão manter o cumprimento das regras desta Política.

3. DEFINIÇÃO

DISPOSITIVOS MÓVEIS: São considerados todos os dispositivos que permitem mobilidade ao colaborador em suas atividades diárias, tais como, notebooks, celulares corporativos, tablets ou quaisquer outros equipamentos que a empresa possa disponibilizar aos colaboradores.

MALWARE: São considerados malware todos os aplicativos sistêmicos que possam danificar ou invadir a base de dados e servidores da empresa, tais como, código, programa ou software malicioso. Destacam-se os mais comuns:

a) **VÍRUS**: é um programa malicioso desenvolvido para infectar o sistema, fazer cópias de si e se espalhar para outros computadores e dispositivos.
b) **SPYWARE**: é um código ou programa espião que captura informações transacionais do usuário automaticamente.
c) **RANSOMWARE**: é um código malicioso que bloqueia o acesso a um determinado conjunto de dados, geralmente usando criptografia, com o objetivo de permitir ao infrator a exigência de um pagamento de resgate (ransom) para restabelecer o acesso às informações.

ENGENHARIA SOCIAL: é termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado à computadores ou informações.

PHISHING: é o termo que designa as tentativas de obtenção de informação identificável através de uma suplantação de identidade e utilização combinada de meios técnicos e engenharia social.

PHARMING: é uma prática fraudulenta semelhante ao phishing, a diferença é que no pharming, o tráfego de um site legítimo é manipulado para direcionar usuários para sites falsos.

VISHING: é o termo usado para descrever um tipo de phishing que combina e-mails ou mensagens de texto (SMS) e VoIP. Funciona de forma semelhante ao phishing.

SMISHING: é um golpe por mensagem de texto, supostamente vinda de uma fonte confiável e criada para induzir o usuário a revelar informações privadas através de mensagens SMS ou de texto.

ATAQUES DDOS (Distributed Denial Of Services) e BOTNETS: são ataques de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores e ocorre principalmente em servidores web. O ataque vem de um grande número de computadores infectados e procura tornar as páginas hospedadas indisponíveis na rede.

INVASÕES (Advanced Persistente Threats): é um ataque de rede de computador furtivo no qual uma pessoa ou grupo obtém acesso não autorizado a uma rede e permanece sem ser detectado por um longo período.

SPAM: são e-mails não solicitados que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamado de UCE (do inglês Unsolicited Commercial E-mail).

4. DIRETRIZES

O Departamento de Segurança da Informação é responsável por proteger os ativos de informação, detectando, respondendo e recuperando o ambiente de uma ameaça cibernética que poderá ser realizada por vários agentes, por exemplo: organizações criminosas, hackers individuais, organismos de Estado, terroristas, colaboradores, competidores etc. Todas as metodologias aplicadas seguem três pilares principais:

- **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade**: garantir a integridade das informações, evitando as modificações indevidas; e
- **Disponibilidade**: garantir que as informações estejam sempre disponíveis e acessíveis para as pessoas especificamente autorizadas.

4.1. Confidencialidade

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas. São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG, gênero, raça, cor, etc.), situação financeira e movimentação bancária;
- Informações sobre produtos e serviços que revelem vantagens competitivas da URBANO BANK frente ao mercado;
- Todo o material estratégico da URBANO BANK (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Quaisquer informações da URBANO BANK, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário.

4.1.1. Tratamento da Informação Confidencial

As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo. Sendo assim, todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização, sendo assim, nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não, ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas à própria URBANO BANK.

4.2. Integridade

Todas as formas de acesso à informação, serviços de rede e dados são controlados tendo como base as necessidades operacionais dos usuários e os requisitos de segurança.

4.2.1. Classificação de Riscos de Segurança da Informação

A identificação dos riscos relacionados à Segurança da Informação permite a priorização nos esforços de acordo com a sua estratégia de gerenciamento de riscos e necessidades do negócio definidos pela Diretoria Executiva da URBANO BANK e demais empresas do grupo. Para estabelecer uma referência ao Negócio, a tabela abaixo descreve os níveis de ameaça e vulnerabilidade. Importante ressaltar que para nível de tratamento a ameaça considerada pode ser tanto externa quanto interna.

Grau de risco	Ameaça (impacto)	Vulnerabilidade (esforço)
1	• Não atinge informações confidenciais. • Não compromete a disponibilidade do sistema.	• Existem controles já testados contra a ameaça. • Baixa complexidade técnica para estabelecer uma linha de defesa.
2	• Pode ou não atingir informações confidenciais. • Possui potencial para afetar a disponibilidade do sistema.	• Existem controles contra a ameaça, porém ainda não testados. • Alguma complexidade técnica para estabelecer uma linha de defesa.
3	• Atinge diretamente informações confidenciais. • Pode paralisar o sistema.	• Ausência de controles contra a ameaça. • Elevada complexidade técnica para estabelecer uma linha de defesa.

Tabela 1: referência para classificação de risco baseado no nível de ameaça e vulnerabilidade ao negócio.

Para medir o índice de fragilidade na Segurança da Informação, é necessário multiplicar o grau de risco da categoria “Ameaça” e o grau de risco da categoria “Vulnerabilidade”, o produto determina, de forma quantitativa, o grau de severidade da falha de segurança, conforme matriz abaixo.

		BAIXO 1 a 2	MÉDIO 3 a 4	ALTO 5 a 9
		Vulnerabilidades		
		1	2	3
Ameaça	1	1	2	3
	2	2	4	6
	3	3	6	9

Tabela 2: matriz de grau de severidade do risco de Segurança da Informação.

4.2.2. Acesso aos dispositivos e softwares

A concessão de acessos aos ambientes de Produção, Desenvolvimento e Homologação (testes) deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação necessários para o pleno desempenho de suas atividades profissionais. Desta forma, a área de Controle de Acessos é responsável por gerir estes acessos e atualizar a Matriz SoD.

Os usuários devem ter identificação única (login e senha), pessoal e intransferível; e são os responsáveis pelas ações realizadas por intermédio desta identificação. As senhas iniciais de sistemas e equipamentos devem ser programadas para a auto expiração, exigindo a sua troca imediata a partir do primeiro acesso do usuário. As novas senhas deverão seguir as regras abaixo:

- Incluir letras maiúsculas e minúsculas.

- Incluir números.
- Incluir símbolos.
- Número de caracteres entre 8 e 12.
- Não começar ou terminar com espaço.
- Não incluir frase comum.
- Não permitir repetição das mesmas senhas utilizadas durante o ano.

Os Colaboradores devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum, ou seja, não informar a ninguém e não anotar em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado / "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (“Ctrl” + “Alt” + “Del” > “Bloquear” ou “tecla do Windows” + “L”).

Os direitos de acesso dos colaboradores, terceiros e fornecedores desligados deverão ser removidos imediatamente após a solicitação pelo departamento de Recursos Humanos.

Semestralmente, as permissões de acesso deverão ser revisadas pelo “Proprietário da Informação” e pelo Gestor imediato do usuário.

Os ativos em geral, dispositivos móveis como Notebook, tables e celulares corporativos, deverão ser identificados de forma individual, inventariados e ter um proprietário responsável, denominado “Proprietário da Informação”. Estes ativos deverão ser protegidos de acessos indevidos, ter documentação atualizada e plano de manutenção formal sob custódia do departamento de Infraestrutura e TI.

Apenas os equipamentos e softwares disponibilizados ou homologados pela URBANO BANK e demais empresas do grupo podem ser instalados e conectados à rede da URBANO BANK. Equipamentos particulares ou privados, como computadores ou qualquer dispositivo portátil que possa armazenar ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o Negócio, nem devem ser conectados às redes da empresa sem a devida aprovação do cargo de liderança responsável.

4.3. Padrões de Segurança da Informação

Trata-se de procedimentos e regras que visam garantir que um processo seja feito sempre de forma padronizada e da maneira mais correta possível.

4.3.1. Hardening

A definição e aplicação do Hardening em servidores e desktops, é realizada juntamente com a equipe de Segurança da Informação, pelas equipes de infraestrutura, que administra os sistemas operacionais Windows (desktops e servidores), e pela equipe de administração de servidores UNIX, LINUX, AIX, e banco de dados.

Para os equipamentos de rede a equipe responsável é a de Redes e Telecom, que devem aplicar e definir o Hardening em conjunto com a área de Segurança da Informação. Todos os documentos de Hardening aplicados no ambiente de tecnologia da Instituição de Pagamento, devem ser avaliados pela área de Segurança da Informação, que tem a função também de fiscalizar e auditar as tecnologias com o objetivo de validar o cumprimento das regras definidas.

Todas as alterações e/ou adição de um novo Hardening devem ser avaliadas e aplicadas somente através do processo de mudanças (GMUD).

4.3.2. Expurgo e Retenção de Dados

É um método eficiente de proteção dos dados armazenados, processo de retenção de dados que identifica quais dados precisam ser retidos e onde ficam, de que forma serão excluídos ou destruídos, com segurança, assim que não forem mais necessários.

- Limitar a quantia de dados armazenados e o tempo de retenção às restrições conforme exigências legais, regulatórias e/ou comerciais;
- Requisitos de retenção específicos para dados do titular da conta de pagamento digital ou do usuário de cartão de crédito ou débito;
- Processos para exclusão segura de dados quando não mais necessários;
- Processos trimestrais para identificar e excluir com segurança os dados do titular do cartão que excederem a retenção definida;
- Os únicos dados do titular do cartão que podem ser armazenados são o número da conta principal ou PAN (desde que ilegível), data de vencimento, nome do titular do cartão e código de serviço;

4.3.3. Prevenção a Perda de Dados (DLP)

Uma ferramenta DLP é um dos mecanismos utilizado contra prevenção de perda de dados. O emprego deste tipo de mecanismo permite à Instituição de Pagamento detectar e evitar situações que podem resultar na perda de dados.

- Detectar e evitar a perda não autorizada de PAN em texto simples (número do cartão aberto), documentos restritos ou classificados como confidenciais, arquivo de configuração de ambientes tecnológicos, código fonte desenvolvido.
- Gerar logs e alertas sobre a detecção de PAN em texto simples deixando o CDE via canais, métodos ou processos não autorizados.
- Investigar as ocorrências em tempo hábil para identificar onde há necessidade de correções e fornecer informações valiosas para ajudar a entender a origem das ameaças.
- Corrigir imediatamente vazamentos de dados ou lacunas no processo, identificados como incidentes, para evitar a perda de dados.

4.4. Protocolos de Segurança

Em ambiente de Tecnologia, um protocolo de segurança (protocolo criptográfico, protocolo de criptografia ou protocolo criptografado), é um protocolo abstrato ou concreto que realiza uma função de segurança relacionada e aplica métodos de criptografia.

Protocolos de criptografia são amplamente utilizados para o transporte de dados em aplicativos de segurança.

a) Todos os serviços, protocolos e portas não seguros precisam estar documentados e justificados;
b) Todas as novas implementações devem ser ativadas com TLS 1.2 ou superior;
c) Implementações existentes que usam SSL ou TLS antigo devem estabelecer um plano formal de migração e redução de riscos, e devem ser colocados em prática antes de 30 de junho de 2018;
d) Os requisitos do PCI DSS diretamente afetados são:
    I. Requisito 2.2.3 Implementar recursos de segurança adicionais para todos os serviços, protocolos ou daemons exigidos considerados não seguros;
    II. Requisito 2.3 Criptografar todo acesso administrativo que não utiliza console com criptografia robusta.
    III. Requisito 4.1 Usar protocolos de segurança e criptografia robusta para proteger dados sensíveis do titular do cartão durante a transmissão em redes abertas e públicas.

Os exemplos de serviços, protocolos ou portas não seguras incluem, entre outros, FTP, Telnet, POP3, IMAP, SNMP e NetBIOS.

Os exemplos de serviços, protocolos ou portas seguras incluem, entre outros, SSH, S-FTP, SSL ou IPSec VPN e TLS.

4.5. Antivírus

São programas de computador concebidos para prevenir, detectar e eliminar vírus de computador e outros malwares.

Os padrões de Segurança da Informação para as regras de anti-vírus/anti-malware estão contidos em documento específico.

4.6. Identificação do usuário

Os usuários terão identificação única, pessoal e intransferível, qualificando-os como responsáveis pelas ações realizadas nas estações de trabalho e demais acessos que utilizarem tais credenciais.

Perfil de acesso de administrador (funcionalidades privilegiadas) somente serão criadas para usuários cadastrados para execução de tarefas específicas.

4.7. Concessão de acesso

A concessão de acessos, terá perfis pré-estabelecidos, por área e função, e deverá ser aprovada pelo gestor responsável de acordo com o perfil da função do usuário para o desempenho da atividade.

4.8. Segregação de funções

Todos os processos são resguardados através da segregação de funções, de forma que as atividades não sejam executadas e controladas pelo mesmo colaborador, mitigando riscos de fraudes ou erros operacionais e até mesmo risco de contencioso trabalhista por acúmulo de atividades e funções.

4.9. Disponibilidade

O departamento de Tecnologia da Informação em conjunto com o de Segurança da Informação devem manter disponíveis todos os recursos de tecnologia necessários para o bom andamento do Negócio. Desta forma, caso o incidente de segurança da informação seja identificado pelo público geral, o mesmo deverá ser reportado ao departamento competente para a devida análise e posterior tratamento.

Falhas são inevitáveis, mas os impactos resultantes como o colapso do sistema, a interrupção no fornecimento do serviço e a perda de dados, podem ser evitados com planejamento e mecanismos necessários para a manutenção da disponibilidade.

Neste contexto, os esforços estão concentrados de forma a garantir a continuidade dos processos e serviços vitais de uma organização ainda que sob o impacto de um desastre súbito e inesperado identificado previamente. Os principais objetivos que devem ser atingidos são:

- Minimizar danos imediatos e perdas numa situação de emergência;
- Assegurar a restauração das atividades, instalações e equipamentos o mais rápido possível;
- Assegurar a rápida ativação dos processos de negócios críticos; e
- Fornecer conscientização e treinamento para as pessoas chave encarregadas desta atividade.

4.10. Segregação de Ambientes / Dados

Os ambientes de produção devem ser segregados dos ambientes de desenvolvimento, testes e homologação e rigidamente controlados.

Todos os dados de teste/simulação e contas dos aplicativos personalizados, Ids e senhas de usuários devem ser removidos antes dos sistemas serem implantados.

4.11. Monitoramento e Auditoria do Ambiente

Os sistemas são monitorados incluindo: estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo a ter rastreabilidade.

Há também no ambiente sistemas de proteção, preventivos que detectam uma possível ameaça, a fim de garantir a segurança das informações e dos perímetros de acesso.

Qualquer informação que é acessada, transmitida, recebida ou produzida utilizando-se dos recursos tecnológicos da Instituição de Pagamento, estão sujeitos a monitoração e auditoria a qualquer momento não necessitando de um aviso prévio.

4.12. Dispositivos Móveis

São considerados dispositivos móveis todos os equipamentos eletrônicos que permitam a mobilidade na execução do trabalho, alguns exemplos: notebooks, gravador de CDs, DVDs, pen-drive, celulares ou smartphones, e etc.

Os recursos computacionais móveis de propriedade da Instituição de Pagamento, são destinados exclusivamente para os serviços e negócios da mesma e devem possuir mecanismos de criptografia ativo e antivírus instalado.

Sua utilização é proibida para fins particulares ou prestação de serviços a terceiros.

4.13. Tecnologias Críticas

São os recursos físicos ou lógicos utilizado no armazenamento, transmissão, processamento e manuseio das informações confidenciais / interna e restrita da Instituição de Pagamento. Enquadram-se nesse conceito: documentos em papel, computadores, VPN, programas de computador, base de dados, linhas telefônicas, servidores, celulares, notebooks, USB , CD´s, etc.

4.14. Contratação de serviços de processamento e armazenamento de dados e de computação em nuvem

A URBANO BANK executa um criterioso processo de escolha e contratação de fornecedores de serviços de processamento e armazenamento de dados, sendo considerado os seguintes itens para a efetiva formalização do contrato de prestação de serviços.

a) Pesquisa detalhada dos possíveis fornecedores, sendo analisado o histórico da empresa no mercado atuante, análise reputacional da empresa e quando possível dos seus sócios e representantes;
b) Análise dos riscos inerentes ao negócio x escopo do serviço prestado x garantias contratuais fornecidas pelo fornecedor;
c) Verificação da capacidade operacional do fornecedor para atender a demanda solicitada pela empresa contratante;
d) Verificação do modelo de acesso aos dados que serão armazenados no ambiente do fornecedor, sendo que, o acesso deverá ser restrito e conter a segurança mínima definida pelos órgãos reguladores;
e) A URBANO BANK poderá a qualquer momento, solicitar evidências de segurança da informação e integridade dos dados processados e armazenados aos fornecedores, bem como, solicitar auditoria que assegure que as obrigações de segurança pelo fornecedor estão sendo adotadas, essas obrigações deverão obrigatoriamente estar representadas em contrato firmado entre as partes;
f) O fornecedor contratado, deverá formalizar a integridade, manuseio, processamento e custódia dos dados através de um termo de responsabilidade e confidencialidade, além disso o fornecedor deverá evidenciar que todos os dados e

informações armazenados em seu ambiente está seguro contra invasão, roubo de dados etc., sendo enviado periodicamente as informações para a empresa.

A URBANO BANK a contratar o fornecedor de serviços de processamento e armazenamento de dados, garantirá que o serviço contempla o monitoramento dos dados transacionados pelo ambiente do fornecedor, através de sistema automatizado, bem como, segregação de dados e ambientes com demais clientes evitando que terceiros possam ter acesso aos dados armazenados. Havendo qualquer situação de risco, fragilidade ou irregularidade identificada o fornecedor deverá corrigir de imediato.

Dado que a URBANO BANK coleta e armazena dados sensíveis e financeiros de terceiros, esta deverá obrigatoriamente contratar empresas de primeira linha, considerando os critérios de avaliação e capacidade para prestar os serviços de processamento e armazenamento de dados, sendo ainda considerado o conceito de segurança de informação com camadas de criptografias e testes tempestivos de segurança (Intrusão, PEN TEST, entre outros), o resultado dos testes, devem ficar em posse da URBANO BANK.
Todas as plataformas sistêmicas da URBANO BANK em que transitam dados do cliente, deverão ser submetidas a auditoria e testes de segurança periodicamente, garantindo a integridade da plataforma e dos dados ali transitados, sendo esses testes executados por consultores independentes.

Todo e qualquer serviço tecnológico, de armazenamento e processamento de dados contratado ou alterado pela URBANO BANK, será após a assinatura do contrato, comunicado ao órgão regulador e demais entidades ou parceiros comerciais que for necessário, de modo que esses possam ter ciência do fornecedor e serviços contratados.

A URBANO BANK não irá contratar ou alterar nenhum serviço de tecnologia que apresente risco de continuidade nos serviços oferecidos a seus clientes. Assim tal avaliação ocorrerá como já descrito no processo de definição do fornecedor.

Caso o fornecedor não possua convênio ou esteja autorizado ou homologado pelo BACEN para oferecer tal serviço, mas a URBANO BANK entenda que o fornecedor está apto a executar tal serviço, a URBANO BANK solicitará autorização ao BACEN para atuar em parceria com o fornecedor, devendo assim o contrato ser firmado após a autorizado do ente regulador.

5. RESPONSABILIDADE

O gerenciamento e monitoramento de segurança da informação na URBANO BANK e demais empresas do grupo, é parte integrante do processo de gestão dos negócios e compreende:

a) A identificação, avaliação, mensuração, mitigação e controle desses riscos.
b) A gestão dos riscos relacionados a segurança da informação é realizada de forma conservadora, respeitando as alçadas e os limites definidos, com o objetivo de proteger a imagem, os valores e princípios da URBANO BANK e demais empresas do grupo, bem como de seus diretores, colaboradores, cliente e fornecedores e parceiros, contribuindo assim para a sustentabilidade dos negócios.
c) Divulgação continua das diretrizes, responsabilidades, conceitos e princípios relacionados a segurança da informação, visando o aculturamento de seus diretores, colaboradores, cliente e fornecedores e parceiros, além da utilização de ferramentas, metodologias e modelos, em linha com o nível de complexidade dos seus negócios, produtos, processos e sistemas, a fim de obter monitoramento reforçado na detecção de indícios de casos suspeitos e nos processos de avaliação e mensuração dos riscos, permitindo a melhor definição de limites e alçadas, assim como a mitigação dos riscos de forma eficiente e eficaz.

5.1. Usuários de dispositivos e softwares

Os usuários possuem a responsabilidade de proteger as informações por eles produzidas no ambiente físico ou sistêmico da URBANO BANK e demais empresas do grupo e respeitar a sua devida classificação, seja esta informação em meio físico ou digital.

Zelar pelos dispositivos e acessos a ambientes e sistemas da empresa, além de comunicar qualquer situação anormal aos departamentos competentes.

5.2. Departamento de Recursos Humanos

O departamento de recursos humanos da URBANO BANK e demais empresas do grupo, deverão formalizar a contratação e o desligamento do colaborador antecipadamente (ao menos 2 dias de antecedência) ao responsável pelo departamento de Segurança da Informação ou Infraestrutura.

5.3. Diretoria de Segurança da Informação

A Diretoria da Segurança da Informação deverá estabelecer e revisar as diretrizes de segurança desta e demais políticas aplicáveis com o objetivo de minimizar os riscos cibernéticos da URBANO BANK e demais empresas do grupo.

Atender e responder eventuais dúvidas de aplicação referente as às diretrizes desta Política.

Adicionalmente a Diretoria de Segurança da Informação terá a responsabilidade em conjunto com o Departamento de Recursos Humanos de implementar programa de capacitação dos colaboradores da área, assim como, elaborar forma de avaliar o desenvolvimento, desempenho e conhecimento dos colaboradores envolvidos, sendo que essa avaliação poderá ocorrer pelo menos 2 (duas) vezes ao ano ou frequência maior se assim a Diretoria entender necessário.

5.4. Departamento de Segurança da Informação

O Departamento de Segurança da Informação será responsável por monitorar todos os incidentes internos e externos da Instituição de pagamento, além de identificar as causas, impactos e possíveis correções, reportando formalmente à sua diretoria e se o incidente for muito grave acionar o Comitê específico para expor o cenário.

Mensalmente o Departamento de Segurança da Informação deverá emitir um relatório gerencial e KPIs dos incidentes ocorridos, incidentes corrigidos, incidentes em fase de correção e “backlogs” de incidentes a serem analisados ou corridos.

Além desse reporte o departamento de Segurança da Informação deverá ainda, em conjunto, com a área de compliance e controles internos definir critérios e controles internos para mitigar riscos de incidentes que impactam a Instituição de Pagamento.

5.5. Diretoria de Riscos, Compliance e PLD

A Diretoria de Riscos, Compliance e PLD será responsável pela aplicabilidade e revisão da presente política bem como pela auditoria da aderência da empresa às diretrizes definidas neste documento, reportando as não conformidades à Diretoria Executiva e a quem mais possa interessar.

5.6. Diretoria Executiva

A Diretoria Executiva será responsável por aprovar a medida disciplinar proposta pelo Departamento de Compliance ou pelo Comitê de Auditoria em casos de atos de corrupção e fraude cometidos. Deverá ainda reafirmar estrategicamente o compromisso da URBANO BANK e demais empresas do grupo com temas relacionados à ética e integridade corporativa.

6. SANÇÕES ADMINISTRATIVAS

O descumprimento das disposições legais ou regulamentares internas pode acarretar sanções disciplinares e administrativas, no caso de Diretores e Colaboradores ou o encerramento do relacionamento comercial, no caso de parceiros, fornecedores ou prestadores de serviços.

Quando a área de Compliance tiver conhecimento de situações por parte do colaborador, que representem violação ao estabelecido nesta Política e demais normas internas, a equipe de Compliance, liderada por seu gestor ou Diretor, deverá analisar o caso e tomar as medidas disciplinares cabíveis, conforme abaixo descritas.

O Diretor ou Colaborador será notificado formalmente para apresentar defesa em até 10 (dez) dias úteis contados do recebimento da notificação, sob pena de serem considerados verdadeiros os fatos imputados e aplicadas as penalidades especificadas adiante. Em todos os casos, as notificações serão tratadas com o maior sigilo possível.

Os procedimentos adotados serão conduzidos pelo gestor ou Diretor da área, a quem cabe também a recomendação final das respectivas penalidades para aprovação pela Diretoria.

As penalidades aplicáveis resumem-se em advertência, suspensão temporária e afastamento definitivo.

A omissão diante da violação conhecida da lei, de qualquer disposição desta política e demais normas internas, não é uma atitude correta e constitui, em si mesma, uma violação das normas internas, passível de aplicação de:

- **Falta Leve:** será considerada "Falta" a violação de qualquer item desta política e das demais normas internas que regem a URBANO BANK e demais empresas do grupo que, a critério do Diretor de Risco, Compliance e PLD, embora tenha ocorrido, não trouxe qualquer prejuízo financeiro, operacional ou à imagem das empresas do grupo.
- **Penalidade:** advertência verbal e anotação no prontuário do Colaborador, mantido para os devidos efeitos de arquivamento ("Prontuário").
- **Falta Grave:** será considerada "Falta Grave" a violação de qualquer item desta política e das demais normas internas, que tenha trazido pequenos prejuízos financeiros, operacionais ou à imagem das empresas do grupo, à critério do Diretor de Risco, Compliance e PLD, ou ainda, se houver reincidência de alguma Falta Leve cometida anteriormente, **por no mínimo 3 (três) vezes em um intervalo de 2 (dois) anos**.
- **Penalidade:** advertência formal, anotação no Prontuário do Colaborador e aplicação de suspensão das atividades pelo período de até 3 (três) dias úteis, formalizada pelo Departamento de Recursos Humanos.
- **Falta Gravíssima:** será considerada "Falta Gravíssima" a violação de qualquer artigo desta política e das demais normas internas, que apresente prejuízos financeiros, operacionais ou à imagem das empresas do grupo, à critério do Diretor de Risco, Compliance e PLD, ou ainda, se houver reincidência de alguma Falta Grave cometida anteriormente, **por no mínimo 3 (três) vezes em um intervalo de 2 (dois) anos.**
- **Penalidade:** afastamento definitivo das atividades exercidas perante a empresa (Desligamento).

A aplicação das penalidades acima não isenta, dispensa ou atenua a responsabilidade civil, administrativa e criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos resultantes da infração da legislação em vigor e das políticas e procedimentos estabelecidos neste documento.

7. REFERÊNCIAS

Tipo de documento	Nome do documento
Lei	LEI Nº 12.965, DE 23 DE ABRIL DE 2014. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.
Norma / Regulamento	ISO 27.001:2009 CIRCULAR N. 3.909 DE 16 DE AGOSTO DE 2018 RESOLUÇÃO N. 85 DE 08 DE ABRIL DE 2021

8. HISTÓRICO

VERSÃO	DESCRIÇÃO DA ATUALIZAÇÃO	APROVADOR	DATA DA VERSÃO
1.0	Primeira publicação.	ANTONIO CARBONARI FILHO	12/11/2021

Acesse nosso site para ver mais!

www.urbanobank.com

Telefone: (11) 2224-3333