BANCO SOL
O banco de todos nós

NORMA DE APLICAÇÃO PERMANENTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NAP – GSC/02/2025

Publicado em:

08-01-2025

NORMA DE A/02PLICAÇÃO PERMANENTE – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. DISPOSIÇÕES GERAIS

No presente capítulo apresentam-se disposições gerais referentes à Norma de Aplicação Permanente da Política de Segurança de Informação:

- Histórico de actualizações e revogação de Normativos Internos;
- Enquadramento legal e Normativos Internos associados;
- Objectivo e âmbito;
- Conceitos, abreviaturas e nomenclaturas;
- Órgãos de estrutura responsáveis;
- Conteúdos regulamentados.

1.1. Histórico de Actualizações e Revogações de Normativos

1.1.1. Histórico de Actualizações

VERSÃO	DATA DE PUBLICAÇÃO	AUTOR	PRINCIPAIS ALTERAÇÕES
1	26/12/2022	Direcção de Organização e Qualidade	Primeira publicação da Política de Segurança da Informação
2	08/01/2025	Direcção de Organização e Qualidade	Revisão periódica da Política no intuito de garantir a reengenharia: Actualização dos procedimentos

1.1.2. Revogações de Normativos

A presente Norma de Aplicação Permanente vem regulamentar a Política de Segurança da Informação, revogando, a versão anterior de 26/12/2022.

1.2. Enquadramento Legal e Normativos Internos

Consideram-se relevantes para a presente Norma de Aplicação Permanente os seguintes diplomas externos:

- Norma ISO/IEC 27001;
- Norma ISO/IEC 27002;
- **Directiva n.º 05/DSB/DRO/2022- Sistema Financeiro**- Gestão dos Riscos Associados às Tecnologias de Informação e Comunicação e à Segurança Cibernética;
- **Aviso n.º 08/2020 Sistema Financeira -** Política de Segurança Cibernética e Adopção de Computação em Nuvem.

1.3. Objectivo e Âmbito

O objectivo da Política de Segurança da Informação é fornecer ao Banco, uma abordagem para a gestão dos riscos da informação e directrizes para a protecção dos activos de informação a todas as Unidades de Estrutura e entidades contratadas para prestação de serviços.

Neste contexto, é interpretado que a informação, os sistemas e os serviços utilizados pelos colaboradores são da exclusiva propriedade do Banco e não podem ser considerados de uso pessoal, salvo disposição em contrário na legislação aplicável.

Assim sendo, está proibida a divulgação, a duplicação, a destruição, o uso inadequado, roubo e o acesso não autorizado à informação pertencente ao Banco, a Clientes e as outras entidades.

O acesso à informação, aos sistemas e aos serviços do Banco deve ser previamente autorizado, de forma adequada em função do seu conteúdo, controlado e devidamente supervisionada, respeitando sempre o princípio do privilégio mínimo necessário.

A Política de Segurança da Informação fornece um conjunto integrado de medidas de protecção que devem ser aplicadas uniformemente no Banco para garantir um ambiente operacional seguro para suas operações comerciais.

A Política de Segurança da Informação (PSI) aqui descrita é aplicável a pessoas ou entidades, com acesso à Informação, aos sistemas e tecnologias da informação e comunicação do Banco Sol ou sob a responsabilidade desta, colaboradores de fornecedores, prestadores de serviços, parceiros, consultores, com acesso à Informação e aos Sistemas de Tecnologias da Informação e Comunicação do Banco Sol, ou sob a responsabilidade desta. O termo "Utilizadores" será utilizado genericamente em referência a qualquer um dos indivíduos ou entidades atrás referidas. A Política deve estar disponível a todos, sendo exigido destes o respeito pelos controlos de segurança implementados, essenciais ao cumprimento sustentável dos seguintes valores mínimos da Segurança da Informação:

- Confidencialidade da Informação – Protecção contra o acesso não autorizado;
- Integridade da informação – Protecção contra a modificação e a destruição não autorizada de Informação, salvaguardando a respectiva fiabilidade e origem;
- Disponibilidade da Informação – Garantir que as informações e serviços estejam acessíveis aos utilizadores autorizados quando necessário.

1.4. Conceitos, Abreviaturas e Nomenclaturas

Apresenta-se em seguida a lista de siglas e conceitos utilizados ao longo da presente Norma de Aplicação Permanente:

- **Activo de Informação -** Qualquer componente (seja humano, tecnológico, software...) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio, onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas.
- **Activos -** É tudo aquilo de tem valor para a instituição.
- **Áreas de gestão de acesso –** são as áreas responsáveis pela definição e gestão das funções e privilégios de acesso de cada utilizador / colaborador.
- **Autenticação -** Propriedade de um sistema que permite identificar quem apode aceder um determinado objecto (como um sistema, arquivo ou instalação) por meio da combinação correcta do nome de utilizador e sua senha de acesso.
- **Backup [Cópia de Segurança] -** Cópia de dados de um dispositivo de armazenamento para outro, permitindo assim, que os mesmos possam ser restaurados em caso de perda dos dados originais.
- **Backup Completo, Full, Total ou Normal -** Faz o backup na íntegra de todos arquivos e directórios seleccionados para a média de backup.
- **Backup Diferencial -** É um backup cumulativo de todos arquivos criados ou alterados desde o último backup completo.
- **Backup Incremental -** É feito o backup apenas dos arquivos criados ou alterados desde o último backup completo ou incremental.
- **Backup -Período de retenção -** Tempo em que os dados ficam guardados, após este período, são descartados, libertando o espaço de armazenamento ocupado, em espaço para novos backups.
- **BCM [Business Continuity Management / GCN (Gestão de Continuidade de Negócio)] -** Processo holístico de gestão que identifica ameaças potenciais para uma organização e os impactos para as operações de negócio que essas ameaças, caso se concretizem, podem causar, e que fornece um framework para uma construção organizacional resiliente com a capacidade para uma resposta eficaz, que salvaguarde os interesses de seus actores principais, a reputação da marca, e actividades de criação de valor.

- **Código-fonte -** É o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica. Após ser compilado, o código fonte transforma-se em software, ou seja, programas executáveis.
- **Confidencialidade -** Propriedade da informação que garante que a mesma não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização, ou seja, é a garantia do resguardo das informações dadas pessoalmente em confiança e protecção contra a sua revelação não autorizada.
- **Continuidade de negócio -** Capacidade estratégica e táctica da organização para planear e responder a incidentes e interrupções de negócio, com objectivo de continuar as operações de negócio num nível aceitável pré-definido.
- **Dados -** Conjunto de valores ou ocorrências em um estado bruto com o qual são obtidas informações com o objectivo de adquirir benefícios.
- **Data Center -** Instalação que centraliza as operações e equipamentos de TI de uma organização, bem como armazenamento, gestão e disseminação seus dados.
- **Disponibilidade -** Propriedade que garante que a informação esteja disponível sempre que requisitada pelos utilizadores autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.
- **Gestores -** Todos aqueles que exercem funções de gestão no âmbito da organização, administrando pessoas e/ou processos.
- **Informação -** Reunião ou conjunto de dados e conhecimentos organizados que possam constituir referências sobre um determinado acontecimento, facto ou evento. Este conhecimento pode ser registado em forma impressa, digital, oral ou audiovisual.
- **Integridade -** Propriedade que garante que a informação não seja adulterada falsificada ou furtada.
- **ISO / IEC -** Comité técnico conjunto da Organização Internacional para Padronização (ISO) e da Comissão Electrotécnica Internacional (IEC), sua finalidade é desenvolver, manter e promover padrões nas áreas de tecnologia da informação (TI) e Tecnologia da Informação e Comunicação (TIC).
- **ISO/IEC 27001 -** Especifica os requisitos para estabelecer, implementar, operar, monitorar, rever, manter e melhorar um sistema de gestão de segurança da informação de acordo com as necessidades específicas de cada organização.
- **ISO/IEC 27002 -** É um padrão de segurança da informação, denominado: Técnica de segurança - Código de prática para controlos de segurança da informação. Funciona como um guia completo de implementação, em que descreve quais controlos devem ser estabelecidos e de que forma. Ela tem como base uma avaliação de riscos dos activos mais importantes da empresa.
- **ISO/IEC 27005 -** É o padrão internacional que lida com o gerenciamento de riscos de segurança da informação. A norma fornece directrizes para o gerenciamento de riscos de segurança da informação em uma empresa, apoiando particularmente os requisitos do sistema de gerenciamento de segurança da informação definido na ISO 27001.
- **Log / Logs -** Expressão utilizada para descrever o processo de registo de eventos relevantes num sistema computacional.
- **MFA [Multi-Factor Authentication / Autenticação Multifactorial] -** É uma solução de autenticação de dois factores que fornece aos utilizadores e administradores uma segunda camada de verificação ao efectuar logon em aplicativos ou portais. O MFA possui duas ou mais maneiras de verificação de acesso, a autenticação é comprovada através de Senha, Dispositivos móveis ou factores presentes no próprio utilizador como Biometria.
- **PSI -** Política de Segurança da Informação.

- **Política de Segurança da Informação -** Conjunto de acções, técnicas e boas práticas relacionadas ao uso seguro de dados, ou seja, trata-se de um documento que determina as acções mais importantes para garantir a segurança da informação.
- **Programa Utilitário -** É um pequeno programa que fornece uma adição aos recursos fornecidos pelo sistema operativo.
- **Proprietário do Activo -** Indivíduo ou entidade que detém a gestão e a responsabilidade pelo controlo de todo o ciclo de vida do activo.
- **RTO [Recovery Time Objective]** - Objectivo de tempo de recuperação, em que o banco sol pode estar sem operar enquanto se efectuam os restauros dos serviços e aplicações para a continuidade dos serviços do Banco.
- **SIEM [Security Information and Event Management / Gerenciamento e Correlação de Eventos de Segurança] -** É uma solução de segurança e auditoria composto por componentes de monitoramento e análise de eventos.
- **SI -** Segurança da Informação.
- **SLA [Service Level Agreement] -** Compromisso assumido por um prestador de serviços de TI perante um cliente. Este compromisso descreve o serviço de TI, os níveis de qualidade que devem ser garantidos, as responsabilidades das partes e eventuais compensações quando os níveis de qualidade não forem atingidos.
- **SOC [Security Operations Center / Centro de Operações de Segurança] -** É um termo genérico que descreve parte ou a totalidade de uma plataforma cujo objectivo é prestar serviços de detecção e reacção a incidentes de segurança a informação.
- **Token -** Dispositivo electrónico gerador de senhas, geralmente sem conexão física com o computador, podendo também em algumas versões, ser conectado a uma porta USB.

1.5. Órgãos de Estrutura Responsáveis

O Gabinete de Segurança Cibernética é responsável pela actualização da presente Norma de Aplicação Permanente.

É da responsabilidade das Lideranças directas, assegurar que o conteúdo da presente Política seja levado ao conhecimento dos seus subordinados.

1.6. Conteúdos Regulamentados

Na presente Norma de Aplicação Permanente encontram-se estabelecidas as regras e princípios orientadores, no que se refere a:

CAPÍTULO	NOME DO CAPÍTULO
2	Política de Segurança da Informação
3	Outorgamento

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

No presente capítulo apresentam-se regulamentados os seguintes temas:

- Funções;
- Responsabilidades Gerais;
- Directrizes Gerais;
- Penalidades;
- Nota de Propriedade e Distribuição;
- Gestão Documental;
- Aprovação e Revisão.

2.1. Funções

No seu âmbito, cabe:

- **Conselho de Administração** – Assegurar que os objectivos da política estejam alinhados com a direcção estratégica do Banco e aprovar a política, assim como supervisionar a sua eficácia;
- **Comité de Informática e Segurança –** Participar da elaboração da política, planear, garantir que a política é mantida e revista periodicamente;
- **Comissão Executiva** – Assegurar os recursos e mecanismos internos necessários à aplicação da política;
- **Gabinete de Segurança Cibernética –** Elaborar e supervisionar periodicamente a aplicabilidade da política;
- **Direcção de Auditoria Interna –** Baseia-se na política para testar os controlos dos processos e procedimentos inerentes a política;
- **Direcção de Gestão de Risco –** Identificar, avaliar, controlar, mitigar e monitorar os riscos inerentes a operacionalização da política;
- **Direcção de Compliance –** Verificar a conformidade da política com as normas vigentes no país;
- **Todas as unidades de Estrutura** – Implementação da política.

2.2. Responsabilidades

2.2.1. Responsabilidade gerais

Todos os utilizadores:

- São responsáveis pela utilização ética, legal e consciente dos recursos computacionais e de informação do banco, incluindo a protecção e o uso adequado de credenciais e autorizações de acesso aos sistemas.
- Devem cumprir as orientações estabelecidas em relação ao uso dos recursos, manter-se actualizados sobre as políticas de segurança da informação e reportar, de imediato, quaisquer suspeitas de incidentes ao responsável apropriado.

Conselho de Administração:

- Avaliar e aceitar os riscos no âmbito da segurança da informação em nome do Banco, assegurando que sejam devidamente monitorizados e controlados;
- Identificar responsabilidades e objectivos de segurança da informação e integrá-los nos processos estratégicos e operacionais relevantes;
- Apoiar a implementação consistente de políticas, normas e padrões de segurança da informação;
- Promover a segurança de informação através de orientações claras e a atribuição de recursos financeiros, tecnológicos e humanos adequados;
- Designar proprietários de informações e garantir a confidencialidade, integridade e disponibilidade dos dados;
- Participar na gestão e resposta a incidentes de segurança, assegurando a resolução eficaz e a prevenção de riscos futuros;
- Comunicar os requisitos da Política de Segurança da Informação (PSI) à força de trabalho e terceiros,

promovendo o alinhamento e a conformidade."

2.2.2. Responsabilidades Específicas

Direcção de Tecnologia e Sistemas de Informação

- Projectar e implementar a arquitetura de SI que suporte a Política de Segurança da Informação do Banco, garantindo que as redes, os sistemas, os serviços e os seus dados estejam adequadamente protegidos;
- Identificar, avaliar e gerir os riscos relacionados com segurança da informação, adoptando, proactivamente, as tecnologias, as técnicas e as estratégias mitigadoras dos riscos e garantir a integridade, confidencialidade e disponibilidade dos activos sob sua gestão operacional.
- Implementar as políticas, normas, procedimentos de segurança de informação e as melhores práticas nas vertentes tecnológicas e operacionais, assegurando a sua monitorização contínua e a resposta a incidentes;
- Desenvolver planos técnicos de resposta a incidentes e a capacidade de resposta, através de intervenções de contenção e de recuperação, assegurando a integridade dos SI e a continuidade operacional do Banco.
- Garantir a conformidade dos processos e das funções de SI com as normas do sector bancário, a legislação nacional e as normas internacionais.
- Garantir que apenas os colaboradores com necessidades de acessos privilegiados os têm configurados, devendo autorizar, rever e garantir a remoção dos mesmos, quando já não se justifiquem;
- Zelar pela eficácia dos controlos de Segurança da Informação (SI) utilizados e informar aos gestores e demais interessados os riscos residuais;
- Criar, implementar e gerir uma Política de Uso Aceitável de Recursos de Tecnologia de Informação;
- Configurar os activos de informação e computacionais concedidos aos utilizadores com todos os controlos necessários para cumprir os requisitos de segurança;
- Gerar e manter registos para auditoria, implementando controlos de integridade para torná-los juridicamente válidos como evidências;
- Garantir a segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- Zelar pela segregação de funções, a fim de restringir ao mínimo necessário os privilégios de cada utilizador e eliminar a existência de pessoas que possam excluir eventos e registos de auditoria das suas próprias acções;
- Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro activo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta (a responsabilidade pela gestão dos "acessos" de utilizadores externos é do gestor do contracto de prestação de serviços ou do gestor UE em que o utilizador externo desempenha suas actividades);
- Proteger continuamente os activos de informação contra código malicioso;
- Assegurar que não sejam introduzidas vulnerabilidades no ambiente de produção e garantir a

actualização tempestiva das aplicações e sistemas;

- Definir regras formais para instalação de software e hardware em ambiente corporativo;
- Responsabilizar-se pelo uso, manuseio e guarda de certificados digitais corporativos;
- Garantir que todos os dispositivos com acesso à rede operem com o relógio sincronizado;
- Monitorizar o ambiente de TI, gerando indicadores de uso da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos, períodos de indisponibilidade e actividade dos utilizadores externos;
- Garantir a utilização de protocolos de criptografia seguros, como SSL/TLS, para garantir a confidencialidade e integridade dos dados durante a transmissão;
- Garantir que os dados sensíveis e confidenciais armazenados nos sistemas de informação do Banco sejam criptografados em repouso e durante a transmissão, utilizando algoritmos robustos e padrões reconhecidos, abrangendo todos os dispositivos de armazenamento e implementando protocolos seguros como SSL/TLS;
- Avaliar e monitorar os prestadores de serviços que têm acesso aos sistemas ou informações sensíveis do Banco;
- Garantir a realização de backups regulares e a recuperação de dados em caso de falhas ou desastres.

Gabinete de Segurança Cibernética

- Promover a consciencialização dos colaboradores em relação à relevância da segurança da informação, assegurando que todos os colaboradores compreendam as suas responsabilidades e as boas práticas para manter a segurança cibernética;
- Desenvolver e implementar um plano de resposta a incidentes de segurança da informação, garantindo que o Banco tem processos bem definidos e a capacidade para responder a falhas e violações de segurança e minimizar os seus potencias impactos.
- Implementar sistemas de monitoramento contínuo de identificação de vulnerabilidades e de ameaças, assegurando uma resposta em tempo útil;
- Identificar, avaliar e compreender os riscos de segurança da informação aos quais o Banco está exposto, gerindo adequadamente estes riscos através da implementação de medidas proactivas e reactivas, com o propósito permanente de melhoria contínua e mitigação;
- Testar e avaliar a eficácia dos controlos de segurança de informação existentes e apresentar, periodicamente, os respectivos relatórios, nos quais deve incluir, detalhadamente, as falhas, as vulnerabilidades e os riscos identificados e propor as correspondentes acções de melhoria;
- Coordenar a realização de testes regulares de recuperação para avaliar a eficácia dos planos de resposta a incidentes e a resiliência dos sistemas do Banco, assegurando que os planos de continuidade de negócios (PCN) estão adequados e apresentando os respectivos relatórios.
- Monitorizar os sistemas de controlo de acesso, garantindo que apenas as pessoas autorizadas e adequadamente capacitadas têm acesso aos sistemas de informação e manter um processo obrigatório de certificação periódica das permissões de acesso.
- Avaliar os riscos cibernéticos potencialmente associados aos fornecedores externos, realizando

auditorias de segurança e garantindo que os contratos incluem cláusulas de segurança cibernética adequadas;

- Propor e coordenar a realização de testes de penetração regulares realizados por entidades especializadas e independentes, com o objectivo de identificar falhas e vulnerabilidades nos sistemas de informação do Banco, antecipando possíveis ataques e avaliando a robustez da infraestrutura de segurança;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação.

Gestores de U.E e DCH

- Comunicar alterações de responsabilidades ou funções internas para revisão e ajuste dos privilégios de acesso aos sistemas do banco.
- Reforçar a segregação de funções para minimizar o risco de fraudes e abusos internos, garantindo que as responsabilidades sejam distribuídas adequadamente.
- Sempre que um colaborador deixe de desempenhar funções no banco ou se ausente por um período superior a 5 dias, o responsável da UE na qual o mesmo desenvolveu / desenvolve a sua actividade deve informar a DTI e DSG para que esta possa desactivar todas as suas contas de acesso as aplicações, a sistemas operativos (que suportavam essas aplicações), os sistemas RAS (Remote Access Service) e/ou VPN (Virtual Private Network), e aos pontos de acesso físico das instalações do banco.

2.3. Directrizes Gerais

Directrizes específicas e procedimentos próprio deverão ser fixados em norma complementar, considerando as seguintes directrizes gerais:

2.3.1. Tratamento da Informação

- Toda informação relacionada às operações do Banco, gerada ou desenvolvida nas suas unidades de estrutura, durante a execução das actividades do colaborador ou qualquer outro profissional contratado constitui um activo do Banco, essencial à condução de negócios e em última análise, à sua existência;
- Os colaboradores e quaisquer outros profissionais contratados pelo Banco devem ter acesso somente às informações estritamente essenciais para a execução de suas responsabilidades;
- Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. O acesso, modificação, divulgação e destruição devem ser efectuados apenas sob autorização da Comissão Executiva;
- Não é permitido armazenar informações não classificadas como públicas em dispositivos pessoais, como smartphones, tablets, ou em dispositivos de armazenamento removíveis, como USBs e discos externos;
- As informações devem ser geridas adequadamente desde a sua criação, passando pelo uso autorizado, até o descarte adequado;
- Qualquer reprodução integral de informações deve possuir a mesma classificação de confidencialidade que o original. As reproduções parciais devem ser avaliadas para determinar se uma nova classificação é necessária;

- Cada categoria de classificação tem um conjunto aprovado de controlos destinados a proteger essas categorias, descritos na Política de Classificação da Informação;
- Cada Unidade de Estrutura deve comunicar os requisitos para o manuseio seguro das informações às equipes de trabalho;
- Deve ser mantido um inventário, seja em formato escrito ou electrónico, de todos os activos de informação;
- Todos os activos de informação devem ter um proprietário de informação estabelecido dentro das linhas de negócios.

2.3.2. Classificação da Informação

A classificação da informação é incumbência do seu responsável habilitado, considerando o nível de confidencialidade necessário no momento de sua geração. No banco, está estabelecido as seguintes categorias para a classificação da segurança de informação:

- **Informação muito confidencial -** É toda informação associada a interesses relevantes do Banco. Se revelada, pode trazer sérios prejuízos financeiros, enorme impacto ao negócio ou repercussões para a imagem da Instituição ou do Governo de Angola;
- **Informação confidencial -** É toda informação cujo conhecimento deve ficar limitado a um número reduzido de pessoas autorizadas. Se revelada, pode trazer grande impacto ao negócio ou repercussões para a imagem da Instituição, embaraços administrativos com funcionários ou trazer vantagens a terceiros;
- **Informação reservada -** É toda informação cujo conhecimento e uso deve estar restrito a um grupo específico de colaboradores ou Unidades de Estrutura do Banco. Não deve ser divulgada, publicada e estar acessível a qualquer colaborador ou não-colaborador;
- **Informação interna -** É toda informação cujo conhecimento e uso está restrito exclusivamente ao âmbito interno e propósitos do Banco, estando disponível para todos os colaboradores, e prestadores de serviço autorizados a circular em suas dependências. Só devem ser reveladas ao público externo mediante autorização;
- **Informação pública -** É toda informação que pode ou deve ser divulgada para o público externo à Instituição.

2.3.3. Conscientização de Segurança

Todos os colaboradores do banco e quando relevante, prestadores de serviço e consultores devem receber treinamento de conscientização adequado e actualizações regulares nas políticas e procedimentos organizacionais, conforme a relevância para sua função de trabalho.

2.3.4. Acesso à rede e aos sistemas de informação

- Para aceder aos sistemas de informação do banco, é necessário obter permissão formal antecipada e seguir as regras estabelecidas na Política de Acesso Lógico do banco;
- O acesso a sistemas, tecnologias e aplicações deve ser feito através de autenticação por utilizador e palavra-passe, sendo que cada utilizador deve ter uma palavra-passe única; Não é permitida a partilha de credenciais de autenticação entre grupos de utilizadores;

- A criação e gestão de contas de acesso dos utilizadores deve ser realizada de acordo com a Norma de Processo – Gestão de acesso, respeitando sempre o princípio de privilégios mínimos;
- É proibido conectar quaisquer dispositivos móveis (*Smartphones* e/ou *Tablet*) incluindo dispositivos de armazenamento amovíveis (USB e Discos Externos) aos sistemas de informação do banco.

2.3.5. Utilização de Acesso à Internet e Correio Electrónico Corporativo

- O acesso à internet é regulado por dois modelos:
  - Modelo geral, que é baseado no princípio de listas autorizadas, onde os acessos são permitidos apenas a sites autorizados;
  - Modelo restrito, que se adapta às necessidades específicas de cada direção e requer validação prévia do administrador de pelouro.
- O acesso do colaborador a internet e correio electrónico corporativo, deverão ser exclusivos para a execução e desempenho dos objectivos do Banco;
- Não é permitido o acesso, exposição, armazenamento, distribuição, edição de material de natureza pornográfica, racista, xenófoba, religiosa, política e desportiva, através do uso dos recursos informáticos do Banco;
- Não é permitido a utilização de softwares de ponto a ponto;
- O acesso a internet para propósitos particulares ou estranhos as actividades do banco poderão ser bloqueadas, sem prévia comunicação ao colaborador, sem prejuízo das demais sanções aplicáveis;
- Os equipamentos, tecnologias e serviços fornecidos para o acesso à *internet* são de propriedade do banco, que pode analisar e se necessário, bloquear qualquer arquivo, caixa de correio electrónico, domínio ou aplicação armazenados na rede/*internet*, estejam eles em disco local, na estação de trabalho ou em áreas privadas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação.

2.3.6. Gestão da Palavra Passe

- As palavras passe devem ser alteradas imediatamente após a emissão para a primeira utilização;
- A palavra passe utilizadas nas aplicações ou sistemas do Banco devem ser exclusivas e diferentes das palavras passe utilizadas para serviços pessoais (ex: email, facebook…);
- A palavras passe devem ser alteradas regularmente e devem cumprir com os requisitos de complexidade descritos na Politica de Gestão de Palavra Passe;
- Deve ser implementado um procedimento de bloqueio de conta em todos os sistemas para limitar tentativas de adivinhação de palavra passe.

2.3.7. Monitorização de Acessos

Para garantir a aplicação das directrizes mencionadas nesta política, além de fixar normas e procedimentos complementares sobre o tema, o Banco poderá:

- Implementar sem aviso prévio, sistemas de monitoria nas estações de trabalho, servidores, correio electrónico, conexões com a internet, dispositivos móveis ou wireless e outras componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar utilizadores e respectivos acessos efectuados, bem como o material manipulado;

- Realizar, a qualquer tempo, avaliação física nos equipamentos de sua propriedade;
- Instalar sistemas de protecção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso;
- Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

2.3.8. Acesso Remoto

- O acesso remoto aos sistemas de informação do Banco deve ser feito mediante autorização formal, em função das necessidades especificas e definidos em procedimento próprio;
- Todo colaborador com o serviço remoto deve ter um acordo de confidencialidade de modos a garantir a protecção da informação acedida;
- As contas devem ser activadas apenas durante o período de tempo necessário;
- Os utilizadores poderão se conectar ou obter acesso apenas aos equipamentos e recursos para os quais tenham permissão e direitos de uso, qualquer acção contraria será considerada uma violação;
- Todos os dispositivos conectados via acesso remoto devem ser propriedade do banco ou aprovados por empresas contratadas;
- Todas as conexões de acesso remoto devem incluir um sistema de "time-out" após um período especificado de inactividade;
- A redistribuição do instalador de VPN do banco ou informações de instalação associadas é proibida;
- A reconfiguração do equipamento de um utilizador para fins de túnel dividido ou homing duplo não é permitida em nenhum momento.

2.3.9. Gestão de Riscos de Informação

- Qualquer sistema ou processo que apoie funções de negócios deve ser adequadamente gerido quanto ao risco de informação e passar por avaliações de risco de informação, pelo menos anualmente, como parte de um ciclo de vida de desenvolvimento de sistema seguro;
- Avaliações de risco de segurança da informação devem ser feitas para novos projectos, implementações de novas tecnologias, mudanças significativas no ambiente operacional ou em resposta à descoberta de uma vulnerabilidade significativa;
- Uma avaliação periódica de riscos deve ser realizada nas instalações de processamento e armazenamento de informações para determinar se os controlos existentes estão operando correctamente e se são necessárias medidas adicionais de segurança física / logica. Estas medidas devem ser implementadas para mitigar os riscos;
- Os resultados da avaliação de riscos e as decisões tomadas com base nesses resultados devem ser documentados.

Nota: Esta política constitui uma parte do conjunto abrangente de políticas implementadas pelo banco para promover a segurança da informação e garantir o cumprimento dos padrões regulatórios e organizacionais, bem como outras que venham a ser aprovadas neste domínio. As políticas listadas abaixo complementam e reforçam os princípios e directrizes delineados nesta norma:

- Política de Classificação da Informação;
- Política de Controlo de Acesso Lógico;
- Política de Gestão da Palavra Passe;
- Política de Correio Electrónico;
- Política de Secretária e Ecrã Limpo;
- Política de Gestão de Acesso Físico ao Data Center;
- Política de Privacidade;
- Política do Plano de Resposta a Incidentes Cibernéticos;
- Política de Gestão de Mudanças;
- Política de Treinamento e Consciencialização de Segurança.

2.4. Penalidades

O não cumprimento desta política constitui falta grave e o utilizador que a viole estará sujeito a acção disciplinar incluindo o despedimento e/ou processo civil e criminal.

2.5. Nota de Propriedade e Distribuição

Este documento é propriedade do Banco Sol, ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

- É permitido fazer cópias inalteradas do documento completo ou em partes, contanto que esta nota de distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais;
- Se este documento for distribuído apenas em partes, instruções de como obtê-lo por completo devem ser incluídas;
- É permitido o uso dos exemplos de documentos e de configuração incluídos neste texto. Tal uso é completamente livre e não está sujeito a nenhuma restrição;

É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa do Banco Sol.

2.6. Gestão Documental

Ao avaliar a eficácia e adequação deste documento, os seguintes critérios devem ser considerados:

- Comunicação interna na Organização;
- Formação aos utilizadores;
- Revisão e auditoria periódica da política;
- Elaboração da documentação de Procedimentos.

2.7. Aprovação e Revisão

A presente política entrará em vigor na data da sua aprovação pelo Conselho de Administração, devendo ser revisto com periodicidade predefinida e quando se verifiquem alterações justificáveis para garantir que se mantenha actualizado; O Gabinete de Segurança Cibernética que deve garantir que o mesmo é revisto pelo menos uma vez por ano.