BANCO SOL
O banco de todos nós

NORMA DE APLICAÇÃO PERMANENTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

NAP – GSC/02

Publicado em:

26-12-2022

NORMA DE APLICAÇÃO 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

1.1.2. Revogações de Normativos

A presente Norma de Aplicação Permanente vem regulamentar a Política de Segurança da Informação, não revogando, nenhum Normativo Interno em vigor.

1.2. Enquadramento Legal e Normativos Internos

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

- **Norma ISO/IEC 27001:2013;**
- **Norma ISO/IEC 27002:2005;**
- **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 FINANCEIRO-** 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 Sol, uma abordagem para a gestão dos riscos da informação e directrizes para a protecção dos activos de informação à todas as Unidades de Estrutura e entidades contratadas para prestação de serviços.

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

A Política 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 empregue 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 – prevenção contra o acesso e a divulgação não autorizada de Informação;
- Integridade da informação – prevenção 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:

- **Activos -** É tudo aquilo de tem valor para a instituição.
- **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.
- **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 registrado 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 registro de eventos relevantes num sistema computacional.
- **Login -** é o processo para aceder um sistema informático restrito feito através da autenticação ou identificação do utilizador, usando credenciais previamente cadastradas no sistema para esse utilizador.
- **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 usuário como Biometria.
- **Patches de Segurança -** Um patch (termo da língua inglesa que significa, literalmente, "remendo") é um programa de computador criado para actualizar ou corrigir um software de forma a melhorar a sua usabilidade, performance e/ou segurança.
- **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.

- **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.

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;
- Revisão e Gestão Documental.

2.1. Funções

- **Administração do Topo** – Assegurar que os objectivos da política estejam alinhados com a direcção estratégica do Banco Sol e aprovar a política;
- **Comité de Informática e Segurança –** Participar da elaboração da política, planear, garantir que a política é mantida e revista periodicamente;
- **Gabinete de Segurança Cibernética –** Elaborar e supervisionar periodicamente a aplicabilidade da politica;
- **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 Gerais

É responsabilidade de todos os utilizadores:

- Seguir de forma colaborativa as orientações fornecidas em relação ao uso dos recursos computacionais e de informação do Banco Sol;
- Pela utilização de suas credenciais e autorizações de acesso aos sistemas, bem como pelas acções decorrentes da utilização destes.
- Utilizar de forma ética, legal e consciente os recursos computacionais e de informação do Banco Sol;
- A salvaguarda da sua informação pessoal e garantir que esta não é ilegal, ilícita ou imprópria face ao código deontológico do Banco Sol.
- Manter-se actualizado em relação a esta Politica de Segurança de Informação (PSI) e às normas e procedimentos relacionados, buscando informação junto a DTI sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

2.2.1. Responsabilidades Específicas

Direcção de Tecnologia e Sistemas de Informação

- Garantir que apenas os utilizadores com necessidade 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.

- Configurar os activos de informação e computacionais concedidos aos utilizadores com todos os controlos necessários para cumprir os requisitos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.

- Gerar e manter registos para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e

fraudes.

Para os registos gerados e/ou mantidos em meio electrónico, deve ser implementado controlos de integridade, de modo a 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 para o Banco Sol.
- 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 "logins" 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 todos os activos de informação do Banco Sol contra código malicioso, e garantir que todos os novos activos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do Banco Sol ou em fase de mudança do ambiente de desenvolvimento ou teste (quando tais ambientes forem acedidos por terceiros, a responsabilidade deve ser explicitada nas cláusulas dos instrumentos contractuais).
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo.
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura de certificados digitais corporativos.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais de Angola.
- Monitorizar o ambiente de TI, gerando indicadores e históricos de uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; e actividade de todos os utilizadores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, *upload/download* de arquivos).

Gabinete de Segurança Cibernética

- Promover a consciencialização dos colaboradores em relação à relevância da segurança da informação;
- Testar a eficácia dos controlos utilizados e informar aos gestores os riscos residuais;
- Realizar verificações periódicas das configurações técnicas e análise de riscos;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação.
- Monitorizar os eventos de Segurança de Informação (vírus, trojans, furtos, acessos indevidos…);

- Avaliar as ameaças tecnológicas e físicas, tendo em conta as potenciais ameaças externas, ameaças internas e ameaças decorrentes de transacções com terceiros;
- Analisar acções para prevenir, detectar e responder aos ataques cibernéticos ou violações de dados, bem como identificar áreas ou preocupações em relação a possíveis vulnerabilidades e melhores práticas;
- Rever aspectos relacionados com os controlos de acesso, planos de resposta a incidentes, recuperação de desastres, acesso físicos e remotos a sistemas e protecção de perímetro aos activos de TI;
- Apoiar na definição de acções a implementar face aos riscos de segurança da Informação.

Gestores de UE e DCH

- Comunicar formalmente as áreas de gestão de acesso (Físico e Logico) sempre que exista uma alteração de responsabilidades ou de funções de um Utilizador interno, para que os privilégios de acesso desse Utilizador, aos diferentes Sistemas e Tecnologias de Informação do Banco Sol, possam ser adequadamente revistos e alterados. Se for Utilizador externo essa competência será do responsável da unidade de estrutura onde o serviço é ou era prestado.
- Sempre que um colaborador do Banco Sol deixe de trabalhar, a equipa de gestão de acessos deve desactivar todas as suas contas de acesso, com base em informação recebida pela DCH. Esta equipa deve desactivar todas as 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 aos edifícios do Banco. A DCH deve também garantir a recolha do cartão do colaborador e de todos os meios informáticos a si disponibilizados pelo Banco Sol (Desktop e/ou Notebook, telemóvel, ...). Deve depois proceder à eliminação de toda a informação de carácter pessoal associado a esse colaborador.
- Sempre que um colaborador de uma entidade externa deixe de desempenhar funções no Banco Sol, o responsável da UE na qual desenvolveu a sua actividade deve informar a equipa de gestão de acessos 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 aos edifícios do Banco. A área interna responsável pelo serviço prestado pela entidade externa deve também assegurar a recolha de eventuais cartões de acesso.

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 Sol, gerada ou desenvolvida nas suas unidades de estrutura, durante a execução de actividades do colaborador ou de um prestador de serviços externos constitui um activo do Banco Sol, essencial à condução de negócios e em última análise, à sua existência.
- 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.

2.3.1.1. Classificação da Informação

Os graus de classificação de segurança da informação, correspondentes ao nível de sensibilidade da informação, definidos no Banco Sol são os seguintes:

- **Informação muito confidencial -** É toda informação associada a interesses relevantes do Banco Sol. 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 Sol. 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 Sol, 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.

2.3.2. Conscientização de Segurança

Todos os colaboradores do Banco Sol 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.

2.3.3. Acesso à rede e aos sistemas de informação

- Acessos a sistemas, tecnologias e aplicações devem ser via autenticação por utilizador + palavra passe que deve ser única para cada Utilizador. Não é permitida a partilha de autenticação por grupos de Utilizadores.
- Deve adoptar-se transversalmente um sistema de gestão de identidades centralizado. Nesse sistema devem estar armazenados os dados que identificam todos os Utilizadores, internos e externos, definindo os seus privilégios de acesso aos diferentes sistemas, tecnologias e aplicações, o período de validade de cada um desses privilégios e a cadeia de autorização.
- O controlo de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos utilizadores aos activos de informação do Banco Sol.
- A criação e gestão de contas deve ser realizada de acordo com procedimento específico para todo e qualquer utilizador.
- O acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do utilizador por período mínimo a ser definido em norma específica.
- As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

- É proibido descarregar qualquer pasta e/ou ficheiro para os dispositivos móveis pessoais (Smartphones e/ou Tablet) incluindo dispositivos de armazenamento amovíveis (USB e Discos Externos) que possam colocar em causa a Confidencialidade e Integridade dos dados.

2.3.4. Utilização de acesso à internet e correio electrónico corporativo

- O uso e acesso do colaborador a internet e correio electrónico corporativo, deverão ser exclusivos para o uso profissional, para a execução e desempenho dos objectivos do Banco Sol.
- Não é permitido o acesso, exposição, armazenamento, distribuição, edição de material de natureza pornográfica, racista, xenófoba, religiosa, politica e desportiva, através do uso dos recursos informáticos do Banco Sol;
- Não é permitido a utilização de softwares de ponto a ponto;
- O acesso a internet para propósitos particulares ou estranhos as actividades do Banco Sol poderão ser bloqueados, 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 Sol, 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

2.3.5. Gestão da Palavra Passe

- Todos os Utilizadores devem estar consciencializados para a importância da escolha de uma palavra passe que não seja fraca.
- As palavras passe devem ser alteradas imediatamente após a emissão para a primeira utilização;
- As palavras passe nunca devem ser partilhadas com outra pessoa por qualquer motivo ou de qualquer maneira que não seja consistente com esta política. Uma palavra passe partilhada constitui um risco para a segurança da informação e como tal deve ser reportado;
- A palavra passe utilizadas nas aplicações ou sistemas do Banco Sol 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.

2.3.6. Monitorização de Acessos

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

- Implementar sem aviso prévio, sistemas de monitoria nas estações de trabalho, servidores, correio electrónico, conexões com a internet, dispositivos móveis ou wireless e outros 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.

2.3.7. Acesso Remoto

- O acesso remoto aos sistemas de informação do Banco Sol deve ser feito mediante autorização formal, em função das necessidades e definidos em procedimento próprio;
- O utilizador que tiver 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 e devem ser desactivadas imediatamente depois disso;
- Os utilizadores devem proteger suas credenciais de acesso e não devem partilhá-las com ninguém por qualquer motivo.
- Os utilizadores apenas poderão se conectar ou obter acesso aos equipamentos e recursos para os quais tenham permissão e direitos de uso, qualquer acção contraria será considerada uma violação na rede.
- Todos os dispositivos conectados às redes internas do Banco Sol via acesso remoto devem ser dispositivos propriedade do Banco Sol ou aprovados por empresas contratadas;
- Utilizadores terceirizados autorizados devem ser obrigados a se autenticar antes de terem permissão para aceder informações que não sejam publicas;
- Todos os dispositivos, de propriedade do Banco Sol e de terceiros, conectados à rede interna do Banco Sol via VPN ou qualquer outra tecnologia devem utilizar um sistema operativo actualizado e configurado correctamente, com *patches* de segurança actualizada e um software antivírus válido e actualizado;
- Ao se conectar remotamente à rede do Banco Sol, os utilizadores devem garantir que o dispositivo remoto não esteja conectado a nenhuma outra rede ao mesmo tempo, com excepção de redes pessoais que estão sob seu controlo total ou sob o controlo total de um terceiro autorizado;
- Todas as conexões de acesso remoto devem incluir um sistema de "time-out" após um período especificado de inactividade;
- É proibida a redistribuição do instalador ou informações de instalação associadas a VPN do Banco Sol;
- Não é permitida a reconfiguração do acesso por parte de um utilizador;
- Deve ser realizada monitorização e registo das actividades executadas pelos utilizadores. Qualquer evento registado, que indique alguma violação dos acessos cedidos deve implicar o bloqueio do utilizador de acordo ao procedimento próprio.

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. Aprovação, Revisão e Gestão Documental

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.

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.