Política de Segurança da Informação e Cibernética do Banco do Brasil S.A.

Versão 1.0

Brasília, maio de 2024

EQUIPE TÉCNICA
Fabiane Moreno
Jéssica Simas
Lusianna Soares
Vinícius Simon

Histórico de Versões

Data	Versão	Descrição	Autor
28/05/2024	1.0	Primeira versão da Política de Segurança da Informação e Cibernética do Banco do Brasil S.A.	Equipe técnica

Sumário

Política de Segurança da Informação e Cibernética do Banco do Brasil S.A.

1. Objetivo

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio e local em que ela esteja contida, com base na legislação vigente, órgãos reguladores, autorreguladores e nas boas práticas de segurança da informação.

2. Responsabilidade

Esta Política é de reponsabilidade do Diretoria de Riscos do Banco do Brasil. Quaisquer mudanças nesta Política devem ser aprovadas pela Diretoria de Riscos do Banco do Brasil.

A alta gestão tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

Essa política se aplica a todos os colaboradores, fornecedores e prestadores de serviços que utilizem ou forneçam serviços tecnológicos relevantes.

3. Público alvo

Esta Política se aplica a todas as instituições do Banco do Brasil.

4. Diretrizes gerais

4.1 Tratamento da Informação:

A informação sob custódia de qualquer instituição do Banco do Brasil, mesmo que pertencente a clientes, colaboradores ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas.

O acesso, geração, utilização, classificação, modificação, distribuição, transferência, armazenamento e eliminação da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados. As instituições do BB reservam-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada, pelo tempo determinado pela instituição, legislação ou regulação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

4.2 Acesso à Informação

O uso de redes externas de comunicação (Internet, redes privadas etc.) deve ser controlado através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e

restringindo–se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.

Adicionalmente, quando o acesso externo for realizado com o propósito de Home Office, deve ser observada e seguida a Política de Home Office disponível na Intranet.

A remessa de dados da organização, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

4.3 Sistemas Aplicativos

Sistemas aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Sistemas aplicativos desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no

desempenho de atividades críticas do sistema. Onde for impraticável implantar a segregação, outros controles como monitoração das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos sistemas os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso. Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga (Capacity Planning).

5. Diretrizes específicas

5.1 Tratamento da Informação

Para o conjunto de informações utilizado por um sistema aplicativo, o Comitê Diretivo de Segurança e Contingência deve designar dois proprietários, diretores do Conglomerado, sendo um deles representante da área operacional e o outro da área de negócios.

São atribuições dos proprietários das informações:

i. Nomear o gestor das informações, a quem cabe propor as regras de acesso às referidas informações, e administrá-las operacionalmente; e

ii. Aprovar as regras de acesso às informações, conforme proposta do gestor.

Cada gestor de informações indicará um gestor substituto, a ser aprovado pelos proprietários, que deverá exercer suas funções em caso de ausência.

Cada gestor da informação e seu substituto receberão um login diferenciado para exercer esta função, ou seja, configurar os sistemas para atender às normas abaixo descritas para tratamento da informação, bem como a concessão de acessos a usuários.

i. Normas para tratamento da informação

Devem ser definidas regras claras para proteção da informação contra perda, alteração, acesso por pessoas não autorizadas, trilha e logs de atividade e rastreabilidade, seja qual for o meio em que vier a ser armazenada (eletrônico, magnético, impresso etc.).

Devem ser claramente definidos os usuários (empresas, áreas, pessoas etc.) das informações, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não-autorizadas, independentemente da forma como estiver disponível.

Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da empresa.

Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda.

Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização.

É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade das Instituições, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Diretoria responsável, e das quais os colaboradores venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

Os usuários devem adotar a prática de classificação da informação com o objetivo de fornecer o tratamento adequado à informação no aspecto de sua confidencialidade.

ii. Recomendações para o tratamento da informação

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco.

As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa.

Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do colaborador que necessita do suporte. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento.

Os gestores devem determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:

a. Riscos inerentes às informações:

- Acesso por pessoas não autorizadas;
- Alteração, utilização, classificação, modificação, distribuição, transferência armazenamento ou eliminação indevida; e
- Indisponibilidade.

b. Consequências:

- Fraudes: Possibilidades de lesarem as instituições do BB ou terceiros (clientes, fornecedores etc.);

- Problemas legais: Possibilidades de gerar prejuízos, multas, penalidades ou embaraços às Instituições, Diretores e Colaboradores do BB, a outras pessoas físicas ou jurídicas;

- Perda de negócio: Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;

- Prejuízo de imagem do BB: Possibilidades de prejudicar a imagem do Banco do Brasil ou de seus colaboradores;

- Problemas de recuperação: Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

5.2 Segurança quanto às Pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos do BB.

i. Identificação das pessoas:

Todas as pessoas com acesso aos sistemas e informações, pertencentes ou em posse do BB, deverão ter uma única identificação (login). As exceções deverão ser devidamente documentadas e aprovadas pelo Comitê responsável.

ii. Declaração de Responsabilidade:

É um compromisso de responsabilidade direta do colaborador para com as informações, equipamentos e outras propriedades do BB a ele confiadas, devendo ser lida e assinada quando de sua admissão.

Este conceito deve ser utilizado também para prestadores de serviço e clientes:

- Prestadores de Serviço: a declaração de responsabilidade deve ser uma das cláusulas do contrato.

- Clientes: a declaração de responsabilidade deve ser uma das cláusulas do termo de adesão ao produto - ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

A declaração de responsabilidade deve ser lida e assinada, dentro dos formatos aceitos e homologados em meio físico ou eletrônico, por todos os colaboradores antes de ser arquivada na respectiva pasta funcional. O Departamento de Recursos Humanos deve garantir que todos os colaboradores tenham sua declaração de responsabilidade assinada.

5.3 Segurança Lógica de Computadores, Redes e Sistemas Aplicativos

Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse do BB.

.

Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão etc.

Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação.

Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários.

As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

i. Normas para segurança lógica de computadores e redes:

Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada negócio, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles.

Cada gestor da informação é responsável por definir e manter atualizados os perfis de acesso aos seus aplicativos visando o acesso mínimo necessário para a execução das atividades bem como evitar conflitos de interesse.

ii. Administração do acesso aos sistemas aplicativos:

As informações devem ser analisadas pelos respectivos gestores da informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis e alçadas.

Os sistemas aplicativos devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

iii. Administração do acesso de usuários:

Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários, respeitando normas internas do BB.

iv. Controle de acesso a computadores e redes:

Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto.

O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

Os ambientes de produção, homologação e desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

v. Normas para controle de acesso a computadores, redes e sistemas aplicativos:

Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;
- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);
- Os sistemas devem ser programados para nunca exibir a senha na tela;
- As senhas devem ser individuais e intransferíveis. A senha é de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;
- As senhas não devem ser triviais e previsíveis;
- Os tipos de caracteres utilizados para a formação da senha devem ser:

1. Letras maiúsculas;
2. Letras minúsculas;
3. Números;
4. Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ?!).

- As senhas deverão ter um tamanho mínimo de 08 (oito) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres

acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;

- Os sistemas devem prever um prazo para a expiração de senhas de no máximo 30 (trinta) dias;

- Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterá-la no primeiro acesso;

- As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de reutilização (mínimo de vinte e quatro senhas);

- Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito;

- Após um máximo de cinco tentativas consecutivas sem sucesso, os acessos devem ser bloqueados até que seja solicitado o desbloqueio do usuário;

- Uma vez aprovada, a senha deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto, um mesmo usuário não deverá utilizar simultaneamente mais de uma estação de trabalho.

vi. Monitoramento de uso e acesso aos sistemas aplicativos:

Todos os sistemas aplicativos deverão:

- Detectar tentativas de acesso não autorizado;

- Registrar eventos de entrada no sistema (login);

- Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas; e

- Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

vii. Processo de desenvolvimento de sistemas:

Os sistemas desenvolvidos deverão observar e seguir as boas práticas de mercado sobre desenvolvimento seguro a fim de mitigar riscos e

vulnerabilidades comumente exploradas nos sistemas. A aderência do processo deve ser realizada através de adequação de processos e/ou uso de tecnologias específicas para esse tipo de finalidade.

Adicionalmente, cabe à Segurança da Informação avaliar a necessidade de testes de segurança sobre qualquer sistema, seja interno, exposto na internet, hospedado fora da infraestrutura tecnológica do BB, desenvolvido internamente ou externamente.

5.4 Segurança no Acesso de Prestadores de Serviço

Este tópico visa estabelecer controles sobre recursos de processamento da informação da organização durante a execução de serviços por contratados externos.

Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. O que for acordado deve ser explicitado no contrato assinado.

É proibida a utilização de equipamentos próprios do prestador conectados à rede da organização sem a devida autorização escrita pela área de segurança da informação que deverá avaliar a necessidade através de justificativa técnica. Se for necessário deve-se segregá-los em uma rede própria e estabelecer um “firewall” para controlar os acessos.

Caso o prestador utilize softwares próprios em equipamentos da organização, deve-se apresentar documentação ou termo de responsabilidade garantindo direito de uso, que será mantido enquanto o software estiver instalado.

5.5 Segurança Física de Computadores

Este tópico destina-se aos usuários e administradores de computadores conectados ou não a uma rede.

O objetivo é garantir que as Instituições estabeleçam, administrem e utilizem computadores de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos.

i. Normas para segurança física de computadores:

Os meios de armazenamento considerados como mídias removíveis devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

Os computadores não ligados a uma rede, e que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

ii. Responsabilidade na segurança física de computadores:

A Ditec é responsável por elaborar e manter atualizado o inventário de hardware e software no Edifício Sede, Agências e Regionais.

A área de Segurança Patrimonial é responsável por garantir o controle sobre o acesso físico aos equipamentos.

5.6 Padrões para Instalação de Computadores

O padrão de instalação para os computadores deve atender a todas as normas estipuladas pelo BB.

A estrutura para manter a segurança física deve obedecer aos padrões de segurança geral do Conglomerado e adequar-se às seguintes especificações:

i. Sala:

- As dimensões do local devem ser suficientes para a instalação dos equipamentos;
- A disposição dos cabos lógicos e de energia deve ser adequada de forma que as pessoas possam transitar livremente;
- As entradas de ar (ventilação) dos equipamentos não devem estar obstruídas;
- Os equipamentos devem estar em locais firmes que evitem trepidações.

ii. Refrigeração e qualidade do ar:

- Climatização deve ser conforme especificado pelo fabricante;
- O ambiente deve estar livre de poluição por poeira, gases ou fumaça a fim de evitar que a poluição penetre nos equipamentos, possibilitando a quebra dos mesmos ou falhas de processamento.

iii. Rede elétrica:

- É recomendável que exista aterramento exclusivo para os equipamentos e que os pontos de energia sejam estabilizados;
- Para os equipamentos considerados críticos recomenda-se a instalação de UPS (Uninterruptable Power Supply), fonte alternativa de alimentação de energia que é ativada automaticamente quando ocorre a queda na alimentação de energia;
- Os equipamentos devem ser instalados em uma rede elétrica seguindo os padrões recomendados pelos fabricantes; e
- As instalações elétricas devem sofrer revisões periódicas.

iv. Equipamentos Contra Incêndio:

- Devem existir equipamentos de combate a incêndios adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível sinalizado e desobstruído, e ser de conhecimento de todos os colaboradores; e

- Devem existir equipamentos de prevenção de incêndios adequados, tais como detectores de fumaça e alarme contra incêndio, devendo existir um meio eficiente de aviso a um órgão de combate a incêndio.

v. Iluminação:

- A iluminação deve ser adequada, evitando a incidência direta da luz do sol sobre os equipamentos.

vi. Precauções quanto à disponibilização das mídias de armazenamento:

- Quando as mídias removíveis de armazenamento forem vendidas, devolvidas ao fabricante ou enviadas para manutenção, as informações nelas contidas devem ser destruídas antes de deixar as dependências do BB.

Importante ressaltar que nos meios magnéticos não é suficiente apagar os dados, devendo-se executar um programa que realmente os destruam.

5.7 Segurança Física dos Servidores de Rede

Este item destina-se aos usuários de sistemas operacionais com características de servidores de rede.

O objetivo é garantir que o Conglomerado administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

i. Normas para segurança física dos servidores de rede:

As mídias removíveis de armazenamento devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

ii. Responsabilidades na segurança física dos servidores de rede:

A Ditec é responsável por:

- Elaborar e manter atualizado o inventário de hardware e software; e
- Garantir o controle de acesso físico aos equipamentos.

5.8 Padrões para Instalação dos Servidores de Rede

O padrão de instalação para servidores de rede deve atender a todas as normas estipuladas pelo BB.

A estrutura para manter a segurança física dos equipamentos de uma rede deverá adequar-se às mesmas especificações utilizadas para a instalação de computadores com as seguintes especificações adicionais:

i. Sala:

- Fechada, mas permitindo a visualização interna do ambiente, com divisórias até o teto.

ii. Rede elétrica:

- Nos servidores, fazer uso de equipamento UPS (homologado por técnicos autorizados) com nobreak; e
- É necessário que exista aterramento exclusivo para os equipamentos e estabilização dos pontos de energia elétrica.

iii. Equipamentos Contra Incêndio:

No caso das salas de servidores e/ou telecomunicações deve-se considerar o uso de dispositivos automatizados de combate a incêndios, agentes extintores limpos como gases e outros recursos específicos a este tipo de ambiente.

iv. Precauções quanto à disponibilização dos meios de armazenamento:

As manutenções mídias removíveis, realizadas no próprio local, devem ser acompanhadas pelo responsável da área.

5.9 Backup e Restore

Este tópico se destina aos usuários e administradores locais das empresas do BB, visando administrar e utilizar os recursos de informática de maneira segura, tomando medidas adequadas que garantam recursos alternativos de processamento na eventualidade de perda dos dados, softwares ou sistemas.

Para a elaboração de um plano de backup devem ser considerados os “backups” do tipo Operacional, Contingencial e Histórico.

Backup Operacional: é a cópia das informações estratégicas que fazem parte do quotidiano do usuário e que são importantes para garantir a continuidade de suas tarefas. Destina-se à recuperação instantânea.

Backup Contingencial: é a cópia das informações sensíveis, softwares e sistemas vitais à continuidade dos negócios do BB e deve ser guardado em local externo. Destina-se a permitir a recuperação em situações catastróficas.

Backup Histórico: é a cópia das informações determinadas por exigência legal ou normas internas e deve ser guardado em local externo.

i. Normas para Backup/Restore:

A elaboração do plano de Backup/Restore deverá levar em consideração os aspectos abaixo:

- Os períodos de atualização dos dados; e
- Particularidades de cada instituição do BB.

As informações consideradas imprescindíveis devem estar presentes nas rotinas de backups operacional e contingencial, levando-se em consideração a periodicidade de atualização dos dados.

As informações devem estar sujeitas às rotinas de backups operacional e contingencial conforme critério definido pelo usuário.

As cópias de backup devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas.

Deve-se manter uma cópia do plano de Backup/Restore juntamente com o backup contingencial.

Devem ser realizados testes de restore periodicamente, mantendo evidências do último teste realizado.

Devem ser mantidas, no mínimo, as duas últimas versões dos backups operacional e contingencial. Para os backups históricos, a quantidade de versões será determinada por exigência legal ou norma interna.

ii. Plano de Backup/Restore - Conteúdo:

Abrangência: Relação dos arquivos e diretórios a serem copiados no processo de backup.

Periodicidade: Intervalo de tempo após o qual o sistema é submetido à rotina de backup.

Retenção: Prazo pelo qual os backups devem ser mantidos.

Procedimentos: Descrição dos procedimentos de backup.

Quantidade de cópias: Número de cópias de backup, locais e meios de armazenamento.

Identificação dos meios de armazenamento: Os meios de armazenamento devem estar devidamente identificados.

Registro do uso das cópias de backup: A manipulação dos meios de armazenamento deve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações.

Manutenção das cópias Backup: Quando o prazo de retenção for superior ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dos dados em novo meio, periodicamente.

A responsabilidade do backup/restore é do administrador local ou da área técnica elaborar, manter e documentar o plano de backups e garantir a execução de seus procedimentos.

5.10 Testes regulares de armazenamento e recuperação de dados

Todo e qualquer meio de armazenamento assim como os procedimentos de recuperação devem ser regularmente testados, garantindo sua efetividade. A periodicidade deve ao menos ser uma por ano, a ser determinada pelo Comitê de Segurança, considerando o nível de risco do negócio. Devem ser mantidas evidências do sucesso dos testes feitos.

5.11 Pirataria

Este item se destina a todos os usuários e administradores de servidores de redes ou computadores, inclusive portáteis, conectados ou não a uma rede e tem como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de softwares dentro das instalações das empresas do BB.

i. Normas contra pirataria:

A quantidade de licenças de softwares não pode ser inferior à quantidade de softwares instalados, mesmo que para fins de testes ou treinamentos, a não ser que esta situação esteja coberta contratualmente.

Não é permitido duplicar software de propriedade do BB a não ser com a finalidade de cópia de segurança e mesmo assim, somente por pessoas autorizadas. Uma licença de uso de software do BB só pode ser instalada em computadores do BB.

Todo software de demonstração deve vir acompanhado de uma autorização formal da empresa proprietária, indicando onde pode ser instalado e por quanto tempo.

É proibida a utilização e reprodução não autorizada de manuais, livros, revistas, periódicos protegidos por direitos autorais.

ii. Responsabilidades quanto à pirataria:

- Verificar se o software a ser instalado é original, conferindo o mesmo com as devidas licenças de uso;
- Se a instalação foi autorizada pelo Responsável Administrativo da Unidade, verificar se o software foi previamente homologado pela equipe técnica; e
- Implementar mecanismos que dificultem a pirataria através de qualquer meio.

5.12 Utilização Segura de Hardware e Software

Todos os equipamentos portáteis (notebooks, laptops, netbooks, ultrabooks, tablets e smartphones) que tenham capacidade de armazenamento de dados, devem seguir os princípios de segurança contidos nesta política. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, os dados devem ser criptografados ou ter seu acesso protegido por senha.

É proibida a utilização de qualquer equipamento particular na rede corporativa do Banco do Brasil.

É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de “softwares” ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas ou por terceiros.

5.13 Acesso à Internet

A Internet abrange vários aspectos e serviços (websites de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades de negócio. A restrição a websites não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede de Internet.

O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (Nome do usuário e endereço acessado são informações obrigatórias no rastreamento).

O usuário deve restringir o acesso aos websites ainda não bloqueados que possam manchar a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (Webmail, jogos etc.). Deve também comunicar o endereço eletrônico desses websites à área de Segurança da Informação, que deverá realizar seu imediato bloqueio.

O acesso à Internet deve ser feito através de "Servidores de Acesso" protegidos por sistemas de Firewall. Quando for necessário o acesso utilizando uma segunda conexão através de modem ou rede wi-fi, a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada. Os requisitos de segurança destas máquinas em particular devem ser respeitados (antivírus e firewall local). Casos específicos como esses devem ser aprovados pelos responsáveis da área de Segurança da Informação.

5.14 Acesso ao Correio Eletrônico

O BB disponibiliza aos seus colaboradores a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios.

As mensagens de correio eletrônico devem ser rastreadas, a fim de permitir o monitoramento para identificar o uso indevido da tecnologia.

6. Plano de continuidade do negócio

Um plano de continuidade do negócio deve garantir a recuperação dos processos críticos do BB quando da indisponibilidade do ambiente ou de quaisquer recursos que impossibilitem o desenvolvimento ou as operações das áreas de negócio.

É de responsabilidade de cada área envolvida no desenvolvimento dos negócios, elaborar, testar e implantar seus planos de contingência. Adicionalmente, o plano deve ser revisado e atualizado anualmente.

A definição de processos críticos de uma empresa ou área, obrigatoriamente, deve obedecer a critérios emanados pelos Diretores responsáveis pela instituição / área.

i. Pontos a serem observados no plano de continuidade do negócio:

Na elaboração de um plano de continuidade do negócio os pontos abaixo devem ser observados:

- As funções críticas devem ser identificadas e definidas;
- Traçar uma estratégia para recuperação de cada função crítica;
- Priorizar as funções críticas para ordenar sua recuperação;
- Identificar as atividades necessárias para recuperar cada função;
- Quantificar os recursos humanos e técnicos necessários ao cumprimento do plano;
- Documentar os processos críticos;
- Identificar os responsáveis pela recuperação de cada processo ou função;

- Ações para restabelecer a operação normal; e

- Identificar os recursos de backup (infraestrutura, hardware, software, sistemas aplicativos e telecomunicações).

ii. Revisões periódicas do plano de continuidade do negócio:

O plano de continuidade do negócio deverá sofrer revisões anuais a fim de identificar pontos que estiverem em desacordo com a situação atual. Deverão ser observados os pontos abaixo:

- Troca de fornecedores ou contratados;
- Alteração de endereços ou números de telefones;
- Mudanças nas prioridades de recuperação;
- Interdependência entre sistemas e aplicativos;
- Mudanças nas funções e nos processos críticos de negócio;
- Mudanças nas práticas operacionais; e
- Atualização da relação de colaboradores críticos.

7. Plano de Conscientização de Segurança da Informação

Um plano de conscientização da segurança da informação deve ser elaborado e executado para atingir o seguinte objetivo:

"Garantir que a Segurança da Informação não seja apenas conhecida, mas compreendida por todos os colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de Segurança de forma a atingir uma melhor utilização e proteção à informação.".

As diretrizes básicas são:

- Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais do BB;

- Divulgação de diversos materiais e alertas referente a Segurança da Informação para colaboradores e clientes;

- Criação de procedimentos de aferição do nível de conhecimento dos usuários em geral;

- Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral; e

- Revisão periódica do plano, adequando as ações às novas necessidades, evitando torná-lo repetitivo.

8. Canais de Relacionamento com o Cliente

Os seguintes canais eletrônicos de relacionamento devem garantir a positivação de informações do cliente:

• Internet Banking e Aplicativo Móvel: através de CPF, senha de acesso e chave se segurança ou confirmação de informações de conhecimento pessoal do cliente.

• SAC: através de CPF e confirmação de informações de conhecimento pessoal do cliente.

• WhatsApp (corporativo): validação do número de telefone que originou a comunicação e confirmação de informações de conhecimento pessoal do cliente.

Observação: Esse canal não é utilizado para serviços transacionais e tem uso permitido apenas através de plataforma corporativa que possui controles de segurança.

Na utilização de mensagens de correio, a privacidade da informação deve ser preservada e a mensagem criptografada. Deve-se utilizar certificados que garantam a integridade da mensagem ou senhas em arquivos que devem ser transmitidas ao cliente por outro meio de comunicação.

Os canais de relacionamento também devem oferecer conteúdo educativo sobre precauções e cuidados a respeito de aspectos de segurança a fim de proteger acessos, contas e recursos dos clientes com o Banco do Brasil.

9. Plano de Resposta a Incidentes

É de responsabilidade da Unidade de Segurança Digital e da Informação – USD, publicar e revisar o plano de resposta a incidentes cibernéticos, esse plano deve conter cada etapa de cada tratativa a partir da identificação de um incidente. Seu objetivo é criar uma abordagem e conduta, minimamente necessária, em caso de um incidente cibernético na instituição.