Política de Segurança da Informação

Código: 13 - 01

1. INTRODUÇÃO

A informação é um importante ativo à operação das atividades comerciais e, para manter a vantagem competitiva no mercado, é um dos principais patrimônios do mundo dos negócios. Tal como os ativos da SAM BR, a informação deve ser adequadamente manuseada e protegida. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da SAM BR. Se não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos e prejudicar o crescimento e vantagem competitiva da SAM BR.

2. OBJETIVO

Descrever as regras e conceitos de Segurança da Informação e Cibersegurança, bem como os princípios e diretivas de segurança, autenticação e senha, direito de acesso, orientações para uso de Skype, e-mail corporativo, acesso remoto, uso de internet e planilhas eletrônicas. Aborda também as classificações da informação e Ciclo de Vida.

Esta política tratará os assuntos de forma genérica, devendo ser lida em conjunto com as políticas e procedimentos de acessos de rede Windows, sistemas e diretórios, e demais de Segurança da Informação do Banco Santander Brasil S.A. designado como “BSBR”.

3. ABRANGÊNCIA

Aplica-se a todos os funcionários, executivos, diretores e estagiários - doravante designados em conjunto como “Colaborador(es)” - da Santander Brasil Gestão de Recursos LTDA. (“SAM Gestão BR”, CNPJ: 10.231.177/0001-52) e Santander Brasil Asset Management DTVM S.A. (“SAM DTVM BR”, CNPJ: 10.977.742/0001-25) - doravante designadas em conjunto como "SAM BR". E no que couber ao Banco Santander Brasil S.A., PRODUBAN e demais prestadores de serviço.

4. NORMAS DE REFERÊNCIA

Emissor	Normas
BSBR	Segurança da Informação: Política de Segurança da Informação - Id 157884

5. DEFINIÇÕES/ CONCEITOS

5.1. SEGURANÇA DA INFORMAÇÃO

É a disciplina que concentra esforços contínuos à proteção dos ativos de informação. Para tanto, visa aos seguintes objetivos:

- **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);
- **Disponibilidade**: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

5.2. CIBERSEGURANÇA

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Cibersegurança é a disciplina que concentra os esforços para a proteção dos ativos de informação em um ambiente virtual, ou seja, o ambiente resultante da interação de pessoas, softwares e serviços por meio de dispositivos tecnológicos e redes conectadas a estes dispositivos.

5.3. GESTOR DA INFORMAÇÃO (OWNER/PROPRIETÁRIO)

O gestor da informação (esteja ela armazenada em sistema ou diretórios de rede) deve ser um representante da área responsável por todo o ciclo de vida da informação.

6. DESCRIÇÃO DA POLÍTICA

A Política de Segurança da Informação é um conjunto de diretrizes, normas e procedimentos que tem a finalidade de estabelecer os objetivos de segurança da informação apropriada ao contexto de negócios.

6.1. PROTEÇÃO DA INFORMAÇÃO

Toda informação gerada ou desenvolvida nas dependências da SAM BR constitui ativo desta, 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 à finalidade à qual foi autorizada pelo gestor da informação.

É diretriz que toda informação de propriedade da SAM BR seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

6.2. RESPONSABILIDADES

Todo Colaborador, prestador de serviços, parceiro ou visitante, deve observar e seguir as políticas, padrões, procedimentos e orientações estabelecidos pela SAM BR.

É imprescindível a compreensão do papel da segurança da informação em suas atividades diárias. Todas as atividades executadas pela SAM BR devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação à segurança da informação.

As áreas de Compliance, Risco e ITOP são responsáveis pela definição de políticas e padrões que apoiem a todos na proteção dos ativos de informação e auxiliem na resolução de problemas relacionados ao tema.

6.3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

6.3.1. Proteção dos Sistemas de Informação e Demais Recursos

As informações e os sistemas de informação, diretórios de rede e bancos de dados devem ser classificados segundo seu nível de confidencialidade. Também devem ser tratados em conformidade com sua classificação durante posse e comunicação a outros colaboradores e público em geral.

Todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem possuir um gestor responsável pela definição de sua correta utilização e segurança, dentre outras responsabilidades, deve autorizar o acesso à informação e ao sistema e garantir que seu uso esteja de acordo com a Política de Segurança da SAM BR.

6.3.2. Acesso a Sistemas e Recursos de Rede

O colaborador é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes do uso destes poderes. O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas pelo gestor responsável e de acordo com a necessidade mínima ao cumprimento de suas funções.

Para sistemas e diretórios, a SAM BR continuará utilizando as políticas de Segurança da Informação do BSBR que determina que semestralmente, os acessos concedidos devem ser revistos pelos respectivos gestores de recursos de informação.

O acesso e o uso de recursos de rede, incluindo mensagens eletrônicas e acesso à Internet, devem estar alinhados às atividades de negócio da SAM BR. O uso esporádico e responsável para fins pessoais é permitido, à medida que não interfira no trabalho do colaborador ou implique conflito de interesses da SAM BR.

A utilização de recursos de rede, sistemas e outras fontes de informação é monitorada pelo BSBR por meio de registros (logs/trilhas de auditoria) e outros mecanismos. Essas informações podem ser coletadas e utilizadas, a critério da SAM BR, à execução de investigações internas ou para atendimento de medidas judiciais, sem aviso prévio às pessoas envolvidas, respeitando-se, porém, a privacidade dos colaboradores.

6.3.3. Utilização dos Recursos de Informação

Apenas os equipamentos e softwares disponibilizados e/ou homologados pelo BSBR podem ser instalados e conectados à rede da SAM BR. Todos os ativos de informação devem ser devidamente guardados, inclusive documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após sua cópia, impressão ou utilização.

6.4. VIOLAÇÃO DA POLÍTICA, NORMAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

As violações de segurança devem ser informadas ao gestor imediato e, simultaneamente, à área de Segurança da Informação. Toda violação ou desvio é investigado para determinação de medidas necessárias, visando à correção da falha ou reestruturação de processos.

Os princípios de segurança estabelecidos nesta política possuem total aderência da Alta Administração da SAM BR e devem ser observados por todos na execução de suas funções. A não conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita funcionários e estagiários a ações disciplinares e trabalhistas e, aos prestadores de serviços e parceiros de negócios, inclui-se a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir.

6.5. DIRETIVAS DE SEGURANÇA DA INFORMAÇÃO

Diretivas de Segurança da Informação regem a conduta e o comportamento em relação a temas de segurança, detalhando a Política de Segurança da Informação e embasando a criação de outras políticas e procedimentos.

De acordo com necessidades específicas decorrente da criticidade das informações com que lidam com leis, resoluções e regulamentos de Órgãos Governamentais e/ou Reguladores, determinadas áreas podem ter regras mais restritivas como áreas separadas por regulamentos internos e externos de Compliance.

6.6. AUTENTICAÇÃO DE SENHA

6.6.1. *Login* e Senha de Acesso

O colaborador é responsável por todos os atos executados com seu identificador (*login*/sigla de acesso), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Os colaboradores devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum. Ou seja, não conta-la a ninguém e não anotá-la em papel;
- Alterar a senha sempre que existir qualquer suspeita de seu comprometimento;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso de seu equipamento por outras pessoas enquanto este estiver conectado/"logado";
- Bloquear o equipamento ao se ausentar (Ctrl + Alt + Del).

6.6.2. *Login* Simultâneo

Não é permitida a conexão à rede com a mesma sigla em mais de um equipamento ao mesmo tempo, pois deve existir um mecanismo de bloqueio automático de conexões simultâneas.

O uso de até 3 *logins* simultâneos pode ser liberado, excepcionalmente, desde que solicitado e aprovado pelo respectivo superintendente (nível N12, equivalente ou superior) do solicitante, confirmando a necessidade conforme um dos casos abaixo:

- Colaboradores de áreas de Suporte Técnico (Produban);
- Colaboradores de áreas de Operação (Produban);
- Colaboradores da área CORO - *Chief Operation Risk Officer* (Produban);

- Colaboradores de áreas que necessitam de acesso a *feeders*: Bloomberg, Reuters, Broadcast etc. (exemplo: equipes específicas de *Global Corporate Banking* (GCB) que usam tais *feeders*). Os *feeders* que serão utilizados devem estar especificados na solicitação.

Ressaltamos que o *login* simultâneo, pelo caráter excepcional, só deve ser usado para cumprir as finalidades pelas quais foi liberado, e nunca como meio de compartilhamento de acessos ou qualquer outro fim não declarado nesta política (exemplo: uso de salas de reunião, sem desconexão da estação de trabalho).

O uso do *login* simultâneo fora dos casos e condições especificadas acima e na solicitação é passível de monitoramento, exclusão sem comunicação prévia e sujeita o colaborador a sanções.

6.7. DIREITO DE ACESSO - AUTORIZAÇÃO

O colaborador é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que lhe são atribuídos, sendo intransferíveis.

A solicitação de acesso à informação deve decorrer da necessidade funcional do colaborador e deve ser autorizado pelo proprietário/gestor do ativo para cada colaborador ou grupo de colaboradores, com direitos e perfis de acesso restritos aos efetivamente necessários à função.

A autorização por alçada competente é necessária para que haja as respectivas atribuições de direitos, de acordo com o processo formal de concessão de acessos.

6.8. ACESSO FÍSICO

Os colaboradores devem conhecer e cumprir as normas de acesso a cada tipo de dependência física da SAM BR, conforme política de Compliance “06 - 04 - Política e Procedimento de Acesso Físico da SAM BR”.

Todos os prédios com operações devem ter controles que assegurem acesso restrito aos Colaboradores autorizados, incluindo ambientes externos, localizados em empresas parceiras. Deve existir mais restrição nas áreas de segurança que requerem um nível de controle mais elevado (exemplo: Centros de Processamento de Dados (CPDs) e áreas onde informações altamente confidenciais são tratadas).

6.9. INVENTÁRIO DA INFORMAÇÃO

Os inventários dos principais ativos de informação (exemplo: *hardware*, servidores, *desktops*, *laptops*, telefones (fixos), *smartphones*, *tablets*) de propriedade da SAM BR associados aos devidos sistemas que

rodam ou suportam e aos respectivos proprietários/gestores, devem ser elaborados e mantidos pela Produban.

6.10. CLÁUSULAS DE CONFIDENCIALIDADE

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam a alertar e responsabilizar o colaborador de que o acesso e o manuseio de informação devem restringir-se ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

Colaboradores: em complemento as cláusulas que integram o contrato de trabalho do RH , os colaboradores assinam o "Termo de Conhecimento e Aceite do Código de Ética" com as seguintes previsões: "Declaro, para todos os fins, ter total conhecimento da responsabilidade de tratar com confidencialidade o acesso e o manuseio de qualquer informação resultado do exercício da minha função ou processo ao qual tenho acesso, comprometendo-me a utilizá-la somente para o propósito profissional designado" e "Declaro, para todos os fins, ter total conhecimento de que todo o produto resultante do meu trabalho (sistema, documentação, metodologia, dentre outros) é propriedade da SAM BR.".

6.11. DIREITOS DE PROPRIEDADE

Todo produto resultante do trabalho dos colaboradores (sistema, documentação, arquivos, metodologia, dentre outros) é propriedade da SAM BR.

6.12. CONFIGURAÇÃO E USO DOS EQUIPAMENTOS

Os equipamentos disponibilizados pela SAM BR devem ser classificados com o mesmo nível de segurança da informação que armazenam. O uso dos equipamentos é restrito aos negócios e atividades da SAM BR.

Equipamentos não mais utilizados pelas áreas devem ser recolhidos. O gestor deve seguir os procedimentos de acordo com o manual 14 - 02 - Governança de Tecnologia da SAM BR.

As medidas de segurança existentes incluem, dentre outras, software antivírus, a extração periódica de cópias de segurança (backup) dos arquivos de dados em rede e controle específico para prevenir o acesso não autorizado ao equipamento.

A informação classificada como confidencial, que esteja armazenada nesses equipamentos, deve ser mantida de forma criptografada.

Os equipamentos da SAM BR devem ser bloqueados automaticamente por inatividade após 10 minutos (exemplo: caso um funcionário se ausente do equipamento por 10 minutos, automaticamente será ativada a tela de "*Computer Locked*" (Ctrl Alt Del) e a proteção de tela.

Exceção aos colaboradores da área de investimentos que, por necessidade e desempenho das atividades, não possuem essa funcionalidade de bloqueio de telas ativadas.

A) Privilégios de Administrador Local e "*Power User*"

O privilégio especial de administrador local ou *power user* pode ser concedido a funcionários e prestadores de serviços do Santander, Isban e Produban, em alguns casos específicos, mediante solicitação e análise da área de Segurança da Informação.

As solicitações devem ser aprovadas por níveis equivalente ou superior a superintendente executivo da área do beneficiário.

Somente áreas de manutenção e suporte técnico da Produban podem ter acesso administrativo a todo o parque de estações de trabalho, por padrão, em decorrência das atividades exercidas.

Ressaltamos que o privilégio de *power user* ou administrador local, pelo seu caráter excepcional, só deve ser usado para cumprir as finalidades pelas quais foi liberado, e nunca como meio de instalar software não homologado ou sem licença, parar serviços ou desinstalar ferramentas, burlar controles e políticas, ou qualquer outro fim não declarado nesta política e na justificativa dada na solicitação.

O uso destes privilégios fora dos casos e condições especificadas acima e na solicitação é passível de monitoramento, exclusão sem comunicação prévia e sujeita o colaborador a sanções.

B) Equipamentos particulares/privados

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, podem ser usados conforme elegibilidade da SAM BR.

C) *Notebook* e dispositivos portáteis

Todas as pessoas que utilizam notebook e/ou dispositivos portáteis devem observar o seguinte:

- Tomar as medidas para mitigar o risco de roubo ou furto do notebook. Não deixá-lo desacompanhado no escritório ou em qualquer local público. Se precisar se ausentar, tenha certeza de que ele está

preso à mesa com um cabo de segurança ou trancado com chave em um armário, fora da visão de outras pessoas;

- Caso viaje de carro, assegure-se que o notebook não está à vista. Coloque-o no porta-malas;
- Se forem armazenadas informações confidenciais no disco rígido ou em dispositivo portátil, devem ser tomadas medidas de segurança adicionais. Contatar a área de Segurança da Informação (caixa corporativa "Seg.Informacao - Institucional") para mais informações, caso seja necessário;
- Quando viajar de avião, transportá-los como bagagem de mão;
- Não utilizá-los em locais públicos onde outras pessoas possam visualizar a tela;
- Os colaboradores devem seguir as regras locais de segurança, quando acessarem Internet:
- Verificar se o antivírus está sendo atualizado semanalmente. Caso tenha dúvida a respeito, contatar a área de Suporte Técnico através de abertura de chamado no EntryPoint na Intranet da SAM;
- Se o notebook for roubado ou perdido, avisar imediatamente o seu gestor e as áreas de Compliance e Tecnologia da SAM através de suas caixas corporativas informadas nos contatos desta política.

Os mesmos princípios são aplicáveis a outros computadores portáteis, tais como: dispositivos móveis, iPhone, iPad, BlackBerry.

D) Extensões de Arquivo não Autorizadas

Há categorias/extensões de arquivos que são potenciais portadores de código malicioso ou que podem permitir acesso indevido e vazamento de informações. Desta forma, é proibido:

- Navegar por sites externos que contenham estes tipos de arquivos;
- Efetuar download (copiar determinados programas, músicas etc.) a partir da Internet e dispositivos externos (CDs, DVDs, pen drives etc.);
- Armazenar nas estações e servidores da SAM BR e/ou;
- Receber por e-mail tais tipos de arquivos.

Arquivos cujo *download*, recebimento e armazenamento são proibidos. O bloqueio automático existente no AntiSpam deve impedir o tráfego desses tipos de arquivo por e-mail.

Por outro lado, há áreas que necessitam encaminhar alguns tipos de arquivos - notadamente arquivos de mídia (wmv, mp3, wav, etc.) para conhecimento, análise, tratamento ou arquivamento por parte de áreas internas da SAM BR, por motivos de negócio e como parte do fluxo de trabalho acordado.

Para estes casos, a liberação da troca de e-mails com esses tipos de arquivos pode ser concedida pela Produban, mediante solicitação, justificativa de negócio e aprovação por superintendente (mínimo N12, equivalente ou superior) da área demandante.

Para casos que envolvam projetos de tecnologia e sistemas formalmente abertos e aprovados, a liberação do bloqueio no ambiente envolvido deve ser concedida pela Produban quando houver a necessidade de transferência, cópia ou gravação de arquivos com extensões potencialmente nocivas, mas que fazem parte de algum componente ou software do pacote ou solução do projeto.

6.13. CORREIO ELETRÔNICO (E-MAIL)

Para troca de mensagens (e-mails) relacionadas à funções de trabalho na SAM BR, deve ser usado somente o sistema padrão de e-mail corporativo.

Os recursos de correio disponíveis para troca de mensagens devem ser usados pelos colaboradores para finalidades de negócios, no auxílio ao desempenho das funções organizacionais. E-mails enviados de fontes externas não são seguros, a menos que sejam criptografados ou digitalmente assinados.

O uso de e-mail para assuntos de caráter pessoal é permitido, desde que não afete os interesses da SAM BR ou a produtividade do Colaborador no exercício de suas funções. A eventual recepção de mensagens de correio dessa natureza deve ser apagada logo após a leitura. E-mails de origem desconhecida ou com arquivos anexados sem que tenham sido solicitados também devem ser descartados, por apresentarem riscos de infecção por vírus, etc. Estes casos devem ser encaminhados as áreas de Compliance e Tecnologia através de suas caixas corporativas para análise.

Cabe ao responsável avaliar e conceder, se julgar apropriado, o acesso aos recursos de e-mail por contratados que estejam prestando serviços à SAM BR.

E-mails enviados externamente representam a SAM BR e, portanto, devem ser autorizados e não apresentar opiniões divergentes da SAM BR.

A limitação do acesso aos recursos de e-mail é também prerrogativa da SAM BR quando considerar que esses recursos estão sendo utilizados de maneira inadequada ou afetando negativamente a disponibilidade e a produtividade dos demais serviços que se utilizam da rede.

Os colaboradores devem observar que os arquivos e outras informações a serem incluídos nos e-mails devem obedecer aos critérios de segurança estabelecidos ao nível de classificação da informação, incluindo a autorização do gestor da informação e a aplicação de criptografia para informação confidencial.

6.14. INTERNET

O uso da Internet destina-se unicamente à finalidade de negócios da SAM BR. Deve ser utilizado somente os *softwares* navegadores (*browsers*) homologados como padrão pela Produban (Internet Explorer e Google Chrome) para acesso e navegação em sites da Internet, que já vêm instalados nas máquinas. As configurações dos *browsers* não devem ser modificadas.

Não devem ser acessados sites que violam a lei, discriminatórios, com ameaças, difamatórios, abusivos, obscenos, com assédios, conteúdo ofensivo, ou possam afetar e danificar o sistema configurado no equipamento usado pelo colaborador.

A Segurança da Informação do BSBR reserva-se ao direito de bloquear o acesso a qualquer site considerado inapropriado e de manter logs de sites visitados para fins de auditoria.

A importação de arquivos de dados (*download*) e outras informações da Internet devem ser efetivamente necessárias e de origem conhecida e confiável para prevenir a recepção de vírus, códigos de programas maliciosos ou fraudulentos, *softwares* ilegais e outros materiais inapropriados.

Informações confidenciais não devem ser publicadas em sites.

A senha da rede; e-mail corporativo e demais sistemas da SAM BR não devem ser usados em sites na Internet, inclusive *Internet Banking*.

A limitação do acesso à Internet é prerrogativa do BSBR, quando considerar que esse recurso está sendo utilizado de maneira inadequada ou afetando negativamente a disponibilidade e produtividade dos demais serviços que se utilizam da rede de informática.

Para o envio de informações pela Internet, são aplicáveis as medidas de segurança estabelecidas ao nível da informação a ser enviada, o que inclui a autorização do gestor da informação e a aplicação de criptografia para informação confidencial.

6.15. COMMUNICATOR, LYNC, SKYPE

As ferramentas *Microsoft Lync* e *Skype for Business* são soluções para troca de mensagens instantâneas que agilizam a comunicação interna, aumentando a produtividade dos colaboradores. Todo conteúdo descrito nas ferramentas deve ser considerado uma conversa formal, na qual não devem ser utilizados termos vulgares ou inadequados que venham a desrespeitar o destinatário ou grupo.

Não é permitida a utilização de linguagem ou imagens impróprias ou obscenas (exemplo: depreciativa, assédio, difamatória, ameaçadora, pornográfica, discriminatória/preconceituosa ou ofensiva quanto a sexo, condição sexual, religião/crenças, etnia, opiniões políticas e demais aspectos pessoais) na redação de mensagens, bem como o engajamento em atividades ilegais, terroristas, fraudulentas, impróprias ou não-éticas. As conversas são gravadas, podendo o conteúdo trafegado ser inspecionado.

São elegíveis à concessão de uso do *Lync* ou *Skype for Business* todos os colaboradores e terceiros da SAM BR localizados nos escritórios, que utilizem *login*/sigla de rede no domínio AM e conta de correio eletrônico da SAM. As ferramentas não podem ser instaladas e utilizadas por colaboradores da área de Investimentos.

6.16. ACESSO REMOTO

O acesso a partir de local externo, viabilizado por telecomunicação, para colaboradores acessarem correio eletrônico e Intranet deve ser autorizado pelos respectivos gestores e avaliado a partir de solicitação formal.

O colaborador é responsável pelos arquivos e outras informações as quais tem acesso, aplicando as medidas de segurança apropriadas ao nível de classificação da informação. Isso inclui controle sobre as cópias impressas e a utilização de criptografia quando se tratar de informação confidencial.

O *token*, dispositivo de segurança usado como identificador de acesso para conexões VPN, deve ser guardado em lugar seguro. Não mantê-lo com o notebook ou com o seu computador.

Caso o *token* seja roubado ou perdido, avisar imediatamente o seu gestor e a área de Suporte. Em caso de furto ou roubo, comunicar imediatamente a Segurança Corporativa - Plantão 24 horas (11) 3249-1008.

6.17. MESA LIMPA

Ao se ausentar da mesa ou do escritório, os colaboradores não devem deixar qualquer informação confidencial à vista, seja em *pendrives*, CDs, DVDs ou equipamentos eletrônicos portáteis, dentre outros. Ao usar uma impressora coletiva, recolher o documento impresso o quanto antes, principalmente se for confidencial, inclusive no final do expediente.

6.18. CONVERSAS EM LOCAIS PÚBLICOS E TELEFONES MÓVEIS

Não discutir ou comentar assuntos confidenciais em locais públicos.

Não enviar mensagens de texto com informações confidenciais, nem com mensagens que possam ser consideradas ofensivas, ameaçadoras, difamatórias, obscenas ou de assédio, para celulares e outros dispositivos móveis. Utilizar as ferramentas de segurança que o celular oferecer, como o número PIN, e sempre mantê-lo em segredo. Se o celular que tenha acesso a informações corporativas for roubado ou perdido o colaborador deverá informar as áreas de Compliance e Tecnologia.

6.19. PREVENÇÃO CONTRA VÍRUS

BSBR possui controles para prevenir que vírus e outros tipos de *malware* entrem e espalhem-se nos sistemas e servidores. Os colaboradores devem seguir os passos abaixo:

- Avisar o *Help Desk*, a Segurança da Informação ou a equipe Respostas a Incidentes (csirt@santander.com.br) quando houver problemas ou suspeita de vírus;
- Não abrir *link* ou arquivo anexado a um e-mail vindo de pessoas desconhecidas ou não esperado;
- Não interromper as atualizações do *software* de antivírus. Caso seja usuário remoto, conectar-se à rede principal pelo menos uma vez por semana para obter as atualizações;
- Não instalar ou executar nenhum *software* ou dados recebidos de fontes externas, de discos ou vindos da Internet antes de certificar-se de que não há vírus.

6.20. DESCARTE DE INFORMAÇÕES

A SAM BR possui fragmentadoras de papel para destruir os documentos confidenciais. Em caso de dúvida na classificação, os documentos devem ser destruídos para prevenir o vazamento de informações.

Para descarte de CDs, DVDs, fitas de *backups*, HD externos, HD de dispositivos como impressoras departamentais, USB *Disk Storage* e outros tipos de mídias, primeiramente todas as informações confidenciais devem ser apagadas.

Após reuniões, seminários ou cursos, assegurar que todos os pertences foram levados da sala. Em caso de trabalho remoto (*home-office*), precaver-se para que não haja vazamento de informação.

6.21. *SOFTWARES* HOMOLOGADOS/LICENCIADOS

O *download*, a instalação e/ou o uso de *softwares* não licenciados e/ou homologados pelo BSBR são proibidos, incluindo os *softwares* obtidos ou comprados pelos próprios colaboradores para fins de trabalho ou pessoais nos equipamentos da SAM BR (servidores, estações, *notebooks*, *smartphones*, *tablets*). Exceções serão aprovadas conforme diretrizes do BSBR.

A utilização de *softwares* não homologados pode colocar em risco a segurança da rede, caso o programa contenha um vírus de computador ou outros códigos maliciosos que provoquem perda de desempenho ou interrupção de sistemas, ou ainda furto ou vazamento de informações confidenciais. Além disso, pode haver penalização ou danos à imagem se algum órgão regulador ou fiscalizador detectar a presença de tais programas em equipamentos da SAM BR.

Periodicamente a Produban realiza varreduras nos equipamentos para comparar os *softwares* instalados com as licenças disponíveis ou lista de *softwares* homologados.

A Produban deve estabelecer um mecanismo que possibilite a remoção de *softwares* que estiverem em desacordo com a lista e versões autorizadas.

A comunicação prévia ao colaborador é facultativa, sendo avaliada caso a caso, conforme eventuais necessidades de remoções imediatas para mitigação de riscos. DTI, Compliance e Segurança da Informação do BSBR podem ser envolvidos para ciência e apoio.

Somente a *End User Technologies* está autorizada a receber as solicitações e providenciar a instalação de *softwares* já homologados, com licença para uso corporativo. Para demandas de desinstalação de *software* sem licença ou não homologado, formalizar a solicitação através de chamado aberto na Intranet da SAM. As solicitações para providenciar a instalação de *softwares* já homologados, com licença para uso corporativo deverão ser endereçadas conforme políticas do BSBR.

Nos casos de demandas que afetem direta e primordialmente a segurança da rede, as demandas devem ser negadas, sem exceção. Nos casos de demandas que afetem compra/liberação de licenças, instalação de versões de *software* que não têm suporte ou estão fora do padrão de tecnologia, as demandas devem ser avaliadas conforme política do BSBR.

Adicionalmente, ressaltamos que os Colaboradores não devem copiar ou fazer e distribuir cópias de *softwares* licenciados pela SAM BR, incluindo qualquer documento associado.

6.22. *BLACKLIST* DE *SOFTWARES*

Blacklist de *softwares* é a lista de categorias de softwares não homologados cuja instalação e uso são proibidos por serem potencialmente nocivos à segurança da rede, máquinas e informações do BSBR. Desta forma, deve haver mecanismo de detecção e remoção de tais softwares em todas as máquinas da SAM BR, com comunicação ao responsável e respectivo gestor. A *blacklist* de segurança contempla as seguintes categorias de softwares proibidos:

- Quebra de senha;
- Construção ou disseminação de *malwares* (programas ou códigos maliciosos);
- Mensageria instantânea (*instant messaging* / chat);
- Compartilhamentos e acessos torrent e p2p de arquivos;
- Captura/análise de pacotes (sniffers)*;
- Varreduras (*scan*) de mapeamento e detecção de vulnerabilidades de rede*;
- Acesso e controle remoto*;
- Transferências de arquivos *(file transfer*) *;
- Acesso direto a bancos de dados*;
- Programação/desenvolvimento de sistemas*;
- Automação do tipo script que levem ao funcionamento de rotinas automatizadas - robôs*;
- Filmes e jogos que violam o direito de cópia.

*Exceto para equipes cujo uso seja inerente às atividades diárias ou autorizado.

Os responsáveis pelas máquinas com *softwares* proibidos estão sujeitos a sanções que podem envolver a perda de privilégios administrativos e comunicação da ocorrência às áreas de Ocorrências Especiais do BSBR, Compliance e RH da SAM BR.

6.23. ENVIO DE ARQUIVOS E INFORMAÇÕES A TERCEIROS/MEIO EXTERNO

O envio em qualquer formato de informações confidenciais da empresa para ambientes externos, independentemente da forma de envio ou destinatário, deve ser autorizado pela respectiva superintendência. Devem ser aplicados controles de segurança para proteção dos dados.

Vale ressaltar que a troca eletrônica de informações e de arquivos de dados com o meio externo deve ser baseada em procedimentos e controles de segurança consistentes com a classificação da informação envolvida (autorização do gestor, criptografia, logs de envio e recebimento).

6.24. LEIS E REGULAMENTOS

É responsabilidade da SAM BR conhecer e cumprir os requisitos legais, normas e padrões locais vigentes.

6.25. RECUPERAÇÃO DE DADOS DE HARD DISKS - HD (DISCO RÍGIDO)

Quando um HD apresentar problemas na leitura/acesso aos seus dados, a equipe de Suporte ao Funcionário (Help Desk) deve ser acionada através de chamado aberto no EntryPoint na intranet da SAM.

As equipes e respectivos níveis de atendimento efetuam todos os trâmites internos cabíveis no intuito de recuperar a maior quantidade possível de informações.

Não é permitido o envio de HDs para tentativa de recuperação de dados em empresas externas devido aos riscos envolvidos, tais como o de vazamento da informação recuperada em terceiros.

6.26. USO DE PLANILHAS ELETRÔNICAS

A) Definições

Planilhas eletrônicas são arquivos criados a partir do Excel para apoio aos processos de negócio das áreas da SAM BR, criadas e usadas com diversos tipos de finalidade e complexidade.

B) Riscos Associados

O uso de planilhas está sujeito a riscos e erros inerentes, tais como:

- Alteração ou destruição da informação por pessoas não autorizadas ou de forma acidental (acesso indevido ou indisponibilidade).
- Divulgação não-autorizada de informações, incluindo a perda ou roubo de informação (perda da confidencialidade).
- Erros de entrada, fórmulas ou processamento incorreto por falta de controles na criação, guarda e administração das planilhas (perda de integridade).
- Erros de link ou interface: Decorrentes da importação ou exportação de dados com outros sistemas

C) Controles

Caso uma área de negócios dependa recorrentemente de planilhas para o processamento ou controle de operações não suportadas pelos sistemas da SAM BR, o gestor da área responsável deve adotar controles para evitar que os riscos acima se materializem e tragam prejuízos à área ou à SAM BR como um todo.

Há duas classificações básicas de planilhas, em que cada qual requer um conjunto diferenciado de controles.

Caso seja imprescindível o uso de planilhas/banco de dados para processos ou informações consideradas críticas, o gestor da área responsável deve adotar medidas para evitar que os riscos tragam prejuízos à SAM BR.

As planilhas críticas devem ser armazenadas em diretórios com acesso restrito, em servidores da rede corporativa, seguindo os procedimentos padrões de backup (cópia de segurança).

D) Material de Apoio

Para apoiar os gestores, a Segurança da Informação do BSBR criou um guia com orientações e instruções de implantação de cada controle, tanto de planilhas críticas quanto das demais.

O guia, chamado Manual - Controles de Planilhas, está publicado na Intranet do BSBR > Institucional > Riscos > Segurança da Informação > Materiais de Apoio.

7. CLASSIFICAÇÃO DA INFORMAÇÃO E CICLO DE VIDA

Toda informação (em sistemas e demais ativos) deve ser classificada para permitir uma análise de riscos e a aplicação de controles de segurança adequados à sua importância (valor), requisitos legais ou regulatórios, sensibilidade e criticidade para a SAM BR, seus clientes e parceiros de negócio.

7.1. CRITÉRIOS GERAIS

É imprescindível que as informações sejam tratadas adequadamente em todo o ciclo de vida, assegurando o nível adequado de proteção. Os seguintes critérios devem ser considerados à definição da classificação dos dados:

- Requisitos legais e regulatórios para assegurar o gerenciamento e proteção dos dados;
- A necessidade de proteger dados pessoais (cadastrais e bancários/financeiros) - exigência de sigilo bancário - de clientes e de colaboradores;
- A proteção dos negócios e da posição da SAM BR no mercado para evitar perdas;
- O valor que a informação pode ter para outras empresas externas à SAM BR;
- O custo de recuperação/reconstrução dos dados em caso de alteração, corrupção ou exclusão;
- O impacto em caso de uso de dados corrompidos ou incorretos.

Qualquer informação exigida por lei ou tribunal, autoridade governamental ou reguladora, ou por força de contrato celebrado e reconhecido entre a SAM BR e terceiros só pode ser divulgada após parecer da área Jurídica da SAM BR.

A classificação da informação deve ser periodicamente reavaliada. Essa periodicidade deve ser definida pelos gestores da informação (aqueles que forem proprietários da informação, ou seja, gestor do sistema, do diretório, etc.). Recomenda-se que essa reavaliação seja feita pelo menos a cada 6 meses.

7.2. CATEGORIAS E MODELOS DE CLASSIFICAÇÃO

Os sistemas e ativos de informação armazenados ou processados no CPD devem ser classificados segundo os critérios confidencialidade, integridade e disponibilidade.

Os demais ativos de informação utilizados pelos usuários finais no dia a dia, devem ser classificados segundo o critério de confidencialidade.

7.2.1. Confidencialidade

A SAM BR adota três categorias segundo a confidencialidade:

- Confidencial (crítica);
- Uso Interno (sensível);
- Público (não sensível).

A) Informação Confidencial

As informações que necessitam de sigilo absoluto devem ser protegidas de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las sempre que necessário. Exigem todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo deste tipo de informação trazem grandes prejuízos à SAM BR, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou danos à imagem da SAM BR, podendo levar à extinção das operações ou prejuízos graves ao crescimento. Exemplos de informação Confidencial:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG, etc.), situação financeira e movimentação bancária;
- Informações sobre produtos e serviços que revelem vantagens competitivas frente ao mercado;

- Todo o material estratégico da SAM BR (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Declarações de salários e projeções, bem como quaisquer informações da SAM BR que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
- Todos os tipos de credenciais de acesso (usuários, senhas, frases, etc.) a sistemas, redes, estações de trabalho, dispositivos móveis e outras informações utilizadas na verificação e autenticação de identidades. Estas informações são pessoais e intransferíveis e não devem ser compartilhadas, sob pena de sanções administrativas.

B) Informação de Uso Interno

As informações de uso e acesso restrito aos colaboradores não devem ser divulgadas fora da SAM BR e, no caso de serviços contratados junto a parceiros de negócio, não devem sair do escopo, fluxo operacional e acessos autorizados. Este tipo de informação inclui atividades, processos e material exclusivo da SAM BR, sendo que a divulgação ao público em geral provoca danos em pequena ou média escala. Exemplos de informações de Uso Interno:

- Relatórios, boletins, pareceres, folhas de trabalho, planilhas e correspondências internas de natureza não confidencial;
- Informações contidas em sistema, mensagens eletrônicas e processos de trabalho que são utilizados por colaboradores quando exercem as funções na SAM BR;
- Informações utilizadas fora das dependências da SAM BR, relacionadas à atividade de trabalho e de natureza não confidencial.

C) Informações Públicas

São informações divulgadas aos meios públicos, sem distinção. Exigem esforços mínimos de segurança. Há um fluxo de processos determinado para a liberação das informações ao público. Em geral, a divulgação em larga escala é incentivada e benéfica à SAM BR.

Exemplos de informação pública: folhetos comerciais e resultados financeiros divulgados ao mercado.

7.2.2. Integridade

A SAM BR adota duas categorias segundo a integridade:

- Controle de Integridade (nível crítico ou sensível): quando são necessárias medidas adicionais para assegurar a integridade da informação, que tem que ser precisa e completa;
- Sem controle de integridade (não sensível): quando não são necessárias medidas para assegurar a integridade.

7.2.3. Disponibilidade

A SAM BR adota três categorias segundo a disponibilidade:

- Crítica: quando a indisponibilidade de um ativo, inclusive for um curto período (inferior a um dia), implique um risco severo ao negócio;
- Média (sensível): quando a indisponibilidade de um ativo, superior a um dia e inferior a uma semana, possa gerar risco significativo ao negócio;
- Baixa (não sensível): quando a indisponibilidade possa prolongar-se por mais de uma semana sem causar nenhum risco significativo ao negócio.

7.3. CICLO DE VIDA DAS INFORMAÇÕES

Toda informação possui um ciclo de vida, desde sua criação até o descarte. Cada colaborador deve ter consciência da importância de cada ativo de informação e tratá-lo conforme cada etapa do ciclo:

- **Geração**: toda informação é gerada com a classificação mínima de Uso Interno até passar pela avaliação do gestor da informação e rotulagem para tratamento específico;
- **Armazenamento**: o armazenamento, tanto físico como lógico das informações, deve seguir os controles definidos pelo gestor da informação com apoio nas medidas tecnológicas disponibilizadas pela SAM BR;
- **Cópia e Transferência**: de acordo com a classificação atribuída, o tratamento de cópias e transferência da informação deve controlar a exposição, a divulgação e destinatários;
- **Utilização**: o acesso às informações ser protegido pelas regras de acesso definidos pelo gestor, restringindo o público autorizado, a permissão concedida é de uso pessoal e intransferível e, caso seja necessário compartilhar, deve seguir a regra conforme a classificação atribuída;
- **Destruição**: quando a informação torna-se desnecessária, a destruição e o descarte devem seguir diretrizes da SAM BR;

- **Perda ou Roubo**: a divulgação de informações em ambiente público deve ser controlada em caso de roubo ou suspeita de perda de informações. O gestor e a área de Segurança da Informação devem avaliar os impactos, danos ou riscos e definir o plano de ação para tratamento.

7.4. DADOS DE EMPRESAS TERCEIRAS

Todas as informações recebidas de empresas externas à SAM BR devem ser tratadas de acordo como foram definidas por estas empresas. Caso nenhum critério tenha sido especificado, devem ser utilizados os procedimentos citados nesta política.

7.5. RESPONSABILIDADES

7.5.1. Gestor da Informação (*Owner*/Proprietário)

As principais responsabilidades e direitos do gestor da informação são:

- Estimar o valor da informação para a SAM BR;
- Classificar a informação de acordo com os critérios definidos;
- Decidir o nível de controle necessário para as informações;
- Definir critérios para concessão de acesso às informações, quando requerido;
- Receber e avaliar solicitações de liberação de dados para terceiros, quando requerido.

7.5.2. Usuário da Informação

Todos os usuários podem ter autorização para adicionar, excluir, modificar ou ler a informação. Para obter o perfil de usuário, o gestor da informação deve aprovar ou reprovar tais acessos. Suas principais responsabilidades são:

- Utilizar as informações apenas para as finalidades dos negócios;
- Seguir os controles definidos pelas regras internas e externas ou políticas.
- O usuário deve possuir acesso à leitura ou processamento de dados, e estas autorizações devem ser definidas nos ambientes de tecnologia e sistemas, de acordo com a permissão liberada ao usuário.

7.5.3. Custodiante da Informação

Os custodiantes da informação são as pessoas e áreas que proveem os serviços de processamento para as áreas da SAM BR. Possuem autoridade dada pelo gestor da informação para tal tarefa. Os custodiantes não possuem acesso aos dados para realizarem suas tarefas, mas para gerenciá-las, o que pode incluir o processamento, armazenamento e acesso. Suas responsabilidades são:

- Assegurar ao gestor da informação que os devidos controles estão implementados;
- Manter os controles para assegurar que somente usuários devidamente autorizados podem acessar dados e que os níveis de acesso estão atribuídos corretamente;
- Assegurar a implementação de medidas de proteção física para gerenciamento e armazenamento das informações;
- Assegurar que os níveis de serviços estão sendo cumpridos;
- Cumprir as políticas de acesso e gerenciamento dos dados aplicáveis;
- Assegurar a disponibilidade da informação em caso de incidentes por meio do desenvolvimento e colaboração no plano de contingência.

Em geral, todas as informações armazenadas em sistemas computadorizados estão sob a custódia da Produban; porém, outras áreas e pessoas podem ser definidas como custodiantes da informação.

Os desenvolvedores de sistemas devem incluir nos sistemas/aplicações da SAM BR mecanismos que viabilizem esta norma.

8. PROCEDIMENTOS

8.1. SOLICITAÇÃO DE ACESSO A LOGIN SIMULTÂNEO

A solicitação deve ser efetuada através da intranet do BSBR na opção: Apoio> Abertura de Chamados> Espaço de Acessos. No formulário do Espaço de Acessos selecionar a opção: Áreas Centrais> Manutenção de Acessos> Acesso *Feeders*. A alçada de aprovação da solicitação é do Superintendente Executivo e o SLA de atendimento é de 2 dias úteis.

9. VIOLAÇÃO

O não cumprimento de algum ponto desta política, intencional ou não, pode levar o colaborador a ser submetido a sanções disciplinares ou legais, dependendo do caso.

Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta política, o Colaborador deve entrar em contato com o seu gestor e/ou com as áreas de Compliance e Tecnologia.

10. VIGÊNCIA E REVISÕES

O presente documento entra em vigor na data de sua publicação e será revisado no período máximo de um ano ou havendo necessidade anterior, o que for menor, para que o documento permaneça sempre atualizado.

CONTROLE DE ALTERAÇÕES	
Histórico de Publicações	**Alterações**
26/04/2017	Publicação inicial
01/01/2018	Revisão e adequação do layout
22/02/2018	Revisão pela área de Risco Operacional
Errata	Alteração do prazo de revisão para um ano.

CONTATOS			
Área	**Nome**	**Telefone**	**E-mail**
ITOP	Katia Sousa	(11) 4130-9241	asset.tecnologia@santanderam.com
Risco Operacional	Marcelo Santos	(11) 4130-9249	asset.riscodemercado@santanderam.com

Diretoria Responsável: Asset Management

Área Responsável: Segurança da Informação