

Código	Documento	Data	Revisão	Páginas
PC017	Segurança da Informação	18/05/2020		15

ÍNDICE

PARTE I - IDENTIFICAÇÃO	2
1. OBJETIVO	2
2. ABRANGÊNCIA.....	2
3. APROVAÇÃO	2
4. GLOSSÁRIO	2
5. REVISÃO.....	2
PARTE II – DESCRITIVO	3
1. INTRODUÇÃO.....	3
2. DIRETRIZES E PROCEDIMENTOS	3
2.1. Definições	3
2.2. Diretrizes Gerais	4
2.3. Sanções.....	13
3. ATRIBUIÇÕES E RESPONSABILIDADES	13
3.1. Colaboradores	13
ANEXO I.....	15

PARTE I - IDENTIFICAÇÃO

1. OBJETIVO

Esta política visa atender os requisitos da Resolução nº 4.557 que dispõe sobre a estrutura de gerenciamento de riscos, parágrafo IV - sistemas, processos e infraestrutura de TI. Busca estabelecer diretrizes para:

- **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, seja acidental ou proposital;
- **Disponibilidade:** Garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

2. ABRANGÊNCIA

Esta política deve ser seguida por todos os colaboradores do FitBank.

3. APROVAÇÃO

Tecnologia – responsável pela manutenção desta política.

Compliance & Controles Internos – responsável pela revisão desta política.

Conselho de Administração – responsável pela aprovação desta política.

4. GLOSSÁRIO

5. REVISÃO

- 18/05/2020 – Versão Original.

PARTE II – DESCRITIVO

1. INTRODUÇÃO

- A Segurança da Informação é uma questão de gestão de risco do negócio. A falha em proteger as informações pode resultar em prejuízo financeiro e ter um impacto negativo na reputação da empresa.
- As normas de segurança da informação estabelecem requisitos mínimos de segurança que todos os colaboradores devem se atentar na condução de suas atividades. Esses requisitos são claros, concisos, legais e regulatórios aplicáveis no contexto onde a empresa realiza seus negócios.
- Caso sejam identificadas ações que estejam em desacordo com o conteúdo dessa política, medidas cabíveis poderão ser aplicadas.

2. DIRETRIZES E PROCEDIMENTOS

2.1. Definições

2.1.1 Vulnerabilidade

- É uma falha ou um ponto fraco no desenvolvimento, na implantação ou no uso da informação. Essa falha ou ponto fraco, pode ser explorado intencionalmente ou não.
- As vulnerabilidades relativas a processos e sistemas, uma vez conhecidas, podem ser exploradas em prejuízo da Instituição, a qualquer tempo. A empresa encontra-se em risco quando não respeita qualquer um dos objetivos de Segurança da Informação.

2.1.2 Informação Confidencial

- Trata-se de informação pessoal ou pessoalmente identificável, dados de cliente, informação proprietária ou não pública, podendo estar em formato escrito, oral, telefônico ou eletrônico. Uma regra geral é supor que qualquer informação que o colaborador receba sobre a empresa ou seus clientes, é uma informação confidencial e, portanto, deve ser protegida contra a divulgação.
- Falhas de sigilo, precisão ou disponibilidade deste tipo de informação trazem grandes danos à empresa, refletidos em perdas financeiras, perda de competitividade e produtividade ou, até mesmo, no comprometimento da imagem.

2.1.3 Categorias de informações confidenciais

- I. Informações pessoais ou pessoalmente identificáveis: informações que podem ser usadas para identificar, direta ou indiretamente, uma pessoa, requerentes de produtos e/ou serviços, colaboradores e seus dependentes ou candidatos a empregos, independentemente da forma como as informações são coletadas ou de onde são coletadas.
- II. Informações proprietárias: informações de propriedade da empresa ou criadas pelo colaborador no âmbito de suas atividades. Isso pode incluir qualquer dado, propriedade intelectual, análise, relatório, sistema ou processo que possa dar à empresa uma vantagem sobre seus concorrentes.
- III. Planos de Negócio atuais ou que tenham sido adotados pela empresa no passado, bem como esboços de novos Planos de Negócio;
- IV. Pesquisas estratégicas desenvolvidas ou contratadas pela empresa;
- VI. Dados de clientes;
- VIII. Senhas de acesso para sistemas, programas e ferramentas da empresa;
- IX. Informação de outra equipe que não se deveria ter acesso;
- X. Custos, preços, lucros, relatórios financeiros ou de custos, produtos, serviços, equipamentos, sistemas, procedimentos, operações, aquisições potenciais.

2.1.4 Incidente de Segurança da Informação

- Trata-se da exploração das vulnerabilidades em processos ou sistemas. Os incidentes, intencionais ou não, ocasionam a perda de qualidade da informação.
- Quando houver suspeita ou conhecimento de ocorrência de atividades que coloquem em risco a segurança das informações da empresa, o colaborador não deve hesitar em informar imediatamente o seu gestor e a área Tecnologia, para a devida tratativa.

2.2. Diretrizes Gerais

- Os colaboradores devem se atentar que o espaço de trabalho da empresa é do tipo “Open Office”, onde todos estão ouvindo conversas de telefone de colaboradores de outras áreas. Quando se trata de conversas com conteúdo sigiloso ou que mereçam maior discrição, aconselha-se o uso de salas de reunião. Também merecem atenção as conversas e manipulação de materiais em espaços de uso comum como copa, banheiro e elevador.

- Enquanto estiver trabalhando para e/ou depois de deixar de trabalhar para a empresa, o colaborador tem a obrigação de proteger as informações pessoais, proprietárias e confidenciais que obteve ou criou enquanto desempenhava suas responsabilidades na empresa.

2.2.1 Autorização para envio de informação confidencial

- As informações confidenciais poderão ser fornecidas à parte receptora, oralmente ou por escrito, através dos seguintes meios, incluindo, mas não se limitando a: CD, e-mail, desenho, modelo, dado, especificação, relatório, compilação, programa de computador, patente, relatório financeiro e econômico de clientes e fornecedores, cópia de contrato, e outros materiais quaisquer que tenham sido obtidos ou conhecidos antes ou depois da vigência desta Política.
- Cópias de material confidencial devem ser feitas com autorização explícita do gestor. A atenção deve ser redobrada para arquivos eletrônicos, uma vez que sua cópia e distribuição são facilitadas. Quando for necessário transferir informações confidenciais, prefira que seja pessoalmente ou através de serviço de entrega confiável, como por exemplo, portador contratado pela empresa.
- Sempre registre as informações básicas dos destinatários da informação confidencial: Nome, local e empresa. É importante lacrar os envelopes que contenham material confidencial e separá-los do correio comum, através da inscrição “confidencial”.

2.2.2 Manutenção de informação confidencial

- Para que a informação se mantenha confidencial, o colaborador deve proceder com sua manutenção e guarda de maneira correta. Seguem procedimentos que podem servir como modelo:
 - ✓ Manter a informação em local seguro, trancado e sem acesso público;
 - ✓ Se a informação confidencial for eletrônica, utilizar meios seguros para armazená-la, como por exemplo, pen drive criptografado, email e armazenamento em nuvem. Para auxílio com esses procedimentos, consultar a área de Tecnologia;
 - ✓ Se a informação confidencial estiver armazenada em notebook ou outro dispositivo móvel, tenha atenção redobrada ao equipamento, uma vez que são alvos visados em assaltos e furtos;
 - ✓ Nunca deixar papéis com informações confidenciais em impressoras ou cestas de lixo, anotações em quadro-branco, arquivos em computadores de uso comum.

2.2.3 Destruição de informação confidencial

- Cópias da informação confidencial em número excessivo ou exemplares desnecessários, devem ser destruídos corretamente, evitando riscos de disseminação da informação para pessoas que não deveriam ter acesso a ela.
- Material físico deve ser destruído utilizando-se trituradores de documentos após o uso. No caso de material eletrônico, destruir as mídias. Se for necessário reaproveitá-las, devem ser utilizados programas especialmente desenvolvidos para apagar todas as trilhas da mídia. Para auxílio com esse procedimento, entrar em contato com a área Tecnologia.
- Se houver perda ou roubo da informação confidencial, avisar o gestor e notificar imediatamente a área Tecnologia para avaliação dos impactos, danos ou riscos e a definição do plano de ação.

2.2.4 Uso de computadores, dispositivos, redes e sistemas

- Computadores, redes e sistemas da empresa, são recursos disponibilizados aos colaboradores para desempenho de suas funções. Dessa forma, todas as informações contidas neles são de propriedade da empresa.
- Mesmo prezando pela privacidade de cada colaborador, alguns procedimentos investigativos que precisem ser instaurados para manter os interesses da empresa ou por determinação judicial, podem requerer rastreamento e verificação de documentos e sistemas sem aviso prévio. Portanto, recomenda-se evitar manter arquivos pessoais armazenados nos recursos da empresa, mesmo sendo permitida a utilização destes para atividades pessoais, desde que não prejudiquem o exercício da função de cada colaborador.

2.2.5 Uso da impressora

- O uso da impressora deve ser estrito para uso profissional. Sendo que mesmo para esse fim, é recomendável que se faça uso com bom senso, evitando desperdício.
- É fortemente recomendável que ao enviar arquivo para impressão, retire-o imediatamente da bandeja da impressora, minimizando a chance de que informações confidenciais sejam compartilhadas indevidamente.

2.2.6 Digitalização de documentos

- É recomendável que a digitalização seja salva em pasta apropriada ao conteúdo e deletado de qualquer pasta compartilhada. Este procedimento é vital para evitar que informações confidenciais, sejam divulgadas indevidamente para pessoas que não deveriam ter acesso a elas.

2.2.7 Uso de senhas

- Para a senha de acesso ao computador e email do colaborador, deve ser dada a mesma importância que se dá a outras senhas utilizadas no cotidiano, como senha bancária. É obrigação do colaborador:
 - ✓ Nunca divulgar ou compartilhar senha com outras pessoas;
 - ✓ Evitar reuso de senhas antigas;
 - ✓ Não anotar senha em papel e deixá-lo sob a mesa, uma vez que facilita cair em mãos de pessoa não autorizada;
 - ✓ Alterar senha todas as vezes que houver suspeita que ela foi descoberta por alguém;
 - ✓ Trocar senha temporária no primeiro acesso ao sistema.

2.2.8 Mesa Limpa e tela limpa

- Informação confidencial deixada em papel sobre a mesa pode ter sua segurança comprometida, passando a ser de conhecimento de pessoas não autorizadas. Dessa forma, cada colaborador deve ter discernimento do que é informação confidencial e atribuir o devido tratamento para garantir que assim permaneça. Um dos cuidados que se deve ter é não deixar papéis com informação confidencial sobre a mesa.
- O colaborador também deve se atentar à informação confidencial disponibilizada na tela do computador ou notebook, quando se ausentar da estação de trabalho. Nesse caso, sempre efetuar o bloqueio por senha através do atalho “CTRL + ALT + DELETE”.

2.2.9 Uso da Internet e e-mail

- A empresa oferece acesso à Internet e email aos seus colaboradores, de maneira que possam exercer suas atividades com eficiência. Estes recursos devem ser utilizados considerando os princípios corporativos de responsabilidade, respeito e profissionalismo.

- A conexão com a Internet está sujeita a diversos riscos, como por exemplo infecção por vírus, portanto, cada colaborador deve estar consciente de que sua estação de trabalho, possuindo este tipo de acesso, também tem sua parcela de contribuição para mantê-la segura. Todos devem se atentar aos sites acessados, bem como aos emails enviados, uma vez que todas as ações realizadas são feitas em nome da empresa.
- A utilização para fins pessoais é permitida, desde que não comprometa os interesses da empresa, não incorra em custos adicionais ou afete negativamente a produtividade do colaborador no exercício de sua função.
- Não é permitido:
 - ✓ Acessar sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento da equipe de Tecnologia;
 - ✓ Utilizar dos acessos aos sistemas, rede e internet disponibilizados pela empresa, inclusive do email corporativo, para visitaç o ou qualquer veiculaç o ou a o, como propaganda e discuss es, que envolva raça, religi o, classe social, pol tica ou pornografia;
 - ✓ Instalar plug-ins e extens es sem o aval da equipe de Tecnologia;
 - ✓ Utilizar sites que exijam informa es confidenciais, senhas, sem oferecer garantia de transmiss o com segurança;
 - ✓ Utilizar vers es gratuitas de sites que recebam upload de informa es e arquivos, que comprimam ou convertam arquivos, uma vez que informa es confidenciais s o inseridas nesses ambientes e n o h  segurança de que assim se mantenham.
- Recomendações importantes
 - ✓ Antes de responder ou enviar uma mensagem, verifique o nome do remetente e destinat rio. Tenha cuidado especial com mensagens de conte do confidencial, para que n o sejam enviadas para destinat rios indevidos;
 - ✓ N o abrir email de origem desconhecida, com nome de remetente ou t tulo suspeito. Apague-o imediatamente;
 - ✓ N o executar programa ou abra arquivo que n o seja esperado, mesmo que seja proveniente de origem conhecida ou aparentemente inofensivo;

- ✓ Não enviar mensagens contendo anexos que não foram incluídos intencionalmente por você. Fique atento à sua estação de trabalho e avise a área Tecnologia e ao seu gestor, quando houver suspeita de infecção por vírus.

2.2.10 Acesso ao e-mail corporativo em ambiente não controlado pela empresa

- Como o e-mail corporativo pode ser acessado de qualquer computador, dentro e fora da empresa e por smartphone, tablet e notebook, também é de responsabilidade do colaborador entender que essa liberdade e flexibilidade de trabalho acarreta responsabilidade de uso de sua parte. Quando o e-mail é acessado de outro computador é necessário verificar se este é dotado de configuração de segurança, uso de softwares originais e antivírus.
- É muito importante que o colaborador se atente ao realizar download de arquivos com informações confidenciais em computador que não seja o corporativo, uma vez que pode ser utilizado incorretamente por outros usuários. É recomendado sempre apagar o arquivo da pasta Downloads após o uso.
- Quando o acesso se dá por aparelho móvel, o colaborador deve se atentar para risco de perda e roubo, já que informações corporativas contidas no e-mail, podem ser usadas indevidamente por terceiros e prejudicar a empresa.
- É importante que o colaborador proteja todos os dispositivos móveis com acesso ao e-mail corporativo com “senha forte”, minimizando a chance de acesso indevido a informações confidenciais. Recomendação para uso de senha forte: 8 caracteres mesclando maiúscula, minúscula, caractere especial e números.

2.2.11 Instalação de software

- Toda instalação de software deve ser feita pela área Tecnologia, pois esta conseguirá avaliar se o software é permitido, já que muitas vezes há versões potencialmente maliciosas ou que introduzem vulnerabilidades que podem gerar vazamento de informações, perda de integridade, violação de direitos de propriedade intelectual.
- Não é permitido que o colaborador instale softwares que permitam acesso remoto, compartilhamento de área de trabalho, visualização de arquivos e acesso à rede de fora do ambiente da empresa, sem o aval da área Tecnologia e de seu gestor, como por exemplo TeamViewer.

2.2.12 Trabalho remoto

- A empresa permite trabalho remoto em algumas condições, porém é solicitado que haja formalmente o aval do gestor e precauções por parte do colaborador, como:
 - ✓ Certificar-se da segurança física do local de trabalho remoto;
 - ✓ Cumprir com os requisitos de segurança nos canais de comunicação, como antivírus e firewall.

2.2.13 Computação móvel

- A atenção para computador móvel, como notebook, deve ser redobrada, principalmente quando transportado.
- Recomendações importantes:
 - ✓ Procurar utilizar cofres em hotéis e outros lugares que tiverem essa estrutura;
 - ✓ Não abandonar o equipamento dentro de veículos e tratá-lo como equipamento sensível quando fizer viagens aéreas, carregando-o como bagagem de mão;
 - ✓ Evitar aparentar que transporta um notebook e outros recursos em locais públicos;
 - ✓ Para colaboradores que utilizam Linux, é imprescindível que criptografe todo o conteúdo dos discos de seu computador. Para auxílio com esse procedimento, consultar a área Tecnologia.

2.2.14 Uso de equipamentos pessoais

- Equipamentos pessoais de colaboradores, como notebooks, smartphones e mídias de armazenamento removível, dentre outros, não podem ser utilizados para guarda ou transferência de informações confidenciais da empresa.
- Há cuidados que devem ser tomados ao se utilizar dispositivos móveis em locais públicos, salas de reuniões e outras áreas desprotegidas. Convém que sejam estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos, por exemplo, através da utilização de técnicas de criptografia.

2.2.15 Uso de programas de mensagens instantâneas

- É proibido o uso destes programas de mensagens que não tenham objetivo profissional. A utilização de programas de mensagens instantâneas pode prejudicar a segurança da informação por ser uma ferramenta que facilita o envio e recebimento de dados, informações e documentos.

2.2.16 Wireless

- A empresa disponibiliza acesso a uma rede wireless que está separada da rede local, a qual fornece aos colaboradores o acesso à Internet.
- A rede wireless para acesso à Internet disponibilizada pela empresa é protegida por senha, seguindo as boas práticas de segurança da informação.

2.2.17 Dispositivos removíveis

- Caso seja necessário que o colaborador copie informações de um dispositivo móvel para a rede corporativa, ou que seja necessária a utilização de mídias de armazenamento como pen drive e dispositivos similares para transporte de informações da empresa, o colaborador deverá obter aprovação formal com seu gestor e solicitar à área Tecnologia a liberação de download e upload de arquivos de e para mídia removível respectivamente. Ao efetuar a transferência de arquivos para ou do dispositivo móvel, fica definido que a segurança dessas informações, passa a ser de responsabilidade do executor da ação.

2.2.18 Admissão e demissão de funcionários

- A área Adm. & Financeiro é quem informa à área Tecnologia toda e qualquer movimentação de temporários, estagiários, e admissão/demissão de colaboradores, para que os mesmos possam ter acesso liberado ou restringido na empresa.
- O cadastramento inclui veiculação de senha e registro de nome como usuário nos sistemas da empresa. Cabe ao gestor do colaborador comunicar à área Tecnologia sobre quais pastas da rede o colaborador terá acesso. No caso de temporário e estagiário, deverá também ser informado o período em que o mesmo trabalhará na empresa, para que na data de seu desligamento possam também ser encerrados seus acessos à rede e sistemas. No caso de demissão, a área Adm. & Financeiro deverá comunicar o fato o mais breve possível à área Tecnologia para que o colaborador tenha seus acessos bloqueados.
- Cabe à área Adm. & Financeiro fornecer esta política e obter o Anexo I preenchido e assinado de cada novo colaborador, bem como de todos os colaboradores na reciclagem periódica de adesão às políticas e manuais. Nenhum colaborador poderá ter acesso à rede e sistemas da empresa, sem ter expressamente concordado com esta política.

2.2.19 Controle de acesso – segregação física e lógica

- Todos os colaboradores portam crachá magnético que limita o acesso por meio de catraca ao prédio e ao escritório da empresa.
- A área Tecnologia é responsável por fazer levantamento periódico de todos os acessos da rede e a validação é realizada pelo gestor de cada equipe. Isso evita que haja acessos por colaboradores que mudaram de equipe ou que já saíram da empresa. O objetivo é mitigar o risco de informações confidenciais serem divulgadas para colaboradores que não deveriam ter ciência delas.

2.2.20 Verificação de necessidade de acesso

- Todo colaborador deve ter acesso a sistemas, pastas e documentos da rede corporativa pertinentes às atividades que desempenha no escopo de seu trabalho. É necessária a revisão deste controle no mínimo anualmente, pela área Tecnologia e gestores de equipes.

2.2.21 Controles contra códigos maliciosos

- A empresa compreende a importância de implementar controles de detecção, prevenção e recuperação para proteção de seus recursos tecnológicos contra códigos maliciosos, como por exemplo vírus, worms, cavalos de tróia, adware ou spyware combinado com adequado programa de conscientização do colaborador.

2.2.22 Treinamento

- Devido à importância de conscientização em relação à segurança da informação, a área Compliance & Controles Internos, com apoio da área Tecnologia, é responsável em elaborar e veicular treinamentos periódicos sobre esse tema para que os colaboradores estejam cientes de suas responsabilidades. Tais treinamentos devem estar alinhados com as políticas e procedimentos relevantes de segurança da informação, levando em consideração as informações a serem protegidas e os controles a serem implementados para essa finalidade.
- É muito importante que o programa seja atualizado regularmente, de modo que ele permaneça alinhado com as políticas e os procedimentos da empresa, e seja construído com base nas lições aprendidas dos incidentes de segurança da informação.
- O treinamento em conscientização pode utilizar diferentes formatos, tais como presencial e online, contemplando os seguintes aspectos:

- a. necessidade de tornar conhecido e estar em conformidade com as obrigações e regras de segurança da informação aplicáveis, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos;
 - b. responsabilidade pessoal por seus próprios atos e omissões e compromissos gerais para manter seguro ou para proteger a informação, que pertença à empresa;
 - c. procedimentos de segurança da informação básicos tais como: notificação de incidente de segurança da informação, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa;
 - d. Disponibilização de equipe especializada para orientação sobre questões de segurança da informação.
- Uma avaliação do entendimento das pessoas pode ser conduzida no final do curso de conscientização, educação ou treinamento para testar a transferência de conhecimento.

2.3. Sanções

- Caso o colaborador não respeite as obrigações estabelecidas nesta política, estará sujeito à aplicação de sanções, que, de acordo com a gravidade da infração praticada, poderão ser advertência escrita, suspensão e demissão. A decisão sobre a sanção a ser aplicada caberá ao gestor do colaborador e à Diretoria Executiva.

3. ATRIBUIÇÕES E RESPONSABILIDADES

3.1. Colaboradores

- Usar ou compartilhar informações confidenciais somente com o propósito para o qual foram coletadas, somente até onde necessário para realizar responsabilidades do seu cargo e apenas com pessoas autorizadas. Nunca acessar ou usar as informações dos clientes ou de outros funcionários, exceto para os devidos fins de negócios.
- Tomar as providências necessárias para garantir que as informações pessoais e proprietárias sejam produzidas, copiadas, transmitidas, armazenadas e descartadas de forma segura, para evitar a divulgação não autorizada destas informações.
- Não compartilhar nem discutir informações pessoais, proprietárias ou confidenciais fora da empresa, salvo quando permitido ou exigido por lei ou regulamentação pertinente, ou diante de intimação ou ordem judicial da jurisdição competente.

- Respeitar a confidencialidade de informações da empresa, mesmo quando seu contrato de trabalho chegar ao fim. Antes de deixar a empresa, devolva todo o material e anotações que tenha posse.
- Relatar imediatamente a divulgação ou recebimento de informações pessoais, proprietárias ou confidenciais ao seu gestor e à área Compliance & Controles Internos.
- Entrar em contato com a área Compliance & Controles Internos sobre dúvidas relacionadas ao uso apropriado das informações de clientes ou colaboradores.
- Não discutir assuntos sensíveis ou informações pessoais, proprietárias ou confidenciais em locais públicos, inclusive na Internet e, tenha cautela ao discutir essas informações em áreas abertas do local de trabalho, como por exemplo ao usar viva-voz.

ANEXO I

DECLARAÇÃO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O colaborador declara ter recebido, lido, compreendido e aderido à Política de Segurança da Informação do FitBank.

O colaborador declara, ainda, para todos os fins e efeitos de direito, estar ciente de que a violação o sujeitará às sanções previstas na Política de Segurança da Informação do FitBank e à eventual responsabilização judicial pelos danos causados e/ou ato praticados, nos termos da legislação aplicável.

Nome: _____

Posição / cargo: _____

Assinatura: _____

Data: