FITBANK INSTITUIÇÃO DE PAGAMENTOS ELETRÔNICOS S.A.

Norma de Classificação da Informação

Código:	**NO005** - Norma de Classificação da Informação
Versão:	1.2
Controle da ISO	27002 / 8 / 8.2 / Classificação da informação
Data da versão:	20/03/2023
Criado por:	Infraestrutura e Segurança da Informação
Aprovado por:	Otávio Farah – CEO Rener Menezes - CTO
Classificação:	Restrita

Sumário

1. Introdução

Essa Norma está de acordo com a Política de Segurança da Informação, que é a principal referência para diretrizes de alto nível de Segurança da informação do FitBank.

A norma de classificação da Informação deve ser de conhecimento de todos os colaboradores, parceiros, terceiros e demais pessoas externas, que tenham acesso a qualquer informação sensível.

2. Objetivo

Este documento visa garantir que os colaboradores sigam as instruções para proteger as informações adequadamente.

A Norma de Classificação da Informação serve para orientar os colaboradores sobre como tratar e proteger de forma adequada dados e informações e entender o valor da informação e a necessidade de proteção conforme o nível da informação. As orientações indicadas nessa Norma buscam atender as diretrizes de segurança da organização e devem ser aplicadas a todo tipo de informação em posse do FitBank, independente do formato (documentos em papel, formato eletrônico, oral, conhecimento de colaboradores etc.).

3. Diretrizes da norma

As orientações abaixo devem ser seguidas para garantir a correta classificação das informações do FitBank:

3.1 Gestão da Informação

A gestão da informação envolve os seguintes processos:

Atividade	**Responsável**
Classificação da informação	Proprietário do ativo
Rótulo das informações	Proprietário do ativo
Tratamento das informações	Pessoas com privilégio de acesso

Sempre que uma informação de fora da organização for recebida, essa informação deve ser classificada de acordo com as orientações descritas nessa Norma pelo gestor da área que recebeu a informação.

Toda informação deve receber uma indicação do seu nível de classificação de confidencialidade. Informações sem essa indicação serão tratadas como informações públicas.

A classificação de cada informação deve ser determinada com base nos critérios abaixo:

- **Valor da informação** – importância que a informação representa no negócio da organização;
- **Criticidade e sensibilidade das informações** – impacto que apresenta no negócio da organização caso a informação se torne pública, houver algum vazamento ou roubo da informação;
- **Obrigações contratuais e legais** – Com base na lista de obrigações regulamentares e contratuais que a organização precisa cumprir como LGPD, Bacen etc.

Os responsáveis pelas informações devem revisar a classificação de confidencialidade de suas informações a cada dois anos e avaliar se essa classificação pode ser alterada.

Todo incidente com informações classificadas deve ser reportado ao time de segurança para o correto tratamento.

3.2 Nível de Confidencialidade

Todas as informações devem ter sua classificação de acordo com os níveis de confidencialidade seguindo a tabela abaixo:

Nível	**Rótulo**	**Critérios de Classificação**	**Restrição de Acesso**
Público (Site institucional, newsletter)	Sem rótulo	Tornar essa informação pública não prejudica a organização.	As informações estão disponíveis para o público em geral

Uso Interno (Políticas, vídeos de integração, documentos, formulários)	USO INTERNO	O acesso não autorizado. As informações podem trazer impacto negativo de pequena escala.	As informações estão disponíveis para os colaboradores e alguns terceiros e parceiros.
Restrito (Dados pessoais dos colaboradores, dados dos sistemas em produção, dados de clientes)	RESTRITO	O acesso não autorizado. As informações podem causar grande impacto aos negócios e a organização.	As informações estão disponíveis somente a um grupo específico de colaboradores e terceiros ou parceiros autorizados.
Confidencial (Logins/Senhas, contratos, propostas comerciais)	CONFIDENCIAL	O acesso não autorizado. As informações podem trazer danos irreparáveis a organização, comprometendo os negócios e a reputação.	As informações estão disponíveis somente para indivíduos específicos da organização.

3.2 Rótulo das Informações

Documentos em papel	O nível de confidencialidade é indicado de forma destacada no documento ou está indicado na capa ou envelope que contém o documentou no local de armazenamento
Documentos eletrônicos	O nível de confidencialidade é indicado de forma destacada em todas as páginas do documento.

Mídia de armazenamento eletrônico	O nível de confidencialidade deve estar indicado na parte superior da mídia.
Informações transmitidas oralmente	O nível de confidencialidade deve ser transmitido antes da informação em si.

4. Gestão das informações Classificadas

Todos os colaboradores, terceiros ou parceiros autorizados que acessam informações classificadas devem seguir as regras abaixo para o tratamento adequado dos ativos:

Tipo de Informação	**Uso Interno**	**Restrito**	**Confidencial**
Documentos em papel	Somente pessoas autorizadas devem ter acesso. Se enviado para fora da Organização, o documento deve ser enviado como carta registrada. Os documentos devem ser mantidos dentro da organização e inacessíveis ao público. Os documentos devem ser removidos de impressoras.	Os documentos devem estar armazenados em armários com chave. Os documentos só podem ser transportados por terceiros dentro e fora da organização se estiverem dentro de envelope fechado. Se o documento for encaminhado para fora da organização, um serviço de confirmação de recebimento deve ser contratado. Os documentos não podem estar expostos em impressoras.	O documento deve ser armazenado em um cofre. O documento só pode ser transferido dentro e fora da organização por pessoa confiável em envelope lacrado. O documento só poderá ser impresso ou copiado se a pessoa autorizada estiver presente e próxima ao aparelho.

		Somente o proprietário do documento pode copiá-lo e destruí-lo.	
Documentos eletrônicos	Somente pessoas autorizadas podem acessar. Quando os documentos forem enviados devem estar protegidos por senha. A tela em que o documento é exibido deve ser bloqueada automaticamente depois de 5 (cinco) minutos de inatividade	Somente pessoas autorizadas a acessar o documento podem acessar a área do sistema de informações em que o documento está armazenado. Quando os documentos forem enviados, devem estar protegidos criptografia e senha. Somente o proprietário pode apagá-lo.	O documento deve ser armazenado com criptografia. O documento só pode ser armazenado em ambientes gerenciados IF. O documento não deve ser enviado por serviços como FTP, WhatsApp e outros. Sempre utilizar meios seguros de transmissão com criptografia como SFTP.
Sistemas de informações	Somente pessoas autorizadas podem ter acesso. O acesso ao sistema deve ser protegido por senha. A tela em que o documento é exibido deve ser	Os usuários devem se desconectar do sistema de informações se saírem do local de trabalho. Os dados devem ser excluídos por meio de algoritmo que garanta a sua eliminação segura.	O acesso ao sistema de informação deve ser controlado com processo de múltiplo fator de autenticação. O acesso ao sistema de informação deve

	bloqueada automaticamente depois de 2 (dois) minutos de inatividade.		ser restrito a usuários e origens de acesso específicas, sempre que aplicável.
E-mails	Somente pessoas autorizadas podem ter acesso. O remetente deve verificar atentamente o destinatário.	O e-mail deve ser criptografado se for enviado para fora da organização.	Todos os e-mails devem ser criptografados.
Mídia de armazenamento eletrônico	Somente pessoas autorizadas podem ter acesso. As mídias ou arquivos devem ser protegidos por criptografia ou no mínimo por senha. A mídia deve estar armazenada em salas com acesso controlado. Se enviada para fora da organização a mídia deverá ser encaminhada como carta registrada.	As mídias e os arquivos devem estar criptografados. A mídia deve ser armazenada em um armário trancado com chave. Se a mídia for encaminhada para fora da organização, um serviço de confirmação de recebimento deve ser contratado. Somente o proprietário da mídia pode apagá-la ou destruí-la.	A mídia deve ser armazenada em cofre de sala de acesso restrito. A mídia só pode ser transferida dentro e fora da organização por pessoa confiável em envelope lacrado.

Informações transmitidas oralmente	Somente pessoas autorizadas podem ter acesso à informação. Pessoas não autorizadas não devem estar presentes na sala quando a informação for transmitida.	A conversa não deve ser gravada. Deve ser realizada em locais reservados.	A conversa feita por meio de comunicação deve ser criptografada.

Os cuidados com o tratamento das informações são cumulativos, ou seja, os cuidados de informações com níveis mais baixos são também aplicáveis aos níveis mais altos.

Os ativos de informações podem ser retirados das instalações somente após autorização do gestor e ciência dos diretores da área.

5. Responsabilidade

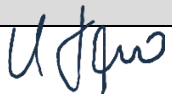
Todos os responsáveis pelas informações do FitBank devem garantir a aplicação das regras desta Norma.

6. Descumprimento

A diretoria de TI deve iniciar uma ação disciplinar sempre que as regras forem violadas ou se as informações forem transmitidas a pessoas não autorizadas.

Todos os incidentes relacionados a gestão de informações, devem ser informados de acordo com o procedimento de gestão de incidentes.

7. Revisão e Aprovação

Revisado por	**Cargo/Função**	**Data**
	Head of Infrastructure and Security	**10 de maio de 2023**
Aprovado por	**Cargo/Função**	**Data**
	CEO	**10 de maio de 2023**
	CTO	**10 de maio de 2023**

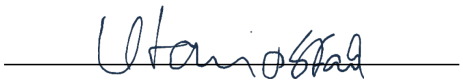
8. Controle de Alterações

Data	**Versão**	**Descrição da alteração**
Setembro/22	1.0	Emissão inicial|Infra e Segurança da Informação
Setembro/22	1.1	Ajuste do item 4 que aborda tartamento de ativos| Infra e Segurança da Informação
Março/23	1.2	Formatação de texto. Correção de *typos*.

Página de assinaturas

Gustavo Ramos
527.812.323-00
Signatário

Rener Menezes
970.499.643-87
Signatário



otavio farah
274.697.938-10
Signatário

HISTÓRICO

10 mai 2023 12:11:11 — **Gustavo Castelo Branco Crisostomo Ramos** criou este documento. (E-mail: gustavo.ramos@fitbank.com.br, CPF: 527.812.323-00)

10 mai 2023 12:11:12 — **Gustavo Castelo Branco Crisostomo Ramos** *(E-mail: gustavo.ramos@fitbank.com.br, CPF: 527.812.323-00)* visualizou este documento por meio do IP 52.67.100.58 localizado em São Paulo - Sao Paulo - Brazil

10 mai 2023 12:11:19 — **Gustavo Castelo Branco Crisostomo Ramos** *(E-mail: gustavo.ramos@fitbank.com.br, CPF: 527.812.323-00)* assinou este documento por meio do IP 52.67.100.58 localizado em São Paulo - Sao Paulo - Brazil

10 mai 2023 13:50:08 — **otavio silveira farah** *(E-mail: otavio.farah@fitbank.com.br, CPF: 274.697.938-10)* visualizou este documento por meio do IP 189.39.222.250 localizado em Santana de Parnaiba - Sao Paulo - Brazil

10 mai 2023 13:51:45 — **otavio silveira farah** *(E-mail: otavio.farah@fitbank.com.br, CPF: 274.697.938-10)* assinou este documento por meio do IP 179.208.204.4 localizado em São Paulo - Sao Paulo - Brazil

10 mai 2023 13:51:23 — **Rener Silva de Menezes** *(E-mail: rener.menezes@fitbank.com.br, CPF: 970.499.643-87)* visualizou este documento por meio do IP 189.39.222.250 localizado em Santana de Parnaiba - Sao Paulo - Brazil

10 mai 2023 13:51:36 — **Rener Silva de Menezes** *(E-mail: rener.menezes@fitbank.com.br, CPF: 970.499.643-87)* assinou este documento por meio do IP 189.39.222.250 localizado em Santana de Parnaiba - Sao Paulo - Brazil