



Política de Segurança da Informação (Fornecedores)

2024



Política de Segurança da Informação (Fornecedores)

Folha de Controle

Código de referência e nº da versão	POL_SI_EXT_V1.0_202408
Publicidade	Informação Externa
Área Proprietária da Política	Segurança da Informação
Políticas e outros documentos relacionados	N/A
Palavras-chave	N/A

Histórico de Versões

Versão	Descrição	Data	Autor
1.0	Versão Inicial	11/2023	Safeway Consultoria
1.1	Revisão de Conteúdo	08/2024	GSGA Advogados

Aprovado por:

Julian Duran

Marcio Saito

Data:

Agosto/2024



Sumário

1. OBJETIVO	4
2. ABRANGÊNCIA	4
3. NORMAS RELACIONADAS	4
4. DIRETRIZES	5
5. PRINCÍPIOS	5
6. REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	7
7. SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO	8
8. REQUISITOS	8



1. OBJETIVO

O objetivo da Política de Segurança da Informação para Fornecedores (“Política”), é estabelecer diretrizes de alto nível abrangendo crenças, metas e objetivos de toda a empresa projetados para atender todos os requisitos de segurança da informação exigidos pelas leis aplicáveis, regulamentos e padrões da indústria.

As diretrizes da Política são projetadas para fornecer uma visão geral de como a Entrepay mantém um ambiente que seja controlado, consistente, seguro e projetado para aumentar a produtividade dos membros da Entrepay e parceiros.

2. ABRANGÊNCIA

Essa Política abrange a todos os colaboradores e terceiros que se relacionam com a Entrepay, em especial, fornecedores e prestadores de serviços que se relacionam com a empresa.

3. NORMAS RELACIONADAS

[RESOLUÇÃO BCB Nº 85/2021](#)

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.



[RESOLUÇÃO BCB Nº 368/2024](#)

Altera as Resoluções BCB ns. 28, de 23 de outubro de 2020; 65, de 26 de janeiro de 2021; 85, de 8 de abril de 2021; 93, de 6 de maio de 2021; 155, de 14 de outubro de 2021; e 260, de 22 de novembro de 2022;

4. DIRETRIZES

A segurança é responsabilidade de todos os colaboradores e terceiros que se relacionam com a Entrepay. Portanto, os indivíduos com acesso às instalações e ativos de informações da Entrepay devem cumprir os requisitos definidos neste documento, bem como em qualquer documentação de padrão(ões) de Segurança da Informação associado(s).

A segurança é uma responsabilidade de trabalho fundamental para todos os membros da equipe e faz parte dos termos e condições de trabalho.

A violação de segurança, intencional ou não, é motivo para ação disciplinar consistente com a gravidade da violação. Espera-se que todos os membros da equipe relatem caso identifiquem a violação destas diretrizes.

5. PRINCÍPIOS

A Entrepay se compromete a proteger as informações de seus fornecedores de acordo com os seguintes princípios:

- Confidencialidade: as informações devem ser mantidas confidenciais e acessíveis apenas a pessoas autorizadas;
- Integridade: as informações devem ser precisas e completas;
- Disponibilidade: as informações devem estar disponíveis quando necessário.



A Segurança da Informação na Entrepay está presente através de três fatores que são determinados por: pessoas, processos e tecnologia. A implementação é realizada de forma eficaz, com a presença de um conjunto de controles de segurança adequados em sua estrutura organizacional, determinados por políticas, processos, procedimentos e a atribuição de responsabilidades através de funções definidas.

Os fornecedores/terceiros devem proteger seus ativos de informação, infraestrutura e sistemas contra destruição, perda, danos técnicos, erros, falsificação, roubo ou uso não autorizado, seja intencional ou acidental.

Os fornecedores/terceiros devem proteger as informações contra ações não autorizadas, incluindo modificação, cópia, acesso ou outras.

Os fornecedores/terceiros devem fornecer orientação estabelecendo uma política de Segurança da Informação, aprovando funções e responsabilidades e fornecendo coordenação consistente dos esforços de segurança em toda a empresa.

Os seguintes princípios orientadores fundamentais devem sustentar quaisquer políticas, padrões, e procedimentos utilizados e ser considerados por parte dos fornecedores/terceiros:

Princípio 1. Utilizar um processo baseado em padrões de mercado (ISO 27001) para identificar, avaliar e tratar informações de segurança aplicáveis aos ambientes Entrepay.

Princípio 2. A informação é um ativo comercial crítico e deve ser protegida em relação à sua importância e valor.

Princípio 3. Os controles são necessários para proteger a confidencialidade, integridade e disponibilidade das informações bens.



Princípio 4. Investir em controles comprovados com base no ciclo de vida, avaliação de custo-benefício e risco análise. O objetivo não é necessariamente eliminar os riscos, mas minimizá-los da forma mais custo-benefício, compensando o custo dos controles contra a redução antecipada de perdas devido a evitar ou mitigar Incidentes de segurança.

Princípio 5. A Segurança da Informação é uma parte inerente da arquitetura de informações da Entrepay e processos operacionais e de gestão. Todos os membros da equipe são responsáveis pelas informações Segurança.

Princípio 6. A Segurança da Informação é um elemento central da governança corporativa da Entrepay.

Princípio 7. A Segurança da Informação é um facilitador de negócios que permite que a Entrepay entre com mais confiança em relações comerciais, mercados e situações com risco aceitável.

Princípio 8. A liderança do segmento tem a responsabilidade de garantir que suas áreas permaneçam em conformidade com a Política de Segurança de Informação da Entrepay.

6. REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação da Entrepay é avaliada pelo menos anualmente, e ajustado, conforme apropriado, considerando mudanças nos requisitos de negócios, tecnologia e ameaças que possam impactar o ambiente da organização ou de seus parceiros de negócio.

As mudanças na política de Segurança da Informação Entrepay são revisadas e aprovadas anualmente.

A Política de Segurança da Informação é divulgada e publicada.



7. SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

O Sistema de Gestão da Segurança da Informação (SGSI) da Entrepay está implementado para que sejam adotadas medidas alinhadas as estratégias, considerando requisitos relevantes de Segurança da Informação e questões como leis e regulamentações relevantes, que possibilitem a proteção da informação.

É realizada a manutenção periódica no Sistema de Gestão da Segurança da Informação (SGSI) da Entrepay, ou conforme a ocorrência de mudanças significativas, realizando avaliações de riscos e a identificação de oportunidades de melhoria, assim como, são consideradas as análises críticas da Alta Direção e os resultados de auditorias, onde o desenvolvimento e implementação dos ajustes necessários são realizados por um grupo específico de responsáveis.

Como parte do processo e contribuição para que o SGSI da Entrepay seja cada vez mais eficaz, é importante que clientes e fornecedores contribuam com as diretrizes aqui descritas e estejam cientes de Política de Segurança da Informação da Entrepay.

8. REQUISITOS

Os fornecedores devem cumprir os seguintes requisitos de segurança da informação:

- Identificação e avaliação de riscos: Os fornecedores devem identificar e avaliar os riscos de segurança da informação associados à sua relação com a Entrepay e/ou apoiar com as informações necessárias para uma avaliação de riscos.



- Medidas de segurança: Os fornecedores devem implementar medidas de segurança para mitigar os riscos identificados.
- Controle de acesso: Os fornecedores devem controlar o acesso dos seus colaboradores às informações da Entrepay de acordo com os princípios de confidencialidade, integridade e disponibilidade.
- Segurança de sistemas e aplicações: Os fornecedores devem proteger os sistemas e aplicações que acessam ou processam informações da Entrepay.
- Segurança de dados: Os fornecedores devem proteger os dados da Entrepay de acordo com as leis e regulamentos aplicáveis.
- Segurança da rede: Os fornecedores devem proteger a rede que acessa ou processa informações da Entrepay.
- Segurança física: Os fornecedores devem proteger as instalações físicas que abrigam informações da Entrepay.
- Segurança da continuidade do negócio: Os fornecedores devem implementar planos de continuidade do negócio para garantir a disponibilidade das informações da Entrepay em caso de incidente.
- Treinamento e conscientização: Os fornecedores devem treinar seus funcionários sobre os requisitos de segurança da informação da Entrepay.
- Auditoria: A Entrepay pode realizar auditorias nos fornecedores para verificar o cumprimento desta política. É responsabilidade dos fornecedores fornecer os insumos necessários para tal avaliação.



- Cumprimento de obrigações contratuais: Aos fornecedores é imprescindível o cumprimento das obrigações de Segurança da Informação descritas no contrato firmado com a Entrepay.
- Cumprimentos regulatórios e legais: Aos fornecedores é imprescindível o cumprimento de obrigações regulatórias e legais relacionadas à Segurança da Informação e privacidade aplicáveis ao negócio da Entrepay, de acordo com as atividades realizadas por estes fornecedores de processamento de informações da Entrepay.

entrepay

