

**BePay-012**  
**POLÍTICA DE SEGURANÇA CIBERNÉTICA**

## **Sumário**

- 1. Objetivo**
- 2. Público Alvo**
- 3. Regras, Papéis e Responsabilidades**
  - 3.1 Procedimentos e Controles Adotados para Garantir os Objetivos de Segurança Cibernética**
  - 3.2 Controles Adotados para a Segurança das Informações Sensíveis**
  - 3.3 Registro, Análise da Causa dos Efeitos de Incidentes Relevantes e Vulnerabilidades**
  - 3.4 Diretrizes Gerais**
  - 3.5 Treinamento de Segurança na BePay**
  - 3.6 Compartilhamento de Informações**
  - 3.7 Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem**
  - 3.8 Sanções e Punições**
  - 3.9 Comunicação**

## 1. Objetivo

O objetivo desta política é orientar os colaboradores e definir os procedimentos e controles da BePay em relação à segurança cibernética, os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, estando em conformidade com a legislação e regulamentação vigentes e normas internas.

É diretriz que toda informação de propriedade da BePay seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade, independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.

## 2. Público Alvo

Esta política submete principalmente à área de Segurança da Informação e todas as áreas da BePay ao seu cumprimento.

Aplica-se a todos os administradores reforçando o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética e demais colaboradores (funcionários, estagiários e terceiros) da BePay, com a recomendação de serem diligentes no cumprimento das diretrizes definidas.

## 3. Regras, Papéis e Responsabilidades

### 3.1 Procedimentos e Controles Adotados para Garantir os Objetivos de Segurança Cibernética

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, onde é de extrema importância a disseminação da cultura de segurança cibernética para garantir a confidencialidade, integridade e disponibilidade das informações, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Para garantir o cumprimento dos princípios dispostos acima, a BePay utiliza diversos meios como as políticas internas, instruções normativas, comunicados corporativos, controles tecnológicos, monitoração e a realização de treinamentos periódicos de segurança da informação e compliance.

### 3.2 Controles Adotados para a Segurança das Informações Sensíveis

A BePay possui diversos controles e procedimentos para garantir a segurança das informações sensíveis, conforme descrito nos tópicos abaixo:

### **3.2.1 Controle de Acesso e Gerenciamento**

A prática de Controle de Acesso e Gerenciamento tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade das informações. A BePay segue as boas práticas no sentido de orientar que todos os usuários devem possuir acesso à informação de acordo com as necessidades de negócio, respeitando a segregação de função baseada em cargo/função. Todo funcionário, estagiário ou prestador de serviços possui apenas um identificador (login) de acesso à informação.

### **3.2.2 Gerenciamento de Riscos e Tecnologia da Informação**

A BePay verifica periodicamente o controle de acessos à internet e controla os aplicativos instalados nos computadores. Vale ressaltar que nenhum usuário possui acesso de administrador local, impossibilitando a instalação de qualquer aplicativo. Somente podem ser instalados aplicativos previamente testados e autorizados por TI. A BePay realiza o monitoramento da rede por meio de software específico.

### **3.2.3 Segurança de Rede**

A segurança é realizada através do monitoramento e gerenciamento da infraestrutura, sendo que todo acesso às redes internas e acessos à internet são controlados por Tecnologia da Informação.

### **3.2.4 Segurança e gerenciamento de Ativos de Sistemas**

Referente ao gerenciamento das parametrizações de segurança, somente a área de Segurança da Informação tem acesso para alterar as configurações de acesso e segurança nos Sistemas de Informação.

### **3.2.5 Gestão de Ameaças e Vulnerabilidades de TI**

O ambiente possui instalado software de antivírus para a proteção contra vírus, arquivos e softwares maliciosos, atualizados periodicamente.

Todas as atualizações de segurança do Windows são gerenciadas e atualizadas frequentemente.

### **3.2.6 Dispositivos e Controles de Mídia**

Somente pessoas previamente autorizadas pela Diretoria Executiva e a Segurança da Informação, têm acesso aos dispositivos móveis e acessos ao leitor de DVD e USB do computador.

### **3.2.7 Segurança Física**

Os recursos e instalações de processamento de informações críticas para as atividades da BePay são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso. Os equipamentos críticos possuem proteção contra desastre físico e recursos para combate a incêndio.

A BePay possui sistema para controle do acesso dos colaboradores, prestadores de serviços ou fornecedores aos locais restritos, que são monitorados por câmeras.

### **3.2.8 Classificação da Informação**

A BePay estabelece em políticas e normas diretrizes para a classificação da informação, seu manuseio e descarte.

A informação é classificada de forma a se indicar a confidencialidade e o nível esperado de proteção.

### **3.3 Registro, Análise da Causa dos Efeitos de Incidentes Relevantes e Vulnerabilidades**

A BePay entende que é de extrema importância a existência de um procedimento que possibilita a detecção tempestiva e a pronta comunicação de incidentes e vulnerabilidades, assegurando assim, a eficácia das medidas a serem tomadas na sequência. A BePay possui os controles que permitem detectar e identificar os incidentes e vulnerabilidades que afetam o ambiente de Segurança Cibernética.

As responsabilidades em relação ao registro, análise e comunicação dos incidentes estão devidamente detalhadas em normativos específicos.

### **3.4 Diretrizes Gerais**

#### **3.4.1 Prestadores de Serviços de Tecnologia**

Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de Tecnologia são previamente definidos em contratos, além disso, todos os contratos firmados com a BePay possuem termo (NDA) ou cláusulas de confidencialidade.

#### **3.4.2 Classificação da criticidade dos Incidentes**

Os incidentes relacionados à Segurança Cibernética seguem os fatores de criticidade definidos em norma interna.

### **3.4.3 Plano de Ação de Resposta a Incidentes**

A elaboração e acompanhamento do plano de ação são coordenados pela a Área de Segurança da Informação, com participação de outras áreas.

### **3.5 Treinamento de Segurança na BePay**

A cultura de Segurança Cibernética é disseminada internamente através de programas de capacitação ministrados periodicamente para todos os colaboradores, garantindo assim que todos estejam cientes das possíveis ameaças e vulnerabilidades que ocorrerem no âmbito da Segurança Cibernética, bem como quais são os procedimentos que devem ser adotados em casos de incidentes.

### **3.6 Compartilhamento de Informações**

A BePay buscando sempre atuar com transparência e objetivando a melhoria dos seus procedimentos relacionados à Segurança Cibernética, tem o compromisso de compartilhar com o BACEN todos incidentes relevantes, tempestivamente, sempre que solicitado.

### **3.7 Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem**

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas na Resolução 3.909 do BACEN.

### **3.8 Sanções e Punições**

A área de Segurança da Informação realiza o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política. Caso haja violação das regras nela dispostas, bem como às demais normas e procedimentos de Segurança da Informação, mesmo que por omissão ou tentativa não consumada, tal violação pode ser classificada como incidente de segurança cibernética, os quais são passíveis de penalidades.

### **3.9 Comunicação**

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail [seginform@bepay.com](mailto:seginform@bepay.com)