PÚBLICO

Moneo | O BANCO DA Marcopolo

POLÍTICA DE SEGURANÇA CIBERNÉTICA

FINALIDADE

Definir diretrizes da empresa para proteção das informações e sua propriedade, as quais visem assegurar:

- **Confidencialidade** da informação, ou seja, assegurar que a informação é acessível somente às pessoas autorizadas;
- **Integridade** da informação, ou seja, garantir que todas as informações estejam integras e precisas durante todo o seu ciclo: Criação, Processamento e Destruição;
- **Disponibilidade** da informação para os processos de negócio, ou seja, assegurar que os usuários autorizados tenham acesso à informação e ativos associados, quando necessário;
- **Conformidade** com requisitos legais e regulatórios;
- **Continuidade** do negócio em caso de eventos de grandes proporções que comprometam a operação do negócio do Banco Moneo;
- **Conscientização** dos colaboradores quanto à importância da segurança da informação.

Descrever como prevenir e responder as ameaças aos sistemas de informação, tais como: acesso sem autorização, revelação, duplicação, modificação, apropriação, destruição, perda, abuso e riscos de ataques cibernéticos (invasões, vírus, *malwares*, *spywares*, *ransomwares,* etc.).
As diretrizes são os conceitos de alto nível que devem ser observados.

OBJETIVO

O objetivo deste procedimento é proteger os ativos da informação do Banco Moneo contra ameaças internas e externas, sendo elas intencionais ou acidentais.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040

Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

RESPONSÁVEIS

Todas as pessoas que, de alguma forma, prestem serviços para o Banco Moneo sejam elas colaboradores ou não, inclusive os visitantes, são obrigadas a obedecer às regras definidas nesta Política.

DEFINIÇÕES

Esta Política estabelece diretrizes sobre a importância e responsabilidades de cada indivíduo na segurança da informação.

FUNÇÕES E RESPONSABILIDADES

- **Alta Administração**
  - A Alta Administração do Banco Moneo é responsável pela aprovação da Política de Segurança Cibernética e por buscar constantemente melhorias nos procedimentos relacionados à Segurança Cibernética, visando proteger as informações sensíveis.

- **Colaboradores, Prestadores de Serviço e Visitantes**
  - Cumprir as diretrizes definidas neste documento e os procedimentos correlatos;
  - Consultar a Área de TI em caso de dúvidas relacionadas à segurança da informação;
  - Informar a Área de TI ocorrências que impactem sobre a segurança da informação;
  - Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;
  - Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para finalidades aprovadas pelo Banco Moneo;

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040

Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

- Utilizar de modo seguro e responsável toda infraestrutura da empresa (computadores, telefonia, dispositivos móveis, e-mail, internet, sistemas e outros);
- Não conectar dispositivos particulares, como notebooks, celulares, câmeras fotográficas, modems de banda larga etc., à rede ou ao seu computador;
- Garantir que somente arquivos relacionados ao trabalho sejam armazenados, transmitidos, processados ou impressos na utilização dos recursos do Banco Moneo
- Comunicar a Área de TI sobre qualquer descumprimento ou violação deste manual e/ou dos seus procedimentos correlatos.

- **Área de TI Moneo e Divisão de TI Corporativa**

  - Implantar e gerenciar controles visando assegurar a confidencialidade, integridade e disponibilidade das informações do Banco Moneo;
  - Analisar, investigar sob demanda e tratar todos os incidentes que envolvem a segurança da informação.
  - Controlar todos os equipamentos (computadores e celulares) e seus responsáveis.
  - Promover ou contratar programas de capacitação dos colaboradores visando promover a cultura sobre Segurança Cibernética.

- **Proprietário da Informação**

  - Classificar as informações que estão sob sua responsabilidade;
  - Autorizar a liberação de acesso aos sistemas e/ou informações sob sua responsabilidade;

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

- Revisar periodicamente liberações de acesso concedidas para colaboradores e terceiros, além de solicitar revogação dos acessos que não são mais necessários.

CLASSIFICAÇÃO DAS INFORMAÇÕES E PRIVACIDADE

Todas as informações do Banco Moneo em meio digital, devem ser classificadas em uma das quatro categorias definidas pelo procedimento de Classificação da Informação: “secreta”, “confidencial”, “uso interno” ou “público”, e de acordo com a criticidade que representam para os negócios do Banco Moneo.
As informações que não estejam classificadas serão consideradas, por padrão, como confidenciais até que o Proprietário da Informação atribua um rótulo.
As informações, estando elas em meio físico ou digital, devem ser classificadas conforme rótulos a seguir:

Categorias de Informação		
Categoria	**Descrição**	**Exemplos**
SECRETA	Informações cujo acesso deve ser muito restrito, mesmo dentro da empresa. Sua revelação sem autorização pode prejudicar seriamente a o Banco Moneo e/ou seus clientes.	Decisões estratégicas.
CONFIDENCIAL	Informações cujo acesso deve ser muito restrito, mesmo dentro da Instituição. Sua revelação sem autorização pode prejudicar seriamente a o Banco Moneo e/ou seus clientes.	Informações privadas dos usuários, contratos, avaliações de mercado e senhas de acesso, dados dos clientes e de suas operações com o banco.
USO INTERNO	Toda informação que não se ajusta claramente nas anteriores, entretanto sua revelação poderia prejudicar ou causar constrangimento ao Banco Moneo	Catálogo de e-mails, materiais de treinamento, políticas e normas, entre outros.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

PÚBLICA	Informação que foi explicitamente aprovada pelo responsável e foi aprovada sua divulgação pela área de Controladoria e ou comercial.	Anúncios de produtos ou serviços, boletins de imprensa, catálogos de produtos, informações legais obrigatórias.

*Informações Secretas e Confidenciais são consideradas como Informações Sensíveis, para fins desse documento.

Informações não classificadas devem ser consideradas por padrão, como confidenciais até que o Proprietário da Informação atribua um rótulo.

Os responsáveis pela informação (área de negócio) devem decidir a quem é permitido o acesso, manipulação, distribuição e uso regular da informação. Além disso, a Divisão de TI Corporativa deve assegurar a existência de controles adequados de armazenamento e disponibilidade durante todo o ciclo da informação. Informações ao se tornarem obsoletas devem ser destruídas. O responsável pela informação tem poder de decidir sobre a destruição da informação, sendo o único impedimento, um parecer da Assessoria Jurídica (corporativo), Tributário (corporativo), Jurídico, Compliance ou Controladoria determinando o período mínimo de armazenamento de informações.

É proibida a cópia desassistida de todo ou parte de documentos considerados “Secreto” ou “Confidencial” para distribuição às pessoas que não sejam nomeadas pelo responsável pela informação a ter acesso a esses dados.

Não é permitida a guarda de documentos considerados “Secreto” ou “Confidencial” em disco rígido de computador pessoal. Todos os documentos devem ser manipulados e estar armazenados nos equipamentos disponibilizados pelo Moneo.

GESTÃO DE ATIVOS

Todos os colaboradores e gestores das áreas de negócios são responsáveis pelos ativos disponibilizados pela TI, para execução das atividades de negócios do Banco Moneo. O colaborador assina um Termo de Responsabilidade ao receber qualquer equipamento eletrônico necessário para o cumprimento de suas atividades. No caso de perda, roubo ou danos ao equipamento, a TI deve ser prontamente informada.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040

Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

Os sistemas e computadores de propriedade do Banco Moneo devem ser usados unicamente para atividades empresariais.

No processo de desligamento, a Área de TI deve receber e registrar, a entrega de todos os equipamentos disponibilizados ao colaborador. A Área de TI deve realizar backup dos dados, caso necessário, e apagar todas as informações armazenadas no dispositivo.

Uso de dispositivos de armazenamento móvel, como *pendrive*, é proibido. Exceto para dispositivos móveis, de propriedade do Banco Moneo e quando utilizados, exclusivamente, nas atividades da empresa. Por norma, todos os computadores (desktops) são entregues aos usuários com as portas USB bloqueadas para utilização. Somente são liberadas mediante autorização do gestor da área de negócio.

GESTÃO DE SOFTWARE

Nenhum colaborador está autorizado a instalar qualquer software ou alterar a configuração do sistema sem a homologação e aprovação da Área de TI.

Somente softwares originais e freeware, com as licenças válidas e autorizadas pela Área de TI possuem permissão de uso.

A Área de TI pode monitorar as estações de trabalho para garantir que somente softwares originais e freeware, homologados pela Área de TI e com licenças válidas, sejam utilizados. Adicionalmente, deve implementar controles que bloqueiem a instalação de software não homologado.

CONTROLE DE ACESSO

A concessão de acesso aos sistemas de informação do Banco Moneo é suportada por um processo formalizado de Gestão de Acessos, onde estabelece as diretrizes para colaboradores, prestadores de serviços e visitantes sobre a importância e as responsabilidades de cada indivíduo sobre a segurança da informação no controle de acesso do Moneo. Esse processo está devidamente

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

descrito no capítulo XII do Manual de Procedimentos – Segurança da Informação (corporativo) e também na norma interna 15.5 – Procedimento de Senhas e Perfil de Acesso. Nessas normas estão definidos os processos para acessos aos sistemas, procedimentos de senha, procedimento de utilização da Internet, VPN e e-mails entre outros controles

O controle de acesso é extremamente importante para garantir que as informações sejam acessadas somente por pessoas autorizadas e essas tenham acesso somente as informações necessárias para o desempenho das suas atividades. O Banco Moneo conta com procedimentos para garantir que somente serão concedidos acessos aos sistemas informatizados com as devidas autorizações, sendo retirados assim que ocorrer o término do contrato de trabalho com o colaborador ou com o prestador de serviços. A área de TI do Banco Moneo realiza trimestralmente junto aos responsáveis das demais áreas uma revisão dos usuários e perfis de acesso dos principais sistemas do banco. Isso para garantir que somente são concedidos acessos nas funcionalidades dos sistemas que são necessárias para o cumprimento das atividades dos colaboradores.

GESTÃO SOBRE INCIDENTES DE SEGURANÇA

Todos os incidentes de segurança como falhas de segurança nos sistemas, funcionamento inadequado de software, uso de software não autorizado, existência de softwares maliciosos, ataques por hackers, sabotagem física, fraudes utilizando os computadores, violação de acesso, entre outros ocorridos, devem ser imediatamente comunicados à Área de TI do Banco Moneo que também reportará a Divisão de TI corporativa. Os incidentes oriundos dos prestadores de serviços terceirizados da mesma maneira deverão ser comunicados a Área de TI do Banco Moneo que reportará a Divisão de TI corporativa. O Comitê de Segurança da Informação corporativo analisa, trata e investiga a causa raiz dos incidentes de segurança da informação reportados.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

A Divisão de TI corporativa realiza a contratação de empresa especializada para realização trimestral de Testes de Vulnerabilidade nos servidores/aplicativos que possuem publicação externa. Esses testes geram Planos de Ação para melhorias na segurança da informação.

Os incidentes de segurança da informação devem ser categorizados e a prioridade do tratamento deve ser definida de acordo com o nível da severidade. A forma de categorização e os processos para informação e tratamento do incidente estão descritos no capítulo XIII do Manual de Procedimentos – Segurança da Informação (corporativo).

AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

O desenvolvimento e/ou manutenção sistêmica deve estar alinhada às boas práticas do ciclo de vida do desenvolvimento de software e considerar os requisitos de segurança definidos no capítulo XIV do Manual de Procedimentos – Segurança da Informação (corporativo) e nas seguintes normas:

- 15.8 - Ambientes e Ferramentas para Desenvolvimento
- 15.9 - Nomenclatura de Projetos
- 15.10 - Núcleo de Desenvolvimento

Para todo sistema desenvolvido ou toda aquisição de novos sistemas, deverá ser aberta solicitação junto a área de TI. Para todo projeto deverá haver controle sobre:

- Aprovações necessárias (área de negócios e TI)
- Responsável pelo projeto
- Descrição da necessidade
- Documentação técnica
- Orçamentos
- Comprovações de testes pela área de TI e de negócios.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

Para todo desenvolvimento, devem existir ambientes segregados, para testes e produção. Todo sistema deve prever o controle criterioso de acessos, com senhas fortes (conforme norma 15.1 - Procedimento de Usuários Senhas e Perfis de Acesso) e perfis de acesso que possibilitem a concessão funcionalidades e dados necessários para o cumprimento da atividade do colaborador. Caso esse software seja acessado externamente a rede da empresa, deverá haver contratação de certificação e maior controle de acesso.

Nenhum colaborador está autorizado a instalar qualquer sistema e programa não autorizado pela Divisão de TI ou pela Área de TI do Moneo.

A aquisição de qualquer sistema deve ser aprovada pela Divisão de TI corporativa ou pela Área de TI do Banco Moneo, após estudo de impactos no ambiente e atendimento à necessidade identificada.

Caso a Divisão de TI corporativa ou a Área de TI do Banco Moneo não possa realizar o desenvolvimento ou manutenção do sistema, por quaisquer que sejam as razões, podem ser contratados serviços de terceiros.

Os softwares, sejam eles desenvolvidos internamente como adquiridos de terceiros, devem prever controles de acessos através de senhas fortes que possibilitem a identificação e a guarda dos logs de acessos. Além disso, para os *softwares* publicados externamente, deverá haver criptografia dos dados trafegados e autenticidade do servidor e do cliente por meio de certificados digitais.

O contrato de prestadores de serviços para desenvolvimento e manutenção de sistemas obrigatoriamente deve conter cláusulas de confidencialidade, além disso, deve definir papéis e responsabilidades do terceiro contratado.

Conforme a Resolução CMN nº 4.893/21 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o Banco Moneo deverá possuir um procedimento efetivo para garantir o cumprimento das regras previstas na regulamentação.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

SEGURANÇA FÍSICA E AMBIENTAL

Ambientes que armazenam e/ou processam informações críticas devem estar protegidos por controles físicos e ambientais apropriados. Esses controles devem ser proporcionais à criticidade dos equipamentos, dos sistemas e das informações mantidas e manuseadas nestas áreas. O monitoramento a distância também deve estar contemplado.

As áreas restritas, que armazenam equipamentos tecnológicos que suportam os negócios do Moneo, devem possuir controles de segurança física conforme descritos no capítulo XVI do Manual de Procedimentos – Segurança da Informação (corporativo) e nas normas 15.1 - Procedimento de Usuários Senhas e Perfis de Acesso e 15.4 - Procedimento De Aplicação De Correções em Sistema de TI.

PLANO DE CONTINUIDADE DE NEGÓCIOS

O Plano de Continuidade deve assegurar a rápida retomada das atividades em caso de falhas ou interrupção das operações, priorizando os recursos que forem mais críticos para a operação.

O Plano de Continuidade de Negócios inclui os processos e procedimentos necessários para recuperação de qualquer interrupção do serviço, independentemente da causa.

O Comitê de Controles Internos e Riscos aprovou o Plano de Contingência do Moneo (16.6 – Plano de Contingência) o qual estabelece os procedimentos em caso de interrupção dos negócios. Nesse Plano, na norma 15.2 - Procedimento de Backup e no capítulo XVI do Manual de Procedimentos – Segurança da Informação (corporativo) estão definidos os procedimentos referentes os testes a serem realizados para garantir a eficácia do Plano de Contingência. Todos os procedimentos executados e problemas identificados durante o teste do Plano de Contingência devem ser documentados para as ações de melhorias e correções do plano.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040

Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

O Banco Moneo também conta com processos bem definidos de backup dos dados (conforme norma 15.2 - Procedimento de Backup). Esse processo permite a rápida recuperação do dado em caso de perdas ou falhas. Há procedimentos de backup de dados dos bancos de dados dos sistemas utilizados pelo Moneo bem como de todos os conteúdos das pastas de rede. O Plano de Contingência engloba testes com o intuito de garantir que esses processos estejam sendo realizados corretamente.

GERENCIAMENTO DE OPERAÇÕES E COMUNICAÇÕES

O Gerenciamento de Operações e Comunicações destina-se a estabelecer as diretrizes de segurança de rede, de gerenciamento da infraestrutura, monitoramento dos serviços prestados por prestadores de serviço, uso do e-mail e ferramentas de comunicação, bem como o acesso à rede através de dispositivos móveis.

Cabe a Divisão de TI Corporativa gerir dispositivos de segurança de rede, tais como: firewall, antivírus etc. Todo acesso, controle, permissões devem obrigatoriamente serem concedidos somente pela Divisão de TI Corporativa e estão devidamente detalhados no capítulo XVIII do Manual de Procedimentos – Segurança da Informação (corporativo).

A Divisão de TI Corporativa e a área de TI do Banco Moneo são responsáveis por manter a atualização dos patches, correções de programas, sempre que novas versões forem disponibilizadas pelo fornecedor.

Anualmente a Divisão de TI Corporativa deve analisar e planejar a capacidade dos servidores que suportam as aplicações e bancos de dados para os negócios.

As áreas também devem avaliar se os serviços prestados por prestadores de serviços atendem às necessidades contratadas, controlar os SLAs (*Service Level Agreements*) estabelecidos em contrato e garantir que os prestadores somente tenham acesso aos locais e dados necessários para a referida

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145

prestação do serviço. Sempre que acessarem dados confidenciais e sigilosos devem possuir o Termo de Confidencialidade devidamente assinado.

O Banco Moneo encoraja o uso de comunicações eletrônicas (Internet, correio eletrônico etc.). Contudo o uso de qualquer um destes recursos implica no reconhecimento de que os sistemas de comunicações eletrônicas e todas as mensagens geradas ou transmitidas através dos mencionados sistemas de comunicações eletrônicos são considerados como propriedade da do Grupo Marcopolo, podendo ser monitoradas sem aviso prévio ou aprovação do usuário, podendo também restringir acesso a determinados conteúdos para garantir a segurança da Informação. Os acessos indevidos detectados durante a revisão dos logs de utilização do acesso à Internet devem ser tratados pelo Comitê de Segurança da Informação Corporativo.

Para dispositivos móveis – que tenham sido fornecidos ao colaborador pelo Banco Moneo – os acessos à rede e e-mail estão atrelados a solicitação formal e devidamente autorizada, para que a área de TI do Banco Moneo e a Divisão de TI Corporativa realize as devidas configurações.

Em caso de perda, roubo ou furto do dispositivo móvel o colaborador deve realizar o procedimento de bloqueio remoto, caso não seja possível, deve notificar a área de TI do banco para que seja providenciado o bloqueio do aparelho.

PENALIDADES

Os prejuízos/perdas ocasionados pelo não cumprimento dessa política serão analisados pela Área de Compliance e encaminhados ao Comitê de Recursos Humanos, que tomará as medidas cabíveis.

(54) 2991 1000
www.bancomoneo.com.br
Ouvidoria: 0800 723 5040
Av. Rio Branco, 4889, 4º andar
Bairro Ana Rech - Caxias do Sul/RS
CEP 95060-145