MONOPÓLIO
CORRETORA DE CÂMBIO

Av. Cmte. Brás de Aguiar, 202 A - Nazaré, Belém - PA, 66035-000 - (91) 3224-1384

Política de Tecnologia e Segurança Cibernética

versão Maio.2019

INTRODUÇÃO

Este guia estabelece as regras e procedimentos básicos que compõem a política de segurança da empresa Monopólio Corretora de Câmbio, implementada segundo os requisitos e determinações de seu planejamento estratégico e alinhada aos dispostos da Resolução 4.658 - BACEN, 26/04/2018.

A implementação das diretrizes descritas neste documento, visa garantir a integridade e disponibilidade dos dados e sistemas de informação corporativos, observando também requisitos de confidencialidade e sensibilidade das informações sob nossa guarda, os riscos inerentes ao nosso modelo de negócio e a natureza de nossas operações.

A elaboração, manutenção e a disponibilização desta Política são de responsabilidade das Áreas de Compliance e de Tecnologia da Informação da Monopólio Corretora de Câmbio

OBJETIVOS

Definir diretrizes que assegurem a capacidade da empresa para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, através da criação de uma Política de Segurança Cibernética e Plano de Ação e Resposta à Incidentes, a serem seguidos por seus colaboradores.

Vale ressaltar que a eficácia das diretrizes e procedimentos indicados neste documento está diretamente ligada ao comprometimento de usuários colaboradores, seus responsáveis hierárquicos ou supervisores e dos integrantes da área de T.I., conforme listadas a seguir:

Comprometimento dos Usuários Colaboradores

Respeitar esta Política de Segurança da Informação;

Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;

Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do Gestor da área de TI;

Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software

Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;

Assegurar que as informações e dados de propriedade da Monopólio Corretora de Câmbio não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico;

Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro;

Relatar para o seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para suas atividades;

Responder pelo prejuízo ou dano que vier a provocar à esta instituição ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Comprometimento dos Responsáveis Hierárquicos
Apoiar e zelar pelo cumprimento desta PSC, servindo como modelo de conduta para os colaboradores sob a sua gestão;

Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSC;

Autorizar o acesso e definir o perfil do usuário junto ao gestor da área de TI;

Autorizar as mudanças no perfil do usuário junto ao gestor da área de TI;

Educar os usuários sobre os princípios e procedimentos de Segurança da Informação;

Notificar imediatamente ao gestor da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;
Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;

Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor da área de TI;

Obter aprovação técnica do gestor da área de TI antes de solicitar a compra de hardware, software ou serviços de informática;

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSC.

Comprometimento da Área de TI
Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSC;

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.;

Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação;

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;

Administrar, proteger e testar as cópias de segurança dos programas e dados relativos ao negócio;

Gerenciar o descarte de informações a pedido dos responsáveis;;

Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário;

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários garantindo a segurança por área do negócio;

Criar a identidade lógica dos colaboradores na empresa;

Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;

Proteger todos os ativos de informação da empresa contra códigos maliciosos e ou vírus;

Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção;

Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa;

Realizar inspeções periódicas de configurações técnicas e análise de riscos;

Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais;

Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento da empresa;

Propor as metodologias sistemas e processos específicos que visem aumentar a segurança da informação;

Promover a conscientização dos colaboradores em relação a relevância da segurança da informação;

Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;

Buscar alinhamento com as diretrizes corporativas da empresa;

Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede − a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

Monitorar o ambiente de TI a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso a internet e aos sistemas críticos da Monopólio Corretora de Câmbio, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior), conforme procedimento publicado na matriz de responsabilidade;

Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade.

1. Padrões e Procedimentos de Segurança da Informação

Todos os acessos ao ambiente de Rede, software de apoio, Sistemas e Dados da empresa, somente será feito após liberação pelo departamento de Compliance.

Controle de Acesso Lógico

O acesso aos dados referentes aos Processos e Produtos da Monopólio Corretora de Câmbio será concedido aos usuários colaboradores somente com base nas suas necessidades funcionais e após a liberação, de autorização dada pelos Gestores, que detém o papel de Proprietário das Informações.

Esta autorização será feita através de documento de Autorização ou e-mail, no qual constarão obrigatoriamente todos dados de identificação do usuário e suas necessidades devidamente discriminada entre acesso para entrada, alteração, exclusão e consulta.

Autorização de Acesso Físico

O acesso a sala de TI que contém os Servidores deverá ser restrito e monitorado por câmeras de vídeo. O acesso será permitido somente a pessoa da área de Ti ou pessoal previamente autorizado, que neste caso deverá estar acompanhado por pessoal do TI.

Apenas os funcionários da área de TI e colaboradores previamente registrados mediante contrato deverão possuir acesso autônomo.

Padrão para Identificação de usuário e senha

Para ter acesso aos sistemas e recursos da rede interna, todos os usuários colaboradores deverão possuir conta individualizada. No caso de pessoal contratado para serviço temporário, o acesso deve possuir prazo para expirar e, quando for o caso, requisitar ter assinado termo de confidencialidade.

Toda solicitação de acesso, precisa ser autorizada pelo responsável da área fim e pelo TI.

A Senha deverá :

- Conter no mínimo 8 caracteres, sendo ao menos uma letra e um número;
- Ser colocada pelo próprio usuário e ser de conhecimento somente dele;
- Ser bloqueada no caso de 3 tentativas fracassadas, podendo ser desbloqueada somente por funcionário do TI;
- Ser trocadas caso haja suspeita de alguém ter conhecimento.

Prestadores de Serviço

A contratação de Prestadores de Serviço que implementam e mantenham a infraestrutura de tecnologia, deve ser formalizada considerando a validação de perfil e idoneidade comprovados, formalizando o seu direito de acesso e o seu comprometimento com o sigilo das informações manuseadas, sendo declarado em documento próprio. Deverá ser realizado o monitoramento integral de suas atividades.

Registro, Proteção e Revisão de Registro de Eventos (Logs)

Os Sistemas, Gerenciador de Banco de Dados e outras Ferramentas de gestão de rede, especialmente as que acessam dados em Produção, geram Registro de operações sensíveis feitas pelo Suporte / Gestão de Infra, e é fundamental que seja mantido registro de acesso e alteração de dados , sendo este mantido protegido de alteração e deleção. Deverá ser feita revisão periódica dos mesmos, quer diretamente, quer usando rotina de extração de operações pontuais com software de extração e análise de dados.

Backup e Restore

Deverá existir backup dos dados e das aplicações existentes na empresa, devendo este ser automatizado e executado preferencialmente fora do horário de produção.

Deverá ser realizado backup diário, semanal e mensal, mantendo cópia criptografada em ambiente interno e externo à empresa.

Devem ser realizados testes de recuperação do backup, para validar a capacidade de restauração

2. Ativos de TI

Deverão ser realizados, em periodicidade a ser definida e divulgada pelo setor de Tecnologia da Informação, inventário de todos os bens de informação. Estes itens serão objeto de classificação, pelo seu impacto para os negócios, entre alto, moderado e baixo, o que determinará, dentre outras finalidades a necessidade de controle sobre ela, a necessidade de armazenamento em áreas de rede (ao invés de gravados em discos locais das estações dos usuários) e relevância para o Plano de Continuidade de Negócios.

3. Aplicativo de Antivírus

Todos os computadores utilizados na empresa deverão possuir anti-vírus instalados para garantir a integridade e proteção dos dados. O mesmo deverá ser mantido em ambiente centralizado e atualizado pela área de Ti.

Não será permitido a nenhum usuário desativar o uso ou desinstalar o software Antivírus.

Deve ser objeto de divulgação aos usuários as melhores práticas preventivas relativas à anexos e links de mensagens de e-mail que são fonte de risco de contaminação por vírus e software similares.

4. Software de Automação de Escritório

Os Softwares utilizados deverão estar catalogados, e ter seus contratos revisados.

A Área de Ti manterá o controle de licenças.

5. Processamento de Dados na Nuvem

Caso haja, serviço de processamento de dados na Nuvem, o mesmo deverá estar em acordo com as políticas indicadas neste documento, atendendo aos requisitos do negócio e à resolução do Banco Central.

6. Regras de uso

Instalação e uso de Software

Os Colaboradores não poderão instalar e/ou utilizar software sem que haja ciência e autorização do responsável do seu Departamento e do Setor de TI, mesmo que o software em questão seja gratuito.

Acesso e uso da Internet

Somente será liberado se solicitado pelo Gerente da área, com aprovação da respectiva Diretoria, sendo indicado o nível de acesso que o mesmo precisará possuir.

Os colaboradores no momento da liberação, receberão instrução e deverão manifestar concordância com as restrições e monitoramento que a empresa considerar necessários para cumprimento das regras de utilização, através de termo com o esclarecimento das boas prática de uso e das possíveis penalidades.

Regras de uso do e-mail

O Colaborador deverá fazer uso exclusivo para atividades Corporativas, e que estejam relacionadas às atividades do setor em que está lotado..

Deverá ter assinatura padronizada e conter mensagem padrão indicativa quanto limitação da responsabilidade sobre o conteúdo da mensagem.

Regras para Manuseio, Troca e Armazenamento de Dados

Não será permitido aos usuários extraírem diretamente informações, sem que seja formalizado um pedido, e aprovado pelo Gestor do Setor, devidamente justificado pelas necessidades funcionais do requisitante. Para garantir que esta restrição seja efetiva, serão bloqueados os dispositivos de leitura e gravação USB e a capacidade de gravação de Unidades de CD e DVD. Exceções a esta regra geral serão avaliadas pelo gestor de TI e Compliance.

Acesso Remoto

Realizado somente pelos colaboradores de TI, para a instalação, configuração e manutenção dos sistemas existentes na Monopólio Corretora de Câmbio. O acesso deverá ser feito via canal de comunicação criptografado e quando realizado deverá registrar o acesso para controle e contar com autorização prévia.

Uso dos Computadores e demais equipamentos de informática

São de uso exclusivo da empresa, não devendo ser deslocados sem a prévia autorização. É de responsabilidade do usuário manuseá-lo corretamente para o cumprimento das atividades da instituição, seguindo os procedimentos operacionais indicados pelas gerências responsáveis.

A manutenção física ou lógica deve ser realizada somente por equipe técnica do Ti ou pessoal designado por eles.

DISPOSIÇÕES FINAIS

A Segurança da Informação deve ser entendida como parte importante da cultura de uma organização, sendo fator determinante para garantir e oferecer um serviço de qualidade e de confiança.

REFERÊNCIA

Banco Central - Resolução 4.658, 26/04/2018