POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

A CPI CENTRAL preocupada com a informação que processa, desenvolveu esta política que descreve as principais diretrizes que cada colaborador precisa seguir para manter elevados padrões de segurança da informação.

A CPI CENTRAL classificou de forma clara e objetiva os tipos de informação que processa, para assim definir as medidas de proteção a serem adotadas por todos os colaboradores. Desta forma, serão evitados eventos como vazamento de informação, aumento descontrolado do nível de acesso de terceiros ou ameaças sistemáticas que podem afetar a boa imagem da empresa e diminuir a sua competitividade no mercado além de trazer riscos de processos penais e administrativos.

2. Escopo / Alcance

Esta política está destinada a todas as pessoas que dirigem CPI CENTRAL, a seus ocupantes de funções gerenciais, empregados, terceiros contratados, temporários, jovens aprendizes e estagiários (“Colaboradores”), bem como aos seus fornecedores e prestadores de serviço.

Ela está regida em todos aqueles territórios domésticos ou internacionais onde CPI CENTRAL opera.

3. Propósito desta Política

A política classifica o tipo de informação processada e descreve os comportamentos aceitáveis e não aceitáveis a fim de garantir a segurança da informação que a CPI CENTRAL possui. A política descreve a forma apropriada de como agir para diminuir ou mitigar riscos relacionados a vazamento de informação e medidas apropriadas para estar em conformidade com os requerimentos legais e regulatórios aplicáveis.

4. Conceitos:

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso de perda dos dados originais, o que pode envolver eventuais remoções acidentais ou dados corrompidos.

Cliente: é aquela Pessoa Jurídica ou Pessoa Física que contrata os serviços da CPI CENTRAL.

Colaborador: refere-se ao membro da liderança, ao ocupante de funções gerenciais, empregado direto e indiretos, contratados, estagiários e jovens aprendizes que estão desenvolvendo atividades na CPI CENTRAL.

Data Protection Officer (DPO): também chamado de Encarregado de Dados, é o responsável por coordenar e por assegurar a conformidade com a Política de Proteção de Dados e requisitos legais/regulamentares locais aplicáveis, também, atua como o canal principal com os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados ANPD.

Erro: equívoco; opinião ou julgamento que contraria a verdade.

Evento: incidente inesperado ou situação que altera a ordem normal da operação.

Informação Confidencial: toda informação que tem acesso restrito a terceiros, incluindo a certos colaboradores. Exemplo: Dados da Folha de Pagamento dos Colaboradores, Informação Privilegiada num processo de Fusão ou Aquisição, Plano Estratégico da CPI CENTRAL

I**nformação Pública:** refere-se a todo conteúdo que o público em geral tem acesso, exemplos: Campanha Publicitária, Informação no Jornal ou mídia social, informação em cartórios e registros.

Informação de Uso Interno: toda aquela informação disponível para uso dos colaboradores da CPI CENTRAL para execução do seu trabalho rotineiro. Em consequência, a informação não é para uso público externo, exemplos: Políticas, Processos & Boas Práticas que não estejam publicadas na página de internet da CPI CENTRAL, e-mails corporativos, comunicados internos, qualquer documento utilizado ou material intelectual utilizado para tarefas diárias.

Recursos de Tecnologia da Informação todos os sistemas, softwares, aplicativos, microcomputadores, equipamentos portáteis, impressoras, telefones digitais, periféricos, mídias magnéticas, redes de computadores, correio eletrônico, internet, todos os recursos e ferramentas de produtividade colocados à disposição dos usuários pela área de TI, com a finalidade única e exclusiva de ajudar a desenvolver as atividades de interesse da CPI CENTRAL.

Titular dos Dados (Titular): pessoa natural ou indivíduo a quem se referem os dados pessoais que são objeto de tratamento.

5. Princípios Gerais:

5.1 Software

- Somente é permitida a utilização de cópias de software que tenham passado pelo processo de homologação e aprovação da Diretoria.

- O usuário não deve adquirir, instalar ou substituir qualquer software sem a devida autorização da Diretoria.

- As necessidades de software devem ser submetidas à área de TI, que efetuará um estudo de viabilidade da aquisição e homologação deles, como forma de garantir sua adesão aos padrões e à política de segurança da empresa.

- Toda contratação de serviços de informática, tais como treinamento, desenvolvimento e consultoria, deve ser submetida à apreciação prévia para aprovação da diretoria da área.

- Não é permitida a duplicação, empréstimo, transferência ou retirada de software para outros equipamentos, dentro ou fora da empresa.

- É permitido o uso de protetor de tela, somente os que são distribuídos com o sistema operacional de cada máquina e os distribuídos pela empresa. A utilização de programas de licença gratuita (freewares), de validade temporária (sharewares) ou fornecidos como demonstração (demos), só poderá ser feita em casos de comprovada necessidade do uso, de forma legal e suportada por autorização formal do responsável da área de TI, desde que não haja programas para a mesma finalidade já adquiridos ou homologados pela empresa.

- Para nenhum fim é permitido ao usuário a utilização de programas não autorizados que afetem a segurança da informação, tais como: programas para descobrir senhas, rastrear portas e acessos, rastreamento de teclados, cavalos de troia, vírus, ferramentas utilizadas por hackers etc.

- Irregularidades ou divergências encontradas em softwares adquiridos antes da publicação deste padrão devem ser comunicadas à Diretoria, que avaliará a regularização.

5.2 Equipamentos de TI

- O usuário é responsável direto pela conservação, guarda e utilização dos equipamentos mantidos à sua disposição.

- Os equipamentos portáteis (notebooks, laptops) devem ser mantidos pelos usuários em lugar seguro, com especial atenção contra furtos e roubos, avarias ou uso não autorizado de terceiros.

- Os Colaboradores que utilizam aparelhos celulares, Smartphones e Notebooks fornecidos pela CPI CENTRAL, são responsáveis diretamente por eles e deverão sempre zelar pela segurança das informações contidas nestes equipamentos, que na maioria das vezes funciona como extensão da estação de trabalho.

- O extravio de aparelhos portáteis corporativos deverá ser comunicado imediatamente a administração e para área de TI para as providências de bloqueio.

- Em caso de perda, furto ou roubo de um dispositivo móvel, o colaborador deverá abrir um Boletim Ocorrência (B.O.) e notificar imediatamente o seu gestor direto.

- É vedada ao usuário a abertura ou tentativa de qualquer tipo de manutenção nos equipamentos.

- Sempre que possível, antes do envio de equipamento para manutenção, venda ou doação, as informações neles contidas devem ser removidas.

5.3 Senhas

- É proibido compartilhar senhas, seja para acesso à rede corporativa, sistemas aplicativos, tanto internos como externos (liberação de recursos, banco de dados, sites etc.), equipamentos, etc. com os colegas de trabalho (ou qualquer outra pessoa), inclusive aqueles de nível hierárquico superior, uma vez que a senha é pessoal e intransferível.

- A senha utilizada pelo Colaborador na execução de suas funções é de responsabilidade do próprio Colaborador, que deve sempre utilizá-la com prudência e integridade, sendo de sua total responsabilidade o seu uso indevido por terceiros.

- Sempre que uma nova senha for disponibilizada pela área de TI, deverá ser obrigatoriamente substituída de imediato pelo Colaborador no primeiro acesso ao recurso concedido.

- Todas as transações efetuadas nos sistemas são registradas e associadas à senha do usuário conectado ao servidor, de modo a responsabilizá-lo no caso de irregularidades.

- Nenhum usuário deverá tomar conhecimento de senhas de outros usuários, seja por meio de software, digitação ou qualquer outro meio.

- O tamanho, as regras de formação e a periodicidade de troca das senhas devem obedecer às normas e recomendações definidas pela área de TI.

- Devem-se utilizar senhas de proteção em arquivos com informações de natureza altamente confidencial.

5.4 Internet e Correio Eletrônico

- O acesso aos serviços de internet e correio eletrônico, através dos computadores conectados à rede, destina-se aos interesses da empresa, apenas para os usuários que possuírem autorização formal do gerente da área. Não utilize e-mail para fins pessoais.

- O uso da Internet somente é permitido para sites de interesses profissionais da empresa.

- Todo correio eletrônico / e-mail transmitido da empresa, interna ou externamente, deve estar identificado com assinatura do usuário.

- No uso dos serviços de internet e correio eletrônico, não é permitido o acesso, a baixa (download), a carga (upload), a armazenagem, o recebimento, o envio e a retransmissão de material (comunicação, arquivo, mensagem, etc.) que possa ser considerado por qualquer pessoa como discriminatória, obscena, ilegal ou ofensiva, ou que tenha qualquer informação considerada confidencial ou de uso restrito dentro da empresa.

- A baixa de software deve ser submetida à área de TI, para assegurar a não exposição da empresa a processos de utilização indevida.

- Não é permitida a transmissão ou retransmissão de propagandas, de boatos, “correntes” ou coisas do gênero, bem como mensagens que contenham documentos anexos de remetentes desconhecidos.

5.5 Arquivos, Backup e guarda de dados na rede

- Os arquivos existentes nos sistemas informatizados (rede, sistemas e aplicativos etc.) da empresa são de uso exclusivo e não devem ser transferidos para outros equipamentos ou dispositivos de armazenamento de dados (memória USB Flash Drive – Pen Drives, CD’s, etc.), a não ser que sejam de/para uso interno, **desde que haja prévio consentimento e autorização da Diretoria**.

5.6 Antivírus

- A área de TI irá instalar e manter atualizada quando aplicável a versão do antivírus nos equipamentos, orientando os usuários sobre as providências a serem tomadas em casos de contaminação.

- Usuários devem manter o antivírus ativo e residente, notificando qualquer anormalidade à área de TI e ao usuário que enviou o arquivo infectado.

- Todos os arquivos recebidos, provenientes de qualquer mídia, não importando sua origem, devem passar por um processo de verificação de vírus antes de sua utilização.

5.7 Mesa e Tela Limpa

Para evitar exposição desnecessária, documentos ou arquivos contendo informações sensíveis:

- Não devem ser deixados sobre a mesa de trabalho ou expostos em tela. Os usuários devem tomar cuidado com a exposição de informações sensíveis na tela de computadores em ambientes de circulação ou públicos. Caso se ausente do seu local de trabalho, o Colaborador deve bloquear sua estação de trabalho (computador) teclas Ctrl + Alt + Del, evitando que outras pessoas possam utilizá-lo em seu lugar.
- Toda documentação deve ser devidamente guardada em gavetas ou armários com chave quando se ausentar da mesa.
- Devem ser retirados da impressora, imediatamente após a impressão.
- Devem ser armazenados em local seguro e adequado, principalmente quando não estiverem em uso.
- Devem ser descartados adequadamente (se possível picotados antes de jogar no lixo).
- No momento de concluir uma reunião presencial numa sala, verifique que a sala não tenha documentos na mesa e que dados na lousa ou em painéis estejam devidamente apagados.

5.8 Uso de Sistemas de Redes Sociais

Atualmente, o acesso às redes sociais (exemplo: Facebook, LinkedIn) já faz parte do cotidiano de grande parte dos usuários da Internet. Entre outros motivos, são utilizadas como busca de candidatos para vagas de emprego, pesquisas de opinião e mobilizações sociais. Porém vale ressaltar que possuem riscos e que alguns cuidados devem ser tomados para evitá-los.

Os principais riscos associados às redes sociais são:

- Invasão de privacidade;
- Furto de identidade;
- Invasão de perfil;
- Uso indevido de informações;
- Danos à imagem;
- Vazamento de informações;

- Recebimento de mensagens contendo códigos maliciosos;
- Instalação de programas maliciosos;
- Acesso à conteúdos impróprios ou ofensivos;

A concessão de acesso às redes sociais implica na utilização adequada, conforme recomendações abaixo:

- É proibido publicar assuntos que comprometam a imagem da CPI CENTRAL, seus clientes ou colaboradores;
- Respeitamos a liberdade de expressão de cada indivíduo. Porém, é recomendado evitar publicar assuntos que provoquem conflitos ou mal-estar com terceiros;
- Não publicar informações do negócio sem prévia autorização por parte da diretoria da CPI CENTRAL.

Cabe ao usuário, manter o sigilo das informações da CPI CENTRAL, sendo de sua total e exclusiva responsabilidade qualquer informação compartilhada nas redes sociais. Ele deverá comunicar imediatamente ao suporte de TI qualquer situação que possa colocar em risco as informações da CPI CENTRAL.

5.9 Uso de Sistemas de Mensageria

Os sistemas de mensageria (exemplo: Whatsapp, Telegram), viraram mais um mecanismo de comunicação diária. No entanto, o mau uso pode deixar CPI CENTRAL exposta. Seguem algumas medidas preventivas a serem adotadas:

- É vetada a criação de grupos no WhatsApp utilizando a logomarca, nome ou qualquer outra identificação visual da CPI CENTRAL, como também comunicar institucionalmente e trocar informações por ferramentas de mensageria;
- É proibido encaminhar qualquer tipo de informação confidencial por meio de sistemas de mensageria;
- Evite encaminhar qualquer tipo de informação a terceiros que pudesse comprometer a imagem da CPI CENTRAL

5.10 Engenharia Social

Engenharia social é a técnica de se aproveitar da boa-fé de pessoas para obter informações que possibilitem ou facilitem o acesso aos recursos computacionais de uma organização por parte de usuários não autorizados. Dentre as informações procuradas destacam-se as seguintes:

- Senhas de acesso;
- Listas de usuários;
- Tipos e versões de sistemas operacionais usados;

- Dados sigilosos sobre produtos e processos da organização.

Os contatos podem ser feitos de forma direta entre o engenheiro social e a vítima por meio de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido. Outra forma de contato é por centrais telefônicas parecidas com serviços de telemarketing onde um banco de dados com informações da pessoa e da empresa é criado e atualizado com base nas conversas destes contatos.

Também podem ser feitos por meio da utilização de softwares ou ferramentas para invadir, como por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar e apagar o e-mail imediatamente.

Em seguida, algumas precauções a serem adotadas:

- Sempre suspeite de qualquer Instituição ou pessoa física desconhecida solicitando fornecimento de informação confidencial, incluindo dados pessoais. Lembre-se que o engenheiro social utiliza mecanismo para gerar simpatia com a vítima, exemplo: ele poderia se fazer passar por um representante de uma instituição, amigo de um colega ou familiar.

- Caso ocorra algum evento onde uma instituição específica solicita certa informação, informe para a pessoa que você retornará a ligação. Em vez de ligar para o número pelo qual a pessoa ligou, utilize os números oficiais da instituição;

- Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertos: .bat, .exe, .src, .lnk, e .com, ou de quaisquer outros formatos alertados pela área de TI.

- No momento de receber uma mensagem, revise o e-mail do remetente. Verifique que o e-mail corporativo coincide com a página de internet;

- Nunca forneça informação confidencial a um e-mail pessoal, exemplo: (gmail, Hotmail, Yahoo).

5.11 Impressão de Documentos

Caso tenha a necessidade de imprimir documentos com informação confidencial, o Colaborador deverá tomar as seguintes medidas:

- Não deixar documentos impressos na impressora, principalmente se ela for de uso compartilhado;

- Guardar informação confidencial em pastas e resguardar em lugares seguros com chave;

- Se o documento que contém informação confidencial não for mais necessário, o colaborador deverá picotar ou rasgar da melhor forma possível para evitar qualquer tipo de vazamento;

- Está totalmente proibido fornecer qualquer tipo de documentação com informação confidencial, sem autorização previa pela diretoria da CPI CENTRAL;

6. Responsabilidades

Diretoria

- Promover uma forte cultura, conforme os requisitos desta política e nos termos da legislação em vigor;
- Conscientizar e divulgar a LGPD junto aos colaboradores e terceiros;
- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir os riscos;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Atender e solucionar as demandas externas e internas relacionadas à LGPD, inclusive aquelas advindas por ocasião de edição de norma técnica expedida pelo ANPD – Autoridade Nacional de Proteção de Dados;
- Revisar, aprovar e atualizar esta política quando houver necessidade de alteração;
- Analisar os relatórios de teste e monitoramento baseado nos requerimentos desta política e garantir que as ações corretivas sejam tomadas para remediar qualquer tipo de deficiência;
- Apoiar a implantação e a manutenção desta política e do cumprimento da legislação em vigor;
- Atender as solicitações e fiscalizações da ANPD;
- Fornecer treinamento e comunicação adequada dos itens desta política;
- Revisar e atuar em caso de ocorrência de exceção a esta política;
- Garantir que os mecanismos estejam em vigor para o registro e monitoramento apropriado de documentos relacionados a esta política;
- Garantir que sejam tomadas as ações corretivas adequadas para remediar deficiências ou incidentes reportados com o apoio do Comitê de Segurança da Informação.

Assessoria Jurídica

- Interpretar leis e regulamentações aplicáveis a esta política;
- Oferecer orientação jurídica em relação às leis e regulamentações aplicáveis para os segmentos, áreas de suporte e controle;
- Garantir que as disposições das Políticas reflitam as determinações definidas nas leis e regulamentações aplicáveis.

Colaboradores

- Ler, entender e praticar esta política e outras relacionadas;
- Informar previamente ao superior imediato ou Diretoria quando houver algum evento de não conformidade com a legislação vigente ou com os princípios desta política;
- Participar de forma periódica nos treinamentos preventivos;
- Questionar ou denunciar em caso de qualquer dúvida referente aos assuntos expostos.
- Não praticar qualquer ato que, embora não previsto em procedimentos de controle, seja contrário aos princípios desta Política, à legislação em vigor e aos princípios da ética, moral e bons costumes.

7. Dúvidas ou Denúncias

Em caso de dúvidas ou preocupação sobre como agir apropriadamente, ou se souber de alguma atividade que saia dos padrões éticos desta Política, sugerimos utilizar os seguintes canais:

Converse com o seu superior imediato: ele é o seu principal orientador. Sugerimos que, se não for lhe causar nenhum desconforto, você converse primeiro com o seu superior imediato. Ele poderá responder algumas das suas perguntas relacionadas ao dia a dia no trabalho e assuntos que envolvam esta política.

Para se comunicar com a Diretoria você pode utilizar o e-mail:

marcia@cpicentral.com.br

Não Retaliação: é proibida qualquer retaliação contra qualquer pessoa que, de boa-fé denuncie atividade ou comportamento que acredite ser ilegal, antiético ou uma violação de nossas políticas. A retaliação é contra os valores da CPI CENTRAL e não será tolerada.

8. Exceções à esta política

As solicitações de práticas de atos que possam ser considerados como regras de exceção ou que, por não estarem bem definidos, necessitem de ajustes na aplicação e interpretação desta política, deverão ser feitas de forma escrita para a Diretoria da CPI CENTRAL.

9. Sanções e Penalidades

CPI CENTRAL não tolera de forma direta ou indireta nenhum tipo de prática antiética ou ilícita que viole os direitos de privacidade de cada Titular. Qualquer violação da Lei aplicável ou desta política poderá causar graves danos a CPI CENTRAL e aos seus dirigentes e, como resultado, poderia ensejar a aplicação

de penalidades disciplinares, multas, ações judiciais, processos administrativos, perda da licença e, ainda, a quebra de contrato com o Cliente.

Assim sendo, a violação da lei aplicável e/ou desta política por qualquer Colaborador ou empresa vinculada a CPI CENTRAL, ensejará sanções disciplinares, com a gradação da pena, conforme a infração praticada, a qual poderá resultar em advertência, demissão por justa causa, rescisão do contrato de fornecimento ou prestação de serviços e responsabilização pela indenização dos danos causados, inclusive com o infrator podendo ser levado às autoridades policiais e judiciais, se a infração for configurada como criminosa.

Não obstante as penalidades previstas, os Colaboradores poderão ser orientados pela Diretoria a imediatamente interromper condutas inadequadas ou inapropriadas nos termos desta Política.

10. Retenção de registros

CPI CENTRAL deve documentar, arquivar e guardar os registros das atividades desenvolvidas e decisões proferidas em procedimentos administrativos ou judiciais decorrentes da aplicação desta Política, no prazo legal, em conformidade com a legislação aplicável da jurisdição onde opera.