ÍNDICE

1. OBJETIVO

Estabelecer diretrizes e requisitos quanto a utilização de recursos de tecnologia da informação e quanto a segurança da informação com o objetivo de garantir a continuidade dos negócios da companhia, bem como zelar pela sua imagem e reputação.

2. APLICAÇÃO E ALCANCE

Todas as atividades executadas para atender os objetivos desta política devem estar em harmonia com os valores da Cinpal. Esta política aplica-se a todos os empregados independentemente de suas atribuições, responsabilidades e nível hierárquico –, consultores externos, colaboradores temporários, parceiros comerciais, clientes, fornecedores ou prestadores de serviços entre outros que possuam acesso aos dados, informações, serviços, sistemas, recursos de tecnologia da informação e recursos de propriedade da Cinpal.

3. REFERÊNCIAS

- ABNT ISO/IEC 27002:2013.
- Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais.

4. DEFINIÇÕES

- PTI: Política de Tecnologia da Informação da Cinpal.
- CSI: Comitê de Segurança da Informação.
- LGPD: Lei Geral de Proteção de Dados Pessoais.
- DPO: Profissional da Cinpal que atua como canal de comunicação (*Data Protection Officer*) entre os titulares de dados pessoais e a Autoridade Nacional.
- TI: Área de Tecnologia da Informação da Cinpal.

Usuário: Qualquer pessoa física (empregado, colaborador ou prestador de serviço) ou jurídica a quem foi fornecido oficialmente pela Cinpal uma conta ou um meio de acesso ao ambiente informatizado e/ou ao ambiente físico da Cinpal.

5. RESPONSABILIDADES

5.1 Diretoria

- Aprovar a PTI e suas revisões, disponibilizar recursos adequados para o cumprimento dos requisitos;

- Apoiar na divulgação e cumprimento dos controles estabelecidos.

5.2 Gestores

- Divulgar a PTI;
- Criar e manter em sua área de responsabilidade um ambiente seguro que esteja em conformidade com os controles estabelecidos;
- Comunicar às áreas de Recursos Humanos e Tecnologia da Informação possíveis violações e não cumprimento da PTI pelo colaborador.

5.3 Área de Recursos Humanos

- Garantir o conhecimento e treinamento adequado da PTI a todos os envolvidos (empregados, colaboradores e terceiros);
- Estabelecer sanções apropriadas quanto ao descumprimento da PTI;
- Aplicar sanções previstas nos profissionais que descumprirem a PTI.

5.4 Área Jurídica

- Garantir que a PTI e suas normas derivadas estejam em conformidade com as leis aplicáveis;
- Avaliar contratos de fornecedores a luz da PTI.

5.5 Suprimentos ou qualquer outra área que contrate fornecedores

- Garantir que todos os fornecedores contratados, dentro de sua área de atuação, conheçam, compreendam e cumpram os requisitos da PTI;
- Utilizar o cumprimento da PTI no processo de avaliação de fornecedores.

5.6 Funcionários, colaboradores e terceiros

- Conhecer, compreender e agir conforme os requisitos da PTI;
- Não divulgar ou compartilhar qualquer informação ou dados para pessoas não autorizadas.

5.7 CSI

- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos;
- Propor alterações nas revisões da PTI e a inclusão, a eliminação ou a

mudança de normas complementares;

- Avaliar os incidentes de segurança da informação e propor ações corretivas;

- Avaliar as medidas cabíveis nos casos de descumprimento da PTI e de normas complementares;

- Aprovar a políticas e normas derivadas da PTI, bem como outros que formalmente necessitarem da aprovação do CSI;

- Eleger o DPO;

- Analisar criticamente a gestão da segurança da informação e tomar ações para a melhoria contínua dos processos relacionados.

5.8 DPO

- Exercer a função de Encarregado do tratamento de dados pessoais, conforme definido na LGPD.

5.9 Tecnologia da Informação

- Atuar de forma a garantir que as diretrizes e requisitos da PTI e suas normas complementares sejam implantadas;

- Propor soluções tecnológicas e de processo voltados a melhoria no atendimento das diretrizes e requisitos da PTI e suas normas complementares.

6. DIRETRIZES GERAIS

Todos dados e informações obtidas, processadas e disponibilizadas pela Cinpal devem estar em conformidade com os princípios de disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditoria.

Todos os profissionais (contratados ou terceiros) com acesso a dados ou informações devem estar cientes de suas responsabilidades pela segurança das informações da Cinpal e devem atuar em conformidade com esta política.

De forma apropriada, toda e qualquer pessoa antes de acessar a rede corporativa ou informações, seja em meio eletrônico ou físico, disponibilizadas pela Cinpal deve tomar conhecimento e compreender esta política.

Todos os prestadores de serviços contratados que de alguma maneira possam ter acesso às informações ou dados em formato físico ou digital devem ter em seus

contratos cláusulas que atendam as normas desta política.

Para proteção da infraestrutura computacional, a área de TI deve fazer uso de ferramentas, controles e processos contra ameaças cibernéticas externas e internas.

Para minimizar o risco de vazamento de informações, devem ser utilizadas ferramentas preventivas em todos os dispositivos móveis, estações de trabalho, serviços de correio eletrônico (*e-mails*), serviços de navegação Web, impressão e, sempre que tecnicamente e financeiramente viável, o uso de criptografia para dados em repouso e em transporte.

Todo o ambiente computacional e físico da Cinpal deve ser monitorado e os acessos controlados com o objetivo de cumprir os requisitos desta política.

Processo de gestão de risco e continuidade dos negócios deve ser estabelecido e mantido para apoiar as decisões da alta direção.

O processo de gestão orçamentária deve garantir recursos adequados para o cumprimento dos requisitos definidos nesta política.

6.1 Comitê de Segurança da Informação (CSI)

O Comitê de Segurança da Informação deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano. Um membro da diretoria, o Gerente de TI e o DPO devem fazer parte do CSI.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

6.2 Classificação da informação

É de responsabilidade do gestor de cada área estabelecer o nível de confidencialidade da informação ou dado, em formato físico ou digital, gerada por sua área de acordo com os critérios a seguir.

6.2.1 Informação Pública

É toda informação ou dado que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral. Sua divulgação não causa qualquer dano a Cinpal ou a outras partes interessadas.

6.2.2 Informação Interna

É toda informação ou dado que só pode ser acessada por empregados e terceiros enquanto estiverem desempenhando atividades para a Cinpal. São informações ou dados que possuem um grau de confidencialidade que sua divulgação ou acesso não autorizado pode comprometer a imagem da Cinpal.

6.2.3 Informação Confidencial

É toda informação ou dado que pode ser acessada por usuários da Cinpal e por parceiros explicitamente indicados. A divulgação ou acesso não autorizado a essa informação pode causar impacto grave (financeiro, de imagem ou operacional) ao negócio da Cinpal.

6.2.4 Informação Restrita

É toda informação ou dado que pode ser acessado somente por usuários da Cinpal explicitamente indicado pelo nome ou por área a que pertence. A divulgação ou acesso não autorizado dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da Cinpal.

6.2.5 Dado Pessoal

Dado tipificado na LGPD.

6.2.6 Dado Pessoal Sensível

Dado tipificado na LGPD.

6.3 Tratamento da informação

Toda informação ou dado gerado no exercício das atividades internas ou no desenvolvimento do trabalho externo, ou seja, fora dos limites físicos da empresa, é considerada patrimônio do Cinpal, devendo ser usada exclusivamente para atender aos interesses da mesma, podendo ainda ser fornecida a terceiros, respeitadas as restrições da classificação das informações, contratos e de leis especificas como a LGPD.

Os profissionais com acesso a dados e informações são responsáveis por classificá-las e a fazer uso dos recursos disponibilizados pela companhia no tratamento delas.

Sempre que tecnicamente possível com os recursos adotados na Cinpal, deve-se utilizar criptografia ou proteções por senha para armazenar e transmitir informação interna, confidencial ou restrita.

Deve-se verificar a autenticidade e a legitimidade de todos os destinatários ao enviar uma informação através de qualquer meio.

6.3.1 Tratamento de dados pessoais e dados pessoais sensíveis

O tratamento de dados pessoais e dados pessoais sensíveis devem seguir os princípios definidos na LGPD:

- Finalidade;
- Adequação;
- Necessidade;

- Livre acesso;
- Qualidade dos dados;
- Transparência;
- Segurança;
- Prevenção;
- Não discriminação;
- Responsabilização e prestação de contas.

Conforme determinado no artigo 5º na LGPD, deve-se manter atualizado o Relatório de Impacto a Proteção dos Dados Pessoais.

Deve-se estabelecer um procedimento operacional específico para tratamento de dados pessoais e dados pessoais sensíveis e recursos técnicos computacionais devem ser empregados para apoiar o cumprimento dos requisitos.

6.4 Gestão de acessos

A gestão de acesso deve seguir o princípio de confiança zero que consiste em:

- Verifique explicitamente: sempre autentique o acesso com o maior número de informações disponíveis.
- Concessão de privilégios mínimos: conceder estritamente o acesso necessário para a execução das atividades, incluindo o horário permitido e o prazo de acesso.
- Presunção de violações: reduza ao mínimo necessário o raio de acesso concedido e monitore sempre.

Todos os funcionários, estagiários, temporários e terceiros autorizados para acessar os ambientes físicos e lógicos da Cinpal devem ter identificação que permita rastrear de forma inequívoca os acessos aos ambientes físicos restritos e aos sistemas informatizados.

Deve-se armazenar os registros de acesso ou trilhas de auditoria em todo ambiente computacional da Cinpal em que for tecnicamente viável, para todas as plataformas, de forma que seja possível a identificação de quem, quando, como e o que foi acessado. Todos esses registros devem ser protegidos contra modificações e ter o acesso controlado.

Um processo de liberação de acesso deve ser estabelecido objetivando que a aprovação de um acesso seja concedida após uma análise crítica, conforme os requisitos estabelecidos nesta política.

Os sistemas devem ser configurados para utilização de senhas fortes e, sempre que possível tecnicamente e apropriado, deve-se fazer uso de fator múltiplo de autenticação. A área de TI deve se utilizar dos recursos disponíveis para bloquear contas ou dispositivos de identificação com tentativas de acessos inválidos.

Os acessos para usuários externos (prestadores de serviço), devem ser liberados com prazo de expiração estabelecido.

6.4.1 Contas de administração

As contas de administração devem fazer uso de fator múltiplo de autenticação. Exceção apenas nos casos que forem tecnicamente inviáveis.

6.4.2 Contas de serviço

As contas de serviço (contas específicas utilizadas por aplicações) devem ser específicas (individualizadas). Exceções devem ser aprovadas pela gerência de TI e devem ser documentadas.

6.4.3 Sistemas de segurança

O acesso aos sistemas de segurança deve ser concedido somente aos profissionais de segurança da informação e patronal (guardadas as atribuições do cargo) para o cumprimento de seus deveres e deve seguir os demais requisitos de gestão de acesso.

6.4.4 Perfil de acesso aos sistemas de negócio

O perfil de acesso ao sistema de negócio concedido ao usuário deve ser aprovado pelo gestor do setor do usuário e pelo gestor responsável pela função do sistema de negócio. O perfil deve ser validado com frequência mínima anual.

6.4.5 Acesso a banco de dados

A atualização de transações (inclusão, alteração e exclusão) nos bancos de dados deve ser processada unicamente pelas aplicações. Os sistemas de bancos de dados devem estar configurados para manter registro (log) das transações. É permitido ao profissional administrador do banco de dados:

- executar apenas operações de manutenção com foco em atender os objetivos de disponibilidade, capacidade e segurança;
- executar funções de consulta (*query*) para atender necessidades específicas das áreas de negócio, atentando-se as outras definições desta política.

Caso haja necessidade de realizar manutenção de dados diretamente no banco de dados, esta manutenção deve ser aprovada formalmente pelo CSI e documentada (a documentação deve conter no mínimo a data da manutenção, o tipo de manutenção, a justificativa, o conteúdo original do dado e o novo conteúdo do dado). Esta é uma atividade extrema e que só deve ser executada após eliminadas todas as possibilidades de serem realizadas através da aplicação pertinente e depois de avaliada e recomendada pelo fornecedor da aplicação.

As contas de acesso ao banco de dados (contas de administração) devem ter o mínimo privilégio, ou seja, acessar apenas o necessário e somente com os direitos necessários

para a execução das atividades.

Sempre que tecnicamente e financeiramente possível, deve-se fazer uso de criptografia nos dados armazenados nos sistemas de banco de dados.

6.4.6 Acesso físico a áreas restritas

Todos os locais que contenham recursos críticos para a continuidade dos negócios da Cinpal, incluindo-se informações, devem estar protegidos adequadamente e o acesso ao ambiente deve ser controlado e monitorado.

6.4.7 Acesso de prestadores de serviço

O acesso concedido a prestadores de serviço deve ter validade definida e configurada no sistema. As responsabilidades e as restrições devem constar nas cláusulas do contrato de prestação de serviço. O prestador de serviço deve ser acompanhado por um colaborador sempre que necessitar acessar alguma área crítica da Cinpal.

6.4.8 Responsabilidade dos gestores

Os gestores são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da companhia. Cabe aos gestores verificar se os seus subordinados estão acessando apenas as rotinas compatíveis com as suas respectivas funções.

6.4.9 Auditorias de acesso

O Departamento de TI deve realizar auditorias periódicas do uso dos recursos de TI e dos acessos aos sistemas informatizados com o objetivo de validar e garantir o cumprimento da PSI.

Cabe ao CSI definir os cargos da TI responsáveis pelas auditorias e a contratação de auditorias externas, sempre que necessário, bem como a análise crítica dos resultados das auditorias e a tomada de ações necessárias para garantir a efetividade do cumprimento da PSI.

6.5 Colaboradores

Não é permitido acumular ou manter intencionalmente dados pessoais além daqueles relevantes na condução do seu negócio. Todos os dados pessoais que porventura sejam armazenados devem ser considerados dados confidenciais e não devem ser usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais não devem ser transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (*e-mails*) usados pelos empregados da Cinpal.

Não é permitido aos empregados, colaboradores e prestadores de serviço

armazenarem dados pessoais nas instalações físicas e no ambiente informatizado da Cinpal. Exceções formalmente autorizadas pela diretoria devem ser controladas e mantidas por tempo determinado e não podem ser armazenadas nos servidores de empresa, e jamais poderão fazer parte da rotina de cópia de segurança.

6.5.1 Admissão, férias, afastamento, suspensão, transferência e demissão

Cabe a área de Recursos Humanos através de um processo (eletrônico ou físico) garantir o fornecimento de informações precisas e no tempo adequado a área de TI e, se apropriado, a área de segurança patrimonial de forma a garantir que os requisitos desta política sejam atendidos quando da admissão, férias, afastamento, suspensão, transferência, promoção e demissão de um empregado ou colaborador.

Durante o processo de admissão, a área de Recursos Humanos é responsável por dar conhecimento apropriado sobre esta política e documentar a ciência através do Termo de Confidencialidade e Sigilo e do Termo de Uso de Recursos de Tecnologia da Informação.

6.6 Gestão de projetos

Todos os projetos das áreas de negócio da Cinpal devem estar em conformidade com as diretrizes e requisitos estabelecidos nesta política, de forma que os princípios da segurança da informação estejam presentes desde a concepção do projeto até a sua conclusão.

6.7 Gestão de ativos

Todos os ativos de tecnologia da informação devem ser identificados, inventariados e protegidos de acessos indevidos.

Somente os profissionais da área de TI, terceirizados autorizados pela área de TI ou profissionais fornecidos pelo fabricante do ativo são responsáveis pelas atividades de instalação, manutenção e desinstalação dos recursos de tecnologia da informação.

Os ativos devem ser divididos em três grupos:

- Software: programas de computador em geral, independente do dispositivo em que operam e da finalidade de uso.
- Hardware: equipamentos computacionais e acessórios correlatos que compõe os recursos de TI, como computadores, impressoras, equipamentos de armazenamento de dados, equipamentos de comunicação etc.
- Informação: qualquer dado em formato digital ou físico relevante para os negócios da companhia (ver classificação da informação).
- Infraestrutura: todos os equipamentos ou serviços que suportam as operações.

6.7.1 Ciclo de vida do ativo

A gestão do ativo está dividida em cinco fases:

- Planejamento: Fase de avaliação dos ativos em uso e de alinhamento dos ativos disponíveis com as a estratégia da companhia. A padronização dos recursos de TI deve sempre ser almejada nesta fase, bem como a análise da capacidade de evolução técnica do recurso.
- Aquisição: Fase de definição do padrão técnico, homologação do ativo e de fornecedores e aquisição e/ou contratação.
- Implantação: Fase de instalação e disponibilização para uso. Deve seguir as definições estabelecidas para a gestão de mudanças.
- Gerenciamento: Fase de controle, apoio técnico, manutenção, atualização e monitoração.
- Obsolescência: Fase em que o ativo deixa de ser útil e sua forma de descarte deve tratada.

6.7.2 Aquisição

A aquisição de qualquer recurso de TI está condicionada à análise e aprovação da área de TI. Cabe a área da TI avaliar a compatibilidade e a homogeneidade com o ambiente tecnológico em vigor, a segurança e os riscos envolvidos. Cabe exceção quando da aquisição de ativos de TI que são fornecidos como parte integrante de equipamentos fabris. Nestes casos, a área de TI deve ser consultada e fazer parte do projeto com o objetivo de assegurar o cumprimento desta política.

6.7.3 Obsolescência

Todos os recursos que contenham dados ou softwares licenciados para a Cinpal devem passar por processo que garanta a eliminação definitiva dos dados e dos arquivos de licenciamento antes de serem destinados para descarte ou reutilização.

A exclusão de dados, seja em formato físico ou digital, deve seguir primeiramente as regulamentações legais, como trabalhistas, tributárias e a LGPD, e secundariamente os requisitos do negócio.

6.7.4 Inventário

Os ativos de software e hardware devem ser inventariados, identificados e registrados. Os dados do inventário devem permitir facilmente a identificação do ativo, sua localização e seu objetivo de uso. Estes dados devem ser mantidos atualizados. O processo de inventário deve certificar o uso correto das licenças de software.

6.7.5 Licenças de uso

Todos os softwares instalados no ambiente de tecnologia da Cinpal devem possuir licença

de uso legalmente adquiridas e somente a área de TI está autorizada a fazer a instalação ou permitir a instalação por outro. Mesmo os softwares que não exigem pagamento da licença para uso comercial estão condicionados a esta norma.

6.8 Gestão de riscos

Todos os riscos à segurança da informação ou a continuidade dos negócios devem ser identificados através de um processo de análise de ameaças, probabilidade de ocorrência das ameaças e os respectivos impactos sobre os negócios da Cinpal caso o evento se realize. Um procedimento documentado deve ser estabelecido definindo a metodologia de gestão de risco.

6.9 Tratamento de incidentes

O plano de resposta a incidentes de TI (falhas dos sistemas de informação, inoperância de serviços, não obtenção de serviço, erros resultantes de dados incompletos ou inconsistentes, violação de sigilo e/ou confidencialidade, tentativas de intrusão, ocorrências de vírus, dentre outras) deve ser executado por uma equipe especializada e treinada. Deve-se fazer uso de ferramentas adequadas para o monitoramento e tratamento desses incidentes. O processo deve ser documentado e deve estabelecer tratamento apropriado para os tipos de incidentes. O tratamento de incidente de segurança da informação deve:

- Estabelecer diretrizes para coleta e preservação de evidências de incidentes;
- Estabelecer um processo formal de comunicação sobre incidentes de segurança da informação que contemple todas as partes interessada

6.10 Continuidade dos negócios

Deve ser estabelecida e documentada uma Política de Recuperação de Desastre (*disaster recovery*) objetivando minimizar ao máximo os impactos causados ao negócio e a outras partes interessadas após um incidente crítico que interfira gravemente nas operações, através da recuperação dos serviços a um nível aceitável, considerando os requisitos da operação.

Levando-se em conta os riscos envolvidos (impacto e probabilidade) e adequações orçamentárias, deve-se manter o ambiente de tecnologia da informação (infraestrutura e sistemas) com redundância adequada (acionamento automático e/ou manual) para atender os requisitos de continuidade dos negócios em casos de incidentes.

6.11 Planejamento da capacidade

A área de TI deve continuamente avaliar a capacidade dos recursos de comunicação, processamento e armazenamento de dados. Esta avaliação deve analisar o consumo de recursos atuais e projetar os recursos futuros, considerando também requisitos de novos negócios e sistemas.

Com base nesta avaliação, a área de TI deve buscar continuamente a otimização do

uso dos recursos, sem sacrificar os requisitos do negócio e deve requisitar durante o período de definição orçamentária, os recursos financeiros necessários (despesas e investimentos) para próximo exercício contábil. Situações não previstas no orçamento devem ser negociadas com a Direção, considerando-se a capacidade dos recursos computacionais em manter a continuidade dos negócios.

6.12 Gestão de mudanças

As mudanças devem ser gerenciadas objetivando:

- Garantir a avaliação do impacto da mudança nos negócios;
- Garantir a utilização de procedimentos padronizados para a execução das mudanças;
- Executar as mudanças aprovadas de forma eficiente e dentro de um risco aceitável para o negócio.

As manutenções e mudanças na infraestrutura computacional devem ser planejadas para serem executadas mensalmente ou em intervalos menores quando se tratar de mudanças emergenciais, como atualização de segurança, objetivando à sustentação e a atualização do ambiente. As mudanças referentes a segurança devem ser priorizadas em relação as de melhoria de desempenho. O calendário de mudanças deve publicado periodicamente, visando à informação e a preparação da base usuária para tal ação.

Os ambientes de produção, homologação e testes devem ser segregados, incluindo redes de comunicação, e com acesso restrito apenas a usuários previamente autorizados.

As mudanças dos ambientes em nuvem devem seguir as recomendações dos provedores e fornecedores quando executados pela área de TI da Cinpal.

Os ambientes em nuvem com a administração terceirizada devem ser contratados com cláusulas de gestão de mudanças compatíveis com os requisitos desta política.

6.12.1 Atualização de sistemas

Todo sistema que necessite de atualização deve ser feito após uma avaliação prévia, exceto atualização de base de dados de antivírus, de forma que uma atualização ainda não sedimentada não crie paralisação de serviços. As atualizações devem ser analisadas considerando-se o grau de criticidade de cada uma. As atualizações devem ser realizadas primeiramente em um ambiente teste, para só depois serem colocadas em ambiente de produção. Exceções devem ter o risco mapeado, analisado e aprovado pela CSI. Devem-se efetuar cópias de segurança, antes de atualizações.

Nenhum sistema, ou sua forma de utilização, deverá ser modificado sem a autorização prévia e formal de seus responsáveis e da área de TI. Todas as manutenções e/ou parametrizações realizadas nos sistemas devem ser registradas, documentadas, homologadas e aprovadas pelos responsáveis. Necessidades de mudanças

emergenciais devem passar pelos mesmos procedimentos obrigatoriamente, independentemente de sua criticidade, levando em consideração apenas a sua prioridade de atuação.

Quando apropriado, a área de TI deve fornecer treinamento ao responsável do sistema e aos responsáveis das áreas usuárias que serão afetadas sobre a funcionalidade e operação do mesmo, incluindo aspectos de segurança e integridade dos dados.

Devem existir ambientes segregados para desenvolvimento, teste / homologação e produção dos sistemas. O ambiente de testes / homologação deve simular as mesmas condições encontradas no ambiente de produção, guardadas as proporções de volumes de dados.

6.12.2 Controle de versão e código-fonte

A área de TI é responsável por zelar pela biblioteca de códigos-fonte de cada sistema. Somente usuários designados e processos automatizados poderão acessar programas em código-fonte. A integridade dos códigos-fonte deve ser salvaguardada utilizando uma combinação de controles de acesso e restrição de privilégios.

As documentações dos sistemas devem ser atualizadas sempre que houver alguma modificação nos mesmos. Devem ser registrados históricos de versão, a alteração executada e o motivo da alteração, por meio da adoção de ferramenta de controle de versão.

O acesso de prestadores de serviço de desenvolvimento / manutenção de sistemas aos códigos fonte somente deve ser feito por motivos válidos de ação sobre os mesmos e com acompanhamento de usuário autorizado a acessar tais códigos-fonte.

Compiladores e editores de códigos-fonte não devem estar acessíveis a usuários que não façam parte da equipe de desenvolvimento em TI.

As versões antigas dos códigos-fonte devem ser arquivadas com indicação clara e precisa da data e período em que estiveram em produção, juntamente com os softwares de suporte, se necessário. A manutenção e a cópia de bibliotecas de códigos-fonte devem estar sujeitas aos procedimentos de controle de mudança.

O código-fonte dos sistemas não deve ser alterado diretamente em produção em resposta a uma mudança emergencial. Deve ser criada uma versão controlada, temporária, a qual deverá ser executada até que o programa em produção possa ser alterado e substituído.

6.13 Gestão dos prestadores de serviço

Todo prestador de serviço de Tecnologia da Informação deve passar por um processo de avaliação quanto a sua capacidade de atender os requisitos técnicos contratuais antes de se firmar o contrato. Os critérios de avaliação devem ser adequados aos riscos de segurança da informação do serviço a ser executado. As evidências da avaliação devem ser documentadas e armazenadas.

Todo contrato celebrado com estes prestadores de serviço deve conter cláusulas

referentes a:

- Metas de atendimento (SLA – *Service Level Agreement*);
- Comunicação imediata quanto a ocorrência de incidentes de segurança da informação;
- Restrições específicas quanto ao acesso e uso dos recursos de TI da Cinpal;
- Explicitação do seu papel e de sua responsabilidade como Operador de dados pessoais, se aplicável.

Cabe a área de TI monitorar e avaliar periodicamente a qualidade dos serviços prestados pelos fornecedores de tecnologia da informação.

6.14 Monitoramento

O acesso aos registros (arquivos, imagens e áudios) dos sistemas de segurança são restritos aos profissionais de segurança da informação e patronal (guardadas as atribuições do cargo) para o cumprimento de seus deveres. Somente o CSI pode autorizar o acesso a estes registros para outras pessoas. Os registros devem ser armazenados pelo tempo necessário para cumprir obrigações legais e responder as necessidades de gestão da Cinpal, após este período, os registros devem ser destruídos de maneira a impossibilitar a sua recuperação.

Para garantir o cumprimento das normas definidas nesta política, a Cinpal poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis (*wireless*) e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação da Diretoria ou por determinação do Comitê de Segurança da Informação;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua posse;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

6.15 Auditoria

Cabe ao SCI a utilização de auditorias independentes para verificar a efetividade das políticas e controles de segurança da informação, assim como a maturidade do sistema de gestão. A periodicidade e o foco da auditoria devem ser adequados ao resultado do monitoramento, as mudanças do ambiente tecnológico e do tratamento de incidentes. Recursos orçamentário devem ser previstos anualmente para este processo.

7. NORMAS GERAIS

7.1 Servidor de arquivos

Deve ser disponibilizado no servidor de arquivos da Cinpal acesso a arquivos compartilhados através de pastas:

- Departamentais ou grupos de trabalho: Deverá conter arquivos pertinentes ao departamento, setor ou grupo de trabalho. As definições de nível de acesso devem ser realizadas pelo responsável do setor, departamento ou grupo de trabalho.
- Público: Arquivos de armazenamento temporário e que devem ser excluídos diariamente.

Como padrão (não obrigatório), todo usuário que acessa a rede deve ter uma pasta no servidor de arquivo para gravação dos arquivos de trabalho. O acesso a pasta deve ser restrito ao usuário e ao seu superior hierárquico.

Sempre que tecnicamente possível, não deve ser permitida a gravação de arquivos pelos usuários nas unidades de armazenamento local. Os usuários devem ser informados sobre os locais corretos para armazenamento de arquivos de trabalho.

A disponibilização de recursos em nuvem para armazenamento de dados deve seguir as mesmas diretrizes.

7.2 Propriedade intelectual

É de propriedade da Cinpal todos os “designs”, criações ou procedimentos desenvolvidos para a Cinpal por qualquer empregado ou profissional contratado.

7.3 Internet

A internet deve ser utilizada apenas para fins profissionais e seu acesso deve ser autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na Cinpal. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição dos gerentes e diretores da Cinpal, com base em recomendação da área de TI.

O Termo de Uso de Recursos de Tecnologia da Informação deve explicitar:

- Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros;
- É proibido fazer o *download* de programas provenientes da Internet nos microcomputadores da Cinpal, sem expressa autorização da área de TI;
- Não é permitido realizar *download* de arquivos que não façam parte do trabalho.

7.3.1 Acesso a convidados

O acesso à Internet concedido a visitantes e a clientes deve ser restrito e controlado, não permitindo o acesso a conteúdo conflituoso com os requisitos desta política. Deve-se fazer uso de ferramentas que possibilite a identificação do usuário (*captive portal*, por exemplo), prover um termo de uso que deve ser aceito e os acessos devem ser registrados e armazenados por no mínimo 1 ano, atendendo a Lei 12.965, Marco Civil da Internet. Este item aplica-se ao acesso concedido aos colaboradores cujos quais obtiverem acesso para uso particular em seus próprios dispositivos.

7.4 Datacenter

Somente os profissionais autorizados das áreas de TI e segurança patrimonial devem possuir acesso ao Datacenter. A liberação de acesso para estes profissionais deve ser controlada e autorizada pelo CSI.

Profissionais contratados para execução de serviços no Datacenter devem ser acompanhados por um profissional de TI durante sua permanência no Datacenter.

Pode-se justificar a entrada de outras pessoas no Datacenter, apenas em emergências, quando a segurança física do Datacenter for comprometida,

O Datacenter deve ter monitoramento de temperatura, umidade, fumaça e energia.

7.5 Acesso à rede corporativa

O acesso à rede de dados da Cinpal (local, WAN ou nuvem) deve ser controlado e monitorado objetivando conter acessos não autorizados, conforme definido nos requisitos de Gestão de Acesso desta política.

7.5.1 Segregação da rede

A rede corporativa da Cinpal deve estar segregada, de forma que haja total separação entre o ambiente interno e o ambiente externo tecnológico. Esta segregação deve ser efetuada em domínios de acordo com as necessidades de negócio e deve ser protegida por recursos tecnológicos o qual deve filtrar o tráfego de informações entre os ambientes.

Deve-se utilizar técnicas de separação lógica de redes (VLAN), não só objetivando ganhos de desempenho, mas também aumento da segurança da informação.

7.5.2 Rede WiFi

A rede sem fio (*wireless)* deve ser configurada com protocolos de segurança atualizados (comunicação criptografada). A opção de identificação das redes *wireless* (broadcast SSID) deve estar desabilitada, exceto para rede destinada a visitantes ou clientes.

O acesso à rede WiFi da Cinpal destinada a visitantes deve ser controlada, conforme Marco Civil da Internet (ver requisito Acesso a convidados).

O usuário que utilizar dispositivos móveis pessoais, mesmo quando autorizado pela instituição, é responsável pelos aplicativos e arquivos contidos em seus equipamentos.

7.6 Ambiente de trabalho

7.6.1 Mesa limpa

Objetivando manter um ambiente seguro e organizado, todos os colaboradores e prestadores de serviço devem adequar-se as seguintes regras:

- Documentos e mídias de computadores que não estão em uso não devem ser deixados sobre as mesas, especialmente fora do horário normal de expediente ou em horário de almoço;
- Quando não utilizados, documentos e mídias devem ser armazenados em locais com fechadura e trancados;
- Ao se ausentar da mesa o computador deve ser bloqueado.

7.6.2 Computador

As estações de trabalho (computador de mesa ou portátil) devem estar configuradas para acionar a proteção de tela automaticamente após período de inoperância. O uso da proteção de tela com senha é obrigatório e o profissional ao se ausentar de sua mesa deve acionar este dispositivo de segurança.

os computadores dos usuários devem estar com as portas USB desabilitadas, exceto para computadores portáteis utilizados por gerentes ou cargos superiores. A liberação do uso das portas USB deve ser justificada e aprovada formalmente pela gerência do departamento do solicitante.

Nenhum dado que necessite cópia de segurança deve ser armazenado na estação de trabalho. A segurança dos dados armazenados é um dos objetivos desta política, desta forma, sempre que tecnicamente e financeiramente viável a gravação de dados deve ser desabilitada nos computadores dos usuários.

O usuário deve finalizar as sessões ativas quando se ausentar do equipamento que está utilizando. Configurações de finalização automática de sessão devem ser habilitadas, sempre que tecnicamente viável.

7.6.2.1 **Computador Industrial**

Os computadores utilizados exclusivamente para controle de equipamentos industriais, seja para um sistema supervisório, interface home máquina (IHM) ou outro uso em que o funcionamento do equipamento fabril depende do computador, devem ter outro equipamento sobressalente (configurado, pronto para uso). Considerando o impacto da interrupção do equipamento industrial, o computador sobressalente deve, sempre que apropriado, operar em paralelo garantindo alta disponibilidade. Esta configuração deve ser seguida desde a concepção do projeto de um novo equipamento industrial.

7.6.3 Impressoras

O uso das impressoras corporativas deve estar relacionado somente a questões profissionais. O uso das impressoras para fins pessoais deve ter autorização do gestor da área.

Informações com caráter confidencial devem ser retiradas da impressora logo após a impressão, evitando assim o acesso indevido ou cópia destas informações.

Sempre que adequado e financeiramente viável, deve-se fazer uso de soluções que controlem a utilização das impressoras e garantam a retirada das folhas impressas apenas pelo usuário que solicitou a impressão.

Deve-se sempre buscar soluções que desestimulem o uso das impressoras.

7.6.4 Descarte de material impresso

Todo material impresso destinado a descarte deve ser destruído de forma a impossibilitar a sua leitura e a recomposição do conteúdo. Deve-se utilizar máquinas picotadoras de papel para o atendimento deste requisito

7.7 Dispositivos móveis

Os usuários autorizados a fazer uso de Notebooks, Tablets, Smartphones ou qualquer outro equipamento computacional de propriedade da Cinpal, devem estar cientes de que:

- Os recursos disponibilizados têm como objetivo único a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- Não é permitido a alteração da configuração do equipamento recebido;
- Estão sujeitos a um maior número de auditorias a fim de manter os usuários destes dispositivos alinhados com a estrutura de segurança necessária.

O controle do uso de *smartphones* e *tablets* da Cinpal deve ser feito através de ferramentas de gestão de dispositivo móvel (MDM) para garantir os requisitos definidos nesta política.

7.7.1 7 BYOD (*Bring Your Own Device*)

Não é permitido aos colaboradores da Cinpal o uso de equipamentos particulares para a execução de suas atividades, modelo conhecido pelo acrônimo BYOD. Exceções devem ser aprovadas pela diretoria e pelo CSI após parecer da área Jurídica e de Recursos Humanos. Os equipamentos referentes a estas exceções devem atender aos requisitos desta política.

7.8 Mensagens eletrônicas

7.8.1 Correio eletrônico (e-mail) corporativo

O colaborador autorizado a utilizar o sistema de correio eletrônico deve ser formalmente informado que não é permitido:

- Uso do e-mail corporativo para fins pessoais;
- Uso do e-mail para divulgar ou compartilhar informações sem autorização;
- Acessar a conta de e-mail de outro colaborador;
- Uso do e-mail para prejudicar ou difamar alguém;
- Envio de mensagens em massa;
- Uso de contas pessoais para tratar de informações da empresa;
- Cadastro do e-mail em sites, fóruns ou redes sociais que não sejam da Cinpal.

Em caso de desligamento de um profissional, a sua conta de e-mail deve ser bloqueada e ter a sua senha de acesso alterada imediatamente.

Para o envio de mensagens em massa, deve-se utilizar de sistemas apropriados de forma a mitigar o risco dos domínios da Cinpal serem classificados como *spam*.

Toda mensagem eletrônica enviada deve conter texto de notificação, com o intuito de que destinatários que porventura recebam mensagens indevidas sejam alertados quanto a sua origem e destino. O texto deve ser aprovado pelo CSI e fornecido pela área de TI.

7.8.2 Outros sistemas mensagem eletrônica

A utilização de software de troca de mensagens eletrônicas (WhatsApp, Telegram, Messenger, Skype, Google Talk etc.) nos computadores e em outros dispositivos da Cinpal é restrita a necessidade de atender os requisitos de negócio. O uso deve ser autorizado pela gerência ou diretoria do usuário solicitante.

7.9 Cópias de segurança (Backup)

Todos os dados da Cinpal devem ter cópias de segurança geradas através de rotinas sistemáticas.

Cópias de segurança dos sistemas integrados e dos servidores são de responsabilidade da área de TI e deverão ser feitas diariamente. Devem ser executados testes que garantam a integridade dos dados das cópias de segurança e registros destes testes devem ser mantidos.

As cópias devem ser arquivadas e organizadas de forma a garantir a possibilidade de restauração de dados pelos períodos:

- Cópias diárias: retenção mínima de 2 semanas;

- Cópias mensais: retenção mínima de 1 ano;
- Cópias anuais: retenção por tempo indeterminado. Eliminação de cópias anuais devem ser formalmente aprovadas pela CSI e pela área Jurídica da Cinpal após avaliação das implicações legais.

As técnicas de cópias completa, incremental e diferencial devem ser utilizadas de forma a se fazer uso dos recursos disponíveis de forma eficaz.

A partir da zero hora do dia 1º de janeiro de cada ano, deve-se processar a cópia completa (Backup Full) de todos os arquivos e sistemas. Deve-se manter cópias de segurança em ambientes distintos aos de processamento.

7.10 Sistemas de troca de arquivos

A utilização de troca eletrônica de arquivos só pode ser feita através dos meios homologados pela área de TI e é restrita às atividades relacionadas ao negócio da Cinpal. A área de TI deve prover soluções corporativas que permitam a rastreabilidade e auditoria dos arquivos trocados.

7.11 Armazenamento externo

7.11.1 Dispositivos de armazenamento

Não é permitido o armazenamento de dados da Cinpal em dispositivos externos de armazenamento (*pen drive*, *smart card*, HD, CD, DVD etc.), exceto para fins de cópia de segurança feita pela área de TI ou para guarda e distribuição de material promocional da Cinpal. Exceções a esta determinação devem ser aprovadas pelo CSI e o usuário deve ser formalmente notificado sobre a sua responsabilidade. As exceções devem ser controladas e a verificação do uso deve ser feita pela TI em intervalos apropriados (auditoria).

7.11.2 Armazenamento em nuvem (*cloud computing*)

O armazenamento de dados em nuvem só é permitido nos serviços contratados pela Cinpal. A área de TI deve utilizar dos mecanismos disponíveis para bloquear o armazenamento e a troca de dados em serviços de nuvem não homologados.

7.12 Teletrabalho

A área de TI deve prover meios para que o teletrabalho (*home office*) ocorra respeitando os requisitos desta norma. Riscos relacionados ao teletrabalho devem ser mapeados, analisados e gerenciados, seguindo o estabelecido na Política de Gestão de Riscos.

7.13 Sistema antivírus

Todas as estações de trabalho devem ter instalado o antivírus corporativo homologado pela área de TI.

O sistema de detecção de vírus de computador deve ser centralizado e atualizado de forma automática. Os usuários não devem intervir no uso do programa antivírus, exceto os usuários de computadores portáteis quando fora da rede interna da Cinpal. O programa de antivírus deve ser configurado para eliminar qualquer suspeita de vírus. As estações de trabalho devem estar configuradas para não permitir que o usuário desabilite o programa antivírus instalado. Somente o profissional autorizado da área de TI deve ter acesso às configurações do console central do programa de antivírus.

Todo arquivo em mídia proveniente de entidade externa à Cinpal deve ser encaminhado a área TI para ser verificado pelo programa de antivírus corporativo.

7.14 Rede virtual privada (VPN)

A área de TI deve disponibilizar uma solução de VPN para garantir acesso remoto segura a rede interna da Cinpal. O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

O sistema que permite o acesso através de uma VPN deve ser configurado para não deixar sessões sem uso conectadas e os usuários devem ser orientados a se manter conectado apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

Em caso de fornecedores necessitarem de acesso VPN para uso de algum sistema da empresa, ele deverá assinar obrigatoriamente o Termo de Confidencialidade e Sigilo.

7.15 Sistemas de telecomunicação/telefonia

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da Cinpal, assim como, o uso de ramais virtuais instalados nos computadores, é responsabilidade da área de TI, de acordo com as definições da gerência de cada área.

7.16 Monitoramento e análise de registro de segurança

Um profissional da área de TI qualificado deve ser responsável por monitorar e analisar os registros dos sistemas de segurança de forma a agir preventivamente na melhoria da segurança e prontamente em caso de ameaça real. Esta atividade pode ser feita por um prestador de serviço qualificado.

7.17 Redes sociais

O acesso a redes sociais é bloqueado por padrão nos computadores, sendo liberado apenas para usuários previamente indicados por seus gerentes para uso como ferramenta de trabalho.

7.18 Sistemas corporativos, Websites e Apps

Todos os sítios de internet (*websites*) ou Apps (programa desenvolvido para dispositivos computacionais móveis como *smartphone* e *tablet*) da Cinpal, independente de sua finalidade (institucional, relacionamento com partes interessadas ou transação comercial) deve garantir a aderência a essa política e as práticas de desenvolvimento seguro devem ser seguidas. *Websites* ou Apps adquiridos ou locados (modalidade de contratação de serviço) de terceiros devem ter sua segurança atestada. Não limitando-se, mas atenção específica deve ser dada no cumprimento dos requisitos da LGPD quanto a *websites* e apps acessados por pessoas externas.

7.19 Sistemas de teleconferência e colaboração

Somente os sistemas de teleconferência e colaboração homologados pela área de TI podem ser utilizados internamente e para relacionamentos com contatos externos.

7.20 Equipamentos de filmagem, fotografia e gravação de áudio

É proibido o uso de equipamentos de filmagem e fotografia dentro das instalações da Cinpal. Somente o responsável pela área pode autorizar a realização de filmagem ou fotografia.

8. Cumprimento de política

Todos os colaboradores, estagiários, temporários ou terceiros devem comportar-se de forma aderente a esta política e como parte dos acordos e condições de contratação, devem atestar o conhecimento e a aderência através da assinatura do Termo de Confidencialidade e Sigilo e do Termo de Uso de Recursos de Tecnologia da Informação (ou código de conduta e ética).

Qualquer violação nas diretrizes e normas presentes nesta política por parte do colaborador irá implicar em sanções administrativas e/ou previstas em lei, sendo analisado cada caso individualmente pela área de RH e Jurídico.

Qualquer violação nas diretrizes e normas presentes nesta política por parte dos estagiários, temporários e terceiros autorizados, ensejará, conforme o caso, no imediato desligamento, sem prejuízo da rescisão de contrato de prestação de serviços celebrado com a empresa responsável e a Cinpal, e da aplicação de penalidades contratualmente previstas.

Deve-se promover constantemente ações de conscientização e treinamentos quanto a segurança da informação, incluindo os aspectos específicos ao tratamento de dados pessoais e dados pessoais sensíveis. Estas ações devem ser aprovadas pelo CSI.

9. Histórico de revisão

Rev.	Data	Descrição
00	24/11/22	Aprovação inicial

10. Distribuição de cópias e protocolo de treinamento

A distribuição deste procedimento se dá conforme tabela abaixo:

Distribuição de cópias e protocolo de treinamentro					
Setor	**Cópias**	**Assinatura**	**Setor**	**Cópias**	**Assinatura**
SGQ	01		DTI	01	
DIN	01		CQU	01	
DFN	01		CQF	01	
DJR	01		CQD	01	
DCM	01		PRU	01	
DRH	01		PRF	01	
PDU	01		PRD	01	
PDF	01		ENF	01	
PDD	01		MAN	01	
PD3	01		SSMA	01	
EXP	01				