Sumário

1. OBJETIVO

O **Grupo CPFL**, através de seu departamento de Segurança da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece nesta política, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações de propriedade do **Grupo CPFL** ou por eles custodiadas e estabelecer as regras para a classificação dos dados e das informações quanto à sua relevância e o nível adequado de proteção dos ativos de informação do **Grupo CPFL** de acordo com seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

Este documento reforça o comprometimento do **Grupo CPFL** com a segurança dos negócios e com boas práticas de mercado.

A Diretoria Executiva do **Grupo CPFL** estabeleceu e apoia as Diretrizes de Segurança da Informação a fim de proteger os ativos de informação e garantir a continuidade dos negócios diante de situações adversas que possam vir a comprometer a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas e dos ativos de informação de propriedade do **Grupo CPFL** e/ou sob sua guarda.

As diretrizes descritas neste documento apresentam uma visão abrangente de Segurança da Informação (nesta incluída a Segurança Cibernética) aplicada aos negócios da empresa e conceitos de alto nível que devem ser observados por todos, que de alguma maneira utilizem recursos tecnológicos, informações e/ou acessem fisicamente as dependências das empresas do **Grupo CPFL**.

Quando necessário, as disposições desta Política serão detalhadas em normas, procedimentos ou padrões específicos.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Esta Política é aplicável ao **Grupo CPFL** e a todas as suas controladas diretas e/ou indiretas, incluindo as que atuam na geração, transmissão, distribuição e comercialização de energia elétrica.

2.2. Área

Todas as áreas do **Grupo CPFL**.

3. DEFINIÇÕES

3.1. Conceitos Básicos

Todos os recursos tecnológicos, de sistemas de informação e de processo de negócio possuem um valor e devem ser protegidos de acordo com a sua importância e criticidade para o negócio. O Sistema de Gestão de Segurança da Informação visa proteger os ativos do **Grupo CPFL**, estejam eles em ambiente físico ou digital, garantir a continuidade dos negócios minimizando

possíveis prejuízos e mitigando os riscos aos quais os ativos estão expostos, sempre considerando os seguintes requisitos:

- **CONFIDENCIALIDADE:** É a garantia de que a informação é acessada somente por usuários devidamente autorizados. Ela pode ser mantida por meio de criptografia de dados armazenados e transmitidos, controles de acessos, classificação dos dados, procedimentos com treinamentos adequados.

- **INTEGRIDADE:** É a garantia de que a informação no momento que é acessada está em sua completeza, totalidade, plenitude, sem qualquer alteração em seu conteúdo, quando foi armazenada. O cumprimento deste atributo de segurança assegura que os invasores ou erros cometidos por usuários não comprometerão a exatidão e a integridade das informações, bem como a autenticidade (certeza quanto a autoria ou origem da informação), não-repúdio (impossibilidade de negação quanto a responsabilidade pelos atos praticados) e auditabilidade (facilidade de se chegar à origem e consistência das informações).Ela pode ser mantida por meio de técnicas de criptografia, gravação de logs de usuários, processos de revisão e aprovação por alçadas diferentes em alterações realizadas em sistemas e informações.

- **DISPONIBILIDADE:** É a garantia de que a informação está disponível para o usuário (que tem tal autorização de acesso) e para o sistema de informação no momento que o **Grupo CPFL** exige, inclusive na hipótese de um desastre. Ela pode ser mantida por meio de procedimentos de backup e respectiva gestão de storage.

- **SEGURANÇA DA INFORMAÇÃO:** Proteção da informação, esteja ela em ambiente físico ou digital contra ameaças para garantir a continuidade das atividades finalísticas e meio do **Grupo CPFL**, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no **Grupo CPFL**.

- **INCIDENTE DE SEGURANÇA DA INFORMAÇÃO:** Ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade, evento adversado, indesejados ou inesperados, confirmados ou sob suspeita que possa comprometer a confidencialidade, integridade ou a disponibilidade das informações, estejam elas em ambiente físico ou lógico do **Grupo CPFL**.

- **INCIDENTE DE MAIOR IMPACTO:** É estabelecido com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do **Grupo CPFL**.

- **INCIDENTE DE DADOS PESSOAIS**: Incidente de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado, a dados pessoais de indivíduos transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento pelo **Grupo CPFL.**

- **INFORMAÇÃO CONFIDENCIAL**: São aquelas com potencial de impacto negativo na prestação de serviços à população, e prejuízo aos negócios do **Grupo CPFL** e de terceiros em caso de comprometimento.

- **SEGURANÇA CIBERNÉTICA**: subclasse da Segurança da Informação, uma vez que seu objetivo é a proteção da segurança da informação em ambiente digital, ou seja, a proteção dos ativos contra ameaças cibernéticas e ataques maliciosos.

- **GRUPO CPFL**: A CPFL Energia S.A., e todas as suas controladas diretas e/ou indiretas, exceto as empresas com seus próprios padrões de governança e gestão que compartilham controle com outras empresas.

- **REDE DE INFORMAÇÃO**: Rede corporativa de dados da empresa, composta por toda infraestrutura de telecomunicações própria e de terceiros destinada aos ativos de Tecnologia da Informação.

3.2. Conceitos Gerais

- **Boas Práticas de Segurança da Informação**
  São consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas;

- **Configurações de Segurança (Baselines)**
  Requisitos, recomendações e melhores práticas de configurações de segurança da informação para os recursos/ativos. Trata-se das configurações mínimas aceitáveis pelo **Grupo CPFL** para ativos/recursos dentro de cada contexto;

- **Controle**
  Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros;

- **Gestor**
  Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção;

- **Informação**
  Qualquer conjunto organizado de dados que possua algum propósito e valor para o **Grupo CPFL**, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, ou estar sob sua custódia de forma direta (arquivamento e processamento interno) ou de terceiros (fornecedores, parceiros e prestadores de serviços que apoiam as atividades do **Grupo CPFL**), como por exemplo, informações armazenadas em nuvem (cloud)

- **Princípios de privilégio mínimo (Least Privilege) e necessidade de saber (Need to Know)**

Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know). Isto é, o acesso deve ser concedido considerando o mínimo necessário para a realização do trabalho, considerando a necessidade da função exercida;

- **Recursos**
  Qualquer recurso, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade do **Grupo CPFL**, que possua valor para a empresa. Podem ser considerados recursos: ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos;

- **Recursos Críticos**
  Recursos essenciais para o funcionamento da operação do **Grupo CPFL** e que possuem informações críticas ou sensíveis, também conhecidos como ativos (assets) críticos. Recursos podem ser tipificados como: pessoas, tecnologia, dados/informações. No caso de tecnologia, temos os elementos de infraestrutura, sistemas de informação e ferramentas;

- **Risco (s)**
  Toda incerteza em relação a eventos ou situações aos quais a instituição está exposta e que podem impactar os resultados do negócio.

- **Ameaça**
  Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais;

- **Vulnerabilidade**
  Fraqueza de um ativo ou controle que pode ser explorado, por uma ou mais ameaças. Ela caracteriza a ausência ou ponto fraco de uma medida preventiva que pode ser explorada.

- **Controles de Segurança**
  Medidas preventivas ou contramedida que servem para mitigar riscos potenciais

3.3. Conceitos Específicos

- **Categorias de Responsabilidades**
  Para operacionalizar o controle dos direitos e deveres relativos à segurança, o **Grupo CPFL** adota o sistema de categorias e responsabilidades.

- **Responsável pelo Ativo**
  Toda a aplicação, sistema ou informação crítica, obrigatoriamente deve ter um Responsável designado. Os Responsáveis devem definir a classificação da informação e o perfil de acesso por usuário (incluindo privilégios) de forma a assegurar o cumprimento dos requisitos de segurança da informação (confidencialidade, integridade e disponibilidade), bem como garantir a retenção de evidências da

execução de seus controles para fornecimento em casos de auditorias ou necessidade do atendimento a regulamentações;

- **Depositário do Ativo**
  Os Depositários têm a posse física ou lógica da informação. Os Depositários são responsáveis pela guarda da informação, incluindo a implementação de sistemas de controle de acesso e a manutenção de cópias de segurança. Também são responsabilidades dos Depositários a implementação, a operação e a manutenção das medidas de segurança de acordo com a classificação da informação realizadas pelos Responsáveis;

- **Usuário**
  Os Usuários são pessoas com a responsabilidade por se familiarizar e obedecer a todos os itens aplicáveis a Segurança da Informação. Dúvidas sobre a manipulação apropriada de um tipo específico de informação devem ser dirigidas ao Depositário do Ativo, ao Responsável pelo Ativo ou à Gestão de Segurança da Informação;

4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- ABNT/ISO 27032-2013;
- ABNT/ISO 31000-2009;
- GED 18744 - Classificação da Informação do Grupo CPFL
- GED 13307 - Política de Gerenciamento de Riscos do Grupo CPFL
- GED 14634 - Utilização do Correio Eletrônico do Grupo CPFL
- GED 18744 - Classificação da Informação do Grupo CPFL
- GED 19127 – Norma de Descarte Seguro do Grupo CPFL
- GED 18928 - Norma Geral de Proteção de Dados do Grupo CPFL
- GED 14141 - Norma para Gestão de Acessos do Grupo CPFL
- GED 18851 - Plano de Resposta a Incidentes de Segurança da Informação do Grupo CPFL;
- GED 19232 - Código de Conduta Ética do Grupo CPFL;
- Esta Política é complementada em demais Normas e Procedimentos do Grupo CPFL.
- Norma Geral de Proteção de Dados do **Grupo CPFL**
- Código de Ética e de Conduta Empresarial do **Grupo CPFL**;
- Esta Norma é complementada pela Política, e demais Normas e Procedimentos do **Grupo CPFL**.

5. RESPONSABILIDADES

Todo Colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações do **Grupo CPFL** e deve cumprir as determinações desta política, bem como das, normas e procedimentos a ela correlatos. A seguir as obrigações e responsabilidades dos envolvidos:

- **Colaborador:**

  - ✓ Utilizar de modo seguro, responsável, moral e ético, todas informações, dados, sistemas e ferramentas de tecnologia disponibilizados pelo **Grupo CPFL**;

  - ✓ Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pelo **Grupo CPFL;**

  - ✓ Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo **Grupo CPFL;**

  - ✓ Descartar adequadamente os documentos e informações impressos/lógicos de acordo com seu grau de classificação e observando as diretrizes de Segurança da Informação;

  - ✓ Notificar a área de Segurança da Informação sobre as violações da Política de Segurança da Informação e/ou demais normas e procedimentos, bem como sobre incidentes de segurança e dados pessoais que venham a tomar conhecimento;

  - ✓ Manter o sigilo das informações que tenha obtido acesso enquanto Colaborador do **Grupo CPFL**, mesmo após seu desligamento da empresa;

  - ✓ Participar ativamente do Programa de Conscientização e Divulgação de Segurança da Informação.

- **Gestor**

  - ✓ Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento das políticas, normas e procedimentos relacionados à segurança da informação;

  - ✓ Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

  - ✓ Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;

  - ✓ Elaborar, com o apoio da Gerência de Segurança da Informação os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;

  - ✓ Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

  - ✓ Garantir que seus subordinados tenham acesso e conhecimento desta Política e padrões de segurança da informação;

- ✓ Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;

- ✓ Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;

- ✓ Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem as diretrizes de segurança da informação estabelecidas no Código de Conduta do **Grupo CPFL**, neste documento e de mais normas e procedimentos correlatos;

- ✓ Autorizar acessos a sistemas e ambientes de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de "menor privilégio" e "necessidade de saber "e que deve estar essencialmente atrelado as funções e tarefas por ele executada;

- ✓ Incentivar suas equipes e colaboradores a participarem das ações relacionadas ao Programa de Conscientização e Divulgação de Segurança da Informação.

- **Gerência de Segurança da Informação**

  - ✓ Buscar alinhamento com as diretrizes da organização;

  - ✓ Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.;

  - ✓ Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;

  - ✓ Executar todas as atividades inerentes ao ciclo de tratamento de vulnerabilidades;

  - ✓ Buscar a utilização segura das redes e serviços das estações de energia elétrica;

  - ✓ Engajar as áreas responsáveis pelas correções no tratamento tempestivo das vulnerabilidades;

  - ✓ Identificar novas ameaças, monitorar as existentes, e fazer o acompanhamento das correções;

  - ✓ Atualizar este documento sempre que aplicável;

  - ✓ Realizar e acompanhar os testes de vulnerabilidades;

  - ✓ Criar simulações de cenários e ameaças para testes de resiliência, de análise das ferramentas e da capacidade e tempo de resposta;

- ✓ Criar procedimentos e controles para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de segurança cibernética;
- ✓ Definir as regras para instalação de software e hardware no **Grupo CPFL;**
- ✓ Homologar os equipamentos pessoais (smartphones e notebooks) para uso na rede do **Grupo CPFL**;
- ✓ Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
- ✓ Desenvolver, disseminar e estabelecer programas de conscientização e divulgação da Política de Segurança da Informação e cultura de segurança cibernética;
- ✓ Implementar, monitorar e reportar a realização de programas de capacitação e de avaliação periódica de pessoal e ações do programa anual de conscientização;
- ✓ Disseminar a cultura de segurança cibernética;
- ✓ Criar medidas para a conscientizar e educar os colaboradores do **Grupo CPFL** sobre aspectos de segurança cibernética;
- ✓ Conduzir o processo de Gestão de Riscos de Segurança da Informação;
- ✓ Conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
- ✓ Identificar, proteger, diagnosticar, responder e recuperar os incidentes cibernéticos, além de prevenir, detectar, responder e reduzir a vulnerabilidade a incidentes cibernéticos;
- ✓ Identificar, avaliar, classificar e tratar os riscos cibernéticos na estrutura estabelecida pelo **Grupo CPFL**;
- ✓ Buscar a cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos, respeitadas as regras de confidencialidade das informações definidas na GED 18744 - Classificação da Informação;
- ✓ Conduzir os processos de monitoração e segurança da informação e dos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política, normas e procedimentos de Segurança da Informação;
- ✓ Definir mecanismos para prevenir, mitigar e recuperar incidentes cibernéticos na Rede de Informação ou na rede das instalações, e para impedir que os incidentes

afetem a operação

- ✓ Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
- ✓ Definir e disponibilizar os treinamentos e programa de conscientização em Segurança da Informação;
- ✓ Auxiliar as demais áreas, incluindo o jurídico na análise de requisitos de segurança de informação nos contratos celebrados com o **Grupo CPFL**, quando aplicável;
- ✓ Propor projetos e iniciativas para melhoria do nível de segurança das informações do **Grupo CPFL**; e
- ✓ Atuar com responsabilidade, zelo e transparência;

- **CISO**
  - ✓ Aprovar os documentos/normas/procedimentos/diretrizes de Segurança da Informação;
  - ✓ Designar um responsável por aprovar os documentos, normas, procedimentos e diretrizes de Segurança da Informação na sua ausência;

- **Diretoria de Tecnologia da Informação**
  - ✓ Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;
  - ✓ Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
  - ✓ Conduzir a gestão dos acessos a sistemas e informações do **Grupo CPFL**;
  - ✓ Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
  - ✓ Informar imediatamente a área de Segurança de Informação, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos do **Grupo CPFL**;
  - ✓ Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
  - ✓ Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio; e

- ✓ Garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como Datacenters. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

- **Comitê de Segurança da Informação**

  - ✓ Propor melhorias, alterações e ajustes na Política de Segurança da Informação;
  - ✓ Propor investimentos relacionados à segurança da informação com o intuito de minimizar riscos (inclusive legais e regulatórios);
  - ✓ Classificar e reclassificar o nível de acesso às informações sempre que necessário;
  - ✓ Avaliar incidentes de segurança e propor ações corretivas;

- **Diretoria Jurídica**

  - ✓ Apoiar, a fim de assessorar a Gerência de Segurança da Informação, sobre as questões jurídicas envolvendo a a aplicação de medidas disciplinares ao responsável interno por violações das Diretrizes de Segurança da Informação e demais normas e procedimentos correlatos;
  - ✓ Orientar a respeito de obrigações legais, regulamentares ou contratuais pertinentes à segurança da informação e de quaisquer requisitos jurídicos de segurança a fim de atender aos requisitos do negócio;
  - ✓ Adotar com apoio da Gerência de Segurança da Informação clausulas pertinentes à segurança das informações nos negócios jurídicos estabelecidos com o **Grupo CPFL** a fim de assegurar que as diretrizes, normas e procedimentos de segurança da informação sejam assumidas por fornecedores, parceiros e terceiros contratados.

- **Fornecedores e Parceiros de Negócios**

  - ✓ Cumprir as determinações da Política, normas e procedimentos de segurança da informação e de proteção de dados do **Grupo CPFL** (quando aplicável);
  - ✓ Cumprir com o acordo de confidencialidade firmado com o **Grupo CPFL**;
  - ✓ Orientar os seus colaboradores, prepostos, terceiros e de seus eventuais subcontratados sobre o cumprimento das determinações da Política, Norma e Procedimentos de segurança da informação e de proteção de dados do **Grupo CPFL**; e
  - ✓ Adotar, na execução do objeto contratual/parceria, medidas de segurança compatíveis com a criticidade da informação utilizada, observando a classificação da informação e demais regras de processamento e sigilo determinadas pelo **Grupo CPFL.**

- **Prestadores de Serviços/Terceiros**

  ✓ Caso manuseiem dados ou Informação Confidencial ou que sejam relevantes para a condução das atividades operacionais em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pelo **Grupo CPFL** deve atender essa Política, ou o Plano de Resposta a Incidentes de Segurança da Informação do **Grupo CPFL,** ou ter procedimentos e controles voltados à prevenção e ao tratamento dos incidentes.

- **Gerência de Proteção de Dados**

  ✓ Orientar a respeito das regras de proteção de dados aplicáveis as informações identificam ou tornam identificável os indivíduos que o **Grupo CPFL** realiza o tratamento de dados.
  ✓ Realizar a avaliação de impacto em proteção de dados com relação aos tratamentos de dados pessoais nas atividades de negócio do **Grupo CPFL**
  ✓ Realizar a avaliação de risco ou dano relevante para os titulares nas hipóteses de incidente de dados, e orientar sobre a notificação a Autoridade Nacional de Proteção de Dados e aos titulares das informações relacionadas ao evento.

- **Alta Administração**

  ✓ Comprometer-se com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética;
  ✓ Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação e da proteção de dados;
  ✓ Fornece as Gerências de Segurança da Informação e Proteção de Dados direcionamento, apoio, recomendações e apontar restrições quando necessário.

6. REGRAS BÁSICAS

A informação é um ativo essencial para os negócios de uma organização e, sendo assim, deve ser adequadamente protegida. Isto é especialmente importante em um ambiente de negócios cada vez mais interconectado.

A proteção dos ativos do **Grupo CPFL** leva em consideração a criticidade da informação e sistemas nos processos de negócio, ou seja, a importância, a indispensabilidade e a capacidade de recuperação das informações e sistemas nos processos operacionais por meio da metodologia BIA (Business Impact Assessment).

Segurança da informação é a proteção das informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade. Isso significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, proteger os funcionários em caso de incidente que o envolva diretamente, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e das marcas da empresa.

O Grupo CPFL, através da Gerência de Segurança da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece nesta política, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da Empresa, de seus colaboradores, clientes, fornecedores e parceiros de negócios.

Em linhas gerais seguir o disposto nesta política significa prevenir fraude, proteger a empresa contra o vazamento de informações, zelar pela privacidade, assegurar a disponibilidade dos sistemas e informações quando necessário e zelar pela proteção da imagem e da marca do **Grupo CPFL**.

6.1 Aspectos Gerais de Gestão de Políticas

É de responsabilidade da área Segurança de Informação a revisão/atualização da Política de Segurança da Informação periodicamente a cada 12 meses, sempre que necessário ou em caso de mudança significativa no contexto de segurança da informação do **Grupo CPFL**, em função de novas leis, sistemas ou incidentes.

Após a atualização periódica desta política, é de responsabilidade do Conselho de Administração do **Grupo CPFL** a aprovação formal.

A política deve contar com medidas de proteção contra quaisquer alterações indesejadas e não-autorizadas, tais como controle de acesso.

6.2 Conformidade

O cumprimento e aderência às leis, regulamentações, Política de Segurança da Informação, normas, obrigações contratuais e padrões de segurança, são obrigatórios e devem ser garantidos por todos os Colaboradores do **Grupo CPFL**.

Responsáveis por recursos críticos do **Grupo CPFL** devem garantir a retenção de evidências da execução de seus controles para fornecimento em casos de auditorias ou necessidade do atendimento a regulamentações.

6.3 Comitê de Segurança da Informação

O **Grupo CPFL** define o Comitê de Segurança da Informação como a maior autoridade para avaliação de políticas, padrões e procedimentos com relação à Segurança da Informação. Uma vez que a segurança total é impossível de ser alcançada na prática, o comitê deve seguir a Norma GED 13307, que define os níveis de riscos aceitáveis para o **Grupo CPFL**.

O Comitê de Segurança da informação é multidisciplinar, sendo composto, preferencialmente, por representantes dos departamentos de Tecnologia da Informação, Jurídico, Recursos Humanos e Auditoria Interna. A definição das pessoas que compõem o comitê cabe ao **Grupo CPFL**.

Medidas disciplinares em relação ao descumprimento das regras dispostas nessa política são de competência do Comitê de Ética do **Grupo CPFL**.

6.4. Classificação da Informação

Toda informação deve ter um proprietário (Gestor da Informação) e uma classificação adequada de acordo com a necessidade do negócio e os requisitos legais para compartilhar ou restringir as informações.
Os ativos físicos, além dos ativos de informação, também devem ser classificados de acordo com o rótulo atribuído à informação armazenada, processada, manuseada ou protegida pelo mesmo e ser compatível com a sensibilidade dos dados e das informações. O **Grupo CPFL** adota as seguintes categorias para classificação da informação, elas estão descritas nos subtópicos a seguir:

6.4.1. Informação Pública

O acesso público a esta informação não causa qualquer dano ao **Grupo CPFL**, seus colaboradores ou parceiros de negócio. Qualquer informação somente poderá ser divulgada ao público se possuir esta categoria de classificação, definida pelo Responsável, conforme 3.3. Conceitos Específicos.

6.4.2. Informação de Uso Interno

Esta informação é compreendida como de acesso e uso do **Grupo CPFL** e, em alguns casos, de seus parceiros de negócio, sendo proibido o seu acesso público (Internet, por exemplo). **O acesso de outros a estas informações pode prejudicar a empresa, seus colaboradores e seus parceiros de negócio**. Informações classificadas como de Uso Interno podem estar em e-mails (para classificação do e-mail, consultar a GED 14634 - Utilização do Correio Eletrônico, relatórios, planilhas de controle, lista de telefones, entre outros.

6.4.3. Informação Confidencial

Informação confidencial é aquela que, devido a sua criticidade aos negócios, deve ter acesso e distribuição restritos e controlados. Portanto, essas informações somente devem ser acessadas por aqueles com reais necessidades de seu conhecimento para desempenhar suas atividades junto à organização. Esta categoria está associada a grupos de informação, tais como informações bancárias, informações sobre clientes ou contratos específicos, informações sobre Recursos Humanos ou outras, cuja divulgação não autorizada possa causar sérios prejuízos à organização. **Informações que não possuírem classificação devem ser tratadas como Informação de Uso Interno**.

Todo colaborador é responsável por garantir a segurança da informação confidencial que esteja sob sua guarda ou alcance, de forma a evitar que essa informação possa ser lida ou copiada por pessoa não autorizada.

6.5. Tratamento da Informação

As informações devem ter (i) regras claramente definidas pelo seu proprietário para proteção contra perda, alteração e/ou acesso indevidos, independente do meio em que são armazenadas; e (ii) usuário explicitamente definido, com os respectivos tipos de direitos de acesso determinados.

6.5.1. Reclassificação da Informação

Sempre que o Responsável identificar que é necessário, deve-se proceder a reclassificação da informação. Quando efetuar uma reclassificação, o Responsável deve comunicar adequadamente todas as partes interessadas.

6.5.2. Destruição da Informação

As informações, quando perdem sua utilidade ou valor, devem ser destruídas ou em se tratando de dados pessoais de indivíduos ou de um grupo de indivíduos anonimizadas (servirá apenas para fins estatísticos).

O Responsável pelo ativo tem poder para decidir sobre a destruição ou anonimização da informação, salvo se houver lei, regulamentação ou norma interna que oriente sobre a destinação da informação. Para maiores informações consultar GED 18744 - Classificação da Informação e/ou 19127 – Norma de Descarte Seguro.
Ao serem descartados, documentos impressos com o rótulo de Confidencial, devem ser destruídos completamente através de equipamentos como fragmentadoras, para que a reprodução não seja efetuada após o descarte.

6.5.3. Armazenamento da Informação

O armazenamento da informação deve ser feito com os controles de segurança adequados ao nível de confidencialidade da informação.

6.5.4. Transmissão da Informação

É desejável que as informações sejam transmitidas através de meios adequados que assegurem o nível de confidencialidade do ativo.

Para maiores informações, consultar a Norma Classificação da Informação (GED 18744).

6.5.5. Compartilhamento

Toda informação compartilhada com terceiros deve ser classificada de acordo com os rótulos estabelecidos. O compartilhamento de informações não é restrito às empresas do mesmo grupo societário. O **Grupo CPFL** adota procedimento de compartilhamento de informações sobre ameaças/vulnerabilidades e outras informações relativas à segurança cibernética de forma sigilosa e não discriminatória. O compartilhamento de informações não compreende aquelas classificadas pelo **Grupo CPFL** como confidencial ou que possam comprometer a sua própria segurança. Ao compartilhar uma informação com terceiros via e-mail, rotular o título do e-mail e o título do documento anexado. No caso de o e-mail conter um anexo com informação Confidencial, deve-se proteger o arquivo com senha. E se tratando de compartilhamento de dados pessoais/sensíveis/menores de 12 anos a área deve seguir os requisitos de privacidade que constam da Norma Geral de Proteção de Dados (GED 18928).

O compartilhamento de informação pessoal de indivíduos deve ocorrer somente se necessário para atingir a finalidade estabelecida em instrumento jurídico/tratamento dos dados, sendo assegurado o registro do compartilhamento de maneira que seja possível o cumprimento dos direitos dos titulares garantidos na Lei Geral de Proteção de Dados.

No caso de compartilhamento de dados pessoais de qualquer categoria, sempre que possível, mascarar as informações retirando qualquer informação que faça referência, ou que possa ser associada ao titular. Quanto menor o poder de identificação do indivíduo ou grupo de indivíduos, menor o risco em caso de acesso indevido/vazamento de dados.

O compartilhamento de qualquer informação classificada como Confidencial somente pode ser transmitido de forma criptografada. Em se tratando de dados pessoais, dados pessoais

sensíveis e/ou de menores de 12 anos é obrigatório que haja o registro da atividade no inventário de dados pessoais identificando no mínimo: local/data/hora/ferramenta de compartilhamento/destinatário autorizado/relação de informações compartilhadas.

Importante: Caso seja necessário realizar o compartilhamento que envolva dados pessoais sensíveis e/ou de menores de 12 anos de idade (i) se internamente, seguirá as regras de gestão de acesso definidas pelo responsável pela base de dados que será impactada com o compartilhamento; e (ii) se externamente deverá o responsável pela extração da informação (a) certificar-se de que o compartilhamento dos dados para terceiro está registrado no "data mapping" da área (consultar Embaixador de Privacidade), sem o qual o dado não poderá ser compartilhado; (b) que existe contrato vigente contemplando regras de proteção de dados; (c) manter registrada a relação de informações compartilhadas de maneira que seja possível confirmar, para atendimento de direitos de titulares, o que foi compartilhado, sobre quem e qual o destinatário (observar prazo prescricional para manutenção da informação); (d) seguir as normas e procedimentos de proteção de dados, bem como as normas de segurança da informação extensivas a proteção de dados.

6.6. Segurança em Recursos Humanos

É extremamente importante assegurar que colaboradores, fornecedores e terceiros tenham conhecimento prévio e devidamente documentado sobre suas responsabilidades com a proteção dos ativos do **Grupo CPFL** e conformidade com as leis e regulamentações relevantes, os conceitos descritos neste tópico devem ser observados desde a pré-contratação até o desligamento ou rescisão de contrato.

6.6.1. Atribuição de Responsabilidade

Os colaboradores, fornecedores e terceiros devem ser claramente informados de sua responsabilidade do ponto de vista de Segurança da Informação, e devem estar de acordo com as Diretrizes de Segurança da Informação do **Grupo CPFL**, os acordos, registros de treinamento e conscientização devem ser registrados em documento apropriado e/ou armazenados em software específico.

6.6.2. Condições Específicas

As seguintes condições descritas nos subtópicos abaixo devem ser observadas pelos gestores de Recursos Humanos.

6.6.3. Termos e Condições de Contratação

É responsabilidade do Departamento de Recursos Humanos obter a assinatura do Termo de Compromisso (anexo) para colaboradores e/ou para dirigentes das empresas do **Grupo CPFL**, a assinatura deve ocorrer no momento da contratação dos colaboradores. O Termo garante que as pessoas estão de acordo com as suas responsabilidades em relação à proteção e o uso adequado dos ativos do **Grupo CPFL**.

6.6.4. Treinamento de Integração

Novos colaboradores e terceiros devem receber um treinamento em Segurança da Informação, com foco nas Diretrizes de Segurança da Informação. Este treinamento pode ser dado juntamente com o treinamento de integração para novos colaboradores efetivos e para terceiros quando no início de suas atividades no **Grupo CPFL** ou no mês subsequente.

6.6.5. Treinamentos Periódicos

É extremamente importante assegurar que colaboradores, e **Terceiros** tenham conhecimento prévio e devidamente documentado sobre suas responsabilidades com a proteção, uso de informações e ativos de informação do **Grupo CPFL**. Para isso, campanhas e materiais de conscientização bem como treinamentos devem ser disponibilizados e adequadamente divulgados.
Registros de treinamento e conscientização devem ser criados em documento apropriado e/ou armazenados em software específico;
Treinamentos de Segurança da Informação devem ser realizados pelo menos anualmente, através de reciclagem disponibilizada na Universidade **Grupo CPFL**;
Os treinamentos de Segurança da Informação devem ser complementados por campanhas de divulgação através de materiais de conscientização a serem disseminados, intercalando com as agendas de treinamento, conforme necessidade. Esses materiais podem ser divulgados através de diversos formatos: e-mail, banners, intranet, documentos em papéis, sites, dentre outros.
O conteúdo dos treinamentos e conscientizações de Segurança da Informação deve abordar os temas da Diretrizes de Segurança da Informação e documentação normativa do **Grupo CPFL**, incluindo, mas não se limitando a:

- Privacidade e classificação da informação;
- Controle de acesso lógico;
- Controle de acesso físico;
- Continuidade de Negócios;
- Incidentes de Segurança da Informação;
- Acesso Remoto e dispositivos móveis;
- Correio Eletrônico, internet e aplicativos corporativos de mensagem instantânea;
- Aquisição, desenvolvimento e manutenção de sistemas.

Exercícios e Simulados periódicos

Periodicamente, a área de Gerência de Segurança de TI executa testes e exercícios simulados para a medição do grau de conscientização dos colaboradores. Esta atividade tem o objetivo de orientar e treinar, bem como aumentar o nível de proteção da companhia com o ganho de maturidade em segurança, adquirida pelos colaboradores.
Os exercícios podem ocorrer por diversos canais de comunicação, como e-mail, mensagens instantâneas etc.

- **Teste de Phishing**

Este exercício é realizado através do envio de e-mails que simulam mensagens mal-intencionadas que visam o roubo de informações ou de credencias de acesso. O objetivo é testar a atenção e percepção do colaborador para identificar o golpe.
Ao final de cada teste, quando o colaborador não for bem-sucedido, haverá um direcionamento automático para um curso obrigatório para reforço dos conceitos aplicados. O gestor imediato

será comunicado, para acompanhamento da evolução de seu liderado. Quando o curso não for realizado, o diretor da área será envolvido para auxílio nesta orientação.

Os Gestores de Recursos Humanos e o Departamento de Gestão de Segurança da Informação são responsáveis por desenvolver e promover programas de treinamento e conscientização sobre segurança da informação, disseminação da cultura de segurança cibernética na instituição e implementação de programas de capacitação e de avaliação periódica de pessoal.

6.6.6. Comportamento Seguro

Independente dos meios onde a informação esteja armazenada ou seja transmitida, cada Colaborador deve assumir um comportamento seguro e proativo impedindo seu acesso por terceiros não autorizados, tanto com relação aos colaboradores, terceiros, fornecedores e parceiros comerciais do **Grupo CPFL**.

É vetado aos colaboradores emitir opiniões em nome do **Grupo CPFL,** quando sua função assim não o permite ou utilizar informações confidenciais ou de uso interno da Organização em: e-mails, sites, redes sociais, publicações impressas, fóruns de discussão, serviços da Internet e outros ambientes públicos, em face da possibilidade de divulgação inadvertida, vide Código de Conduta.

Não deve realizações conexões em áreas públicas como shoppings e aeroportos, evite acessar, visualizar ou editar qualquer informação ou página que precise do input de dados confidenciais, como senhas, informações bancárias ou dados referentes ao **Grupo CPFL**.

6.6.7. Processo Disciplinar

O descumprimento das normas descritas nas Diretrizes de Segurança da Informação do **Grupo CPFL** pode acarretar, sem prejuízo de indenização dos danos causados:

- ✓ Advertência verbal;
- ✓ Advertência escrita;
- ✓ Suspensão temporária dos direitos de acesso;
- ✓ Rescisão contratual sem pagamento de multas pelo **Grupo CPFL**;
- ✓ Demissão.

Os Departamentos de Recursos Humanos e Tecnologia da Informação devem manter procedimentos formalizados para assegurar o tratamento dos incidentes de segurança e dar uma resposta gradual que considere os seguintes fatores:

- ✓ Natureza da violação;
- ✓ Gravidade da violação;
- ✓ Impacto no negócio;
- ✓ Quantidade de violações do infrator.

6.6.8. Comunicação de Alteração de Cargos

Para gestão de acesso adequada é de responsabilidade do Departamento de Recursos Humanos notificar a Diretoria de Tecnologia da Informação quando ocorrerem mudanças de cargo ou atividade.

6.6.9. Bloqueio dos Direitos de Acesso

Caso ocorra afastamento temporário de colaboradores ou terceiros, por motivo de férias, licenças para tratamento de saúde ou maternidade, o Departamento de Recursos Humanos tem a responsabilidade de notificar a Diretoria de Tecnologia da Informação para que sejam tomadas as devidas providências. A Diretoria de Tecnologia da Informação deve analisar cada caso de acordo com as permissões concedidas ao colaborador. Para casos de Terceiros, o gestor do contrato e/ou da área que o terceiro pertence, deve notificar a Diretoria de Tecnologia de Informação.

6.6.10. Revogação dos Direitos de Acesso

É responsabilidade do Departamento de Recursos Humanos notificar desligamentos a Diretoria de Tecnologia da Informação para que sejam tomadas as devidas providências. Para casos de Terceiros, o gestor do contrato e/ou da área que o terceiro pertence, deve notificar Departamento

6.7. Controle de Acessos

Para garantir um nível de proteção adequado aos sistemas e informações do **Grupo CPFL**, assim como para atendimento a regulamentações, foi definido que todos os acessos dos usuários devem ser devidamente registrados, aprovados pelos responsáveis e revisados periodicamente. Quando viável tecnicamente, o provisionamento de direitos de acesso deve ser automatizado e métodos de detecção de erros devem ser estabelecidos.

6.7.1. Condições Gerais

As condições gerais descritas nos subtópicos a seguir devem ser observadas, principalmente, pela Diretoria de Tecnologia da Informação e áreas que, de alguma maneira, executam tarefas relacionadas aos acessos no ambiente de tecnologia da informação.

6.7.2. Registro do Usuário

Todo usuário que acessa o ambiente de Tecnologia do **Grupo CPFL** deve ser identificado lógica e unicamente através de sua conta (“user-ID” e senha) de uso exclusivo.

6.7.3. Cadastro e exclusão

É responsabilidade da Diretoria de Tecnologia da Informação implantar e controlar procedimentos de aprovação, criação, bloqueio e exclusão dos usuários nos sistemas. Quando tecnicamente viável, as informações dos colaboradores, contidas na base de dados da área de Recursos Humanos, devem ser utilizadas como fonte para o cadastro do colaborador nos demais sistemas.

6.7.4. Controle de Privilégios

É responsabilidade da Diretoria de Tecnologia da Informação controlar os direitos de acesso como “super usuário”, administrador ou quaisquer outras denominações que signifiquem poderes adicionais para instalar, alterar ou apagar informações. Os controles devem observar, pelo menos:

- ✓ Utilização de um usuário diferente do normal, quando este estiver executando tarefas de “super usuário”;
- ✓ Clara identificação de quais usuários tem acesso às “contas privilegiadas”;
- ✓ Quando tecnicamente viável, manter o registro de uso das contas.

Apenas usuários autorizados e aprovados pelo Gerencia de Segurança da Informação e gestor do responsável podem possuírem privilégios de ADM para o ambiente.
As exceções serão analisadas e deverá ser aprovado pelo gestor do responsável informando o risco que há em ter este tipo de acesso, preenchendo o "Termo de Responsabilidade para o privilégio de ADM Local", e o acesso utilizando ferramenta de Cofre de Senhas.

6.7.5. Privilégios em Equipamentos Específicos

É responsabilidade da Diretoria de Tecnologia da Informação configurar os direitos dos usuários de domínio de forma que estes possuam direitos mínimos de acesso na estação de trabalho, mas suficientes à execução de suas tarefas.

Necessidades específicas devem ser justificadas no "Termo de Responsabilidade para o privilégio de ADM Local e devem ser aprovados pelo superior do solicitante (cargo mínimo de Gerente) e pelo Gerente da Segurança da Informação, deve ser anexado ao chamado de liberação de acesso aberto no Portal de Serviços Compartilhados.

6.7.6. Configuração das Senhas de Acesso

É responsabilidade da Diretoria de Tecnologia da Informação, sempre que tecnicamente viável, parametrizar os sistemas com, no mínimo, as seguintes regras:

- ✓ Utilização no mínimo de oito caracteres;
- ✓ Utilização de caracteres alfanuméricos;
- ✓ Não permitir padrões repetidos, como por exemplo: sequência alfabética "ABCDE" ou numéricas "12345";
- ✓ Exigir a troca periodicamente;
- ✓ Não permitir o uso das últimas vinte e quatro senhas;
- ✓ Exigir a troca da senha padrão no primeiro acesso do usuário;
- ✓ Bloqueio do acesso após cinco tentativas malsucedidas.

A Diretoria de Tecnologia da Informação, para casos específicos e visando proteger os ativos do **Grupo CPFL** pode definir um período diferente dos padrões definidos acima.

6.8. Armazenamento de Senhas

As senhas cadastradas para acesso aos ambientes e sistemas do **Grupo CPFL** são pessoais e intransferíveis, sendo sua guarda e uso exclusivas para o usuário autorizado. Desta forma, não podem ser guardadas de forma legível em arquivos, bases de dados, macros de software, chaves de função, terminais ou em outros locais, nos quais, pessoas sem autorização possam ter acesso.

6.8.1. Senhas Padrão

É responsabilidade da Diretoria de Tecnologia da Informação alterar a senha de equipamentos ou sistemas que utilizem uma senha padrão, no momento de sua instalação ou recebimento, antes de sua entrada em atividade. O padrão da nova senha deve seguir as definições de procedimentos específicos e/ou das Diretrizes de Segurança da Informação.

6.9. Utilização de Usuário Privilegiado

Contas de usuários padrão, com acessos privilegiados, como por exemplo, "root", "administrador" e outras não podem ser utilizadas em tarefas que não sejam específicas de administração dos ambientes de tecnologia.

6.9.1. Revisão de Acessos

Os responsáveis por perfis de acesso devem revisar os direitos concedidos aos usuários, de acordo com a periodicidade de cada ambiente. Um esforço conjunto do Responsável e Recursos Humanos é recomendado para revogar os direitos redundantes ou desnecessários.

Usuários com privilégios especiais de acesso a sistemas críticos devem ter seus direitos revisados periodicamente conforme definido a periodicidade de cada ambiente. Como privilégios especiais se entendem funções de administradores ou operadores com direito de escrita ou alteração nos sistemas e/ou em Banco de Dados.

6.9.2. Perfis de Uso e Direitos

Devem ser criados perfis de acessos para os usuários com a finalidade de se reduzirem riscos relacionados ao gerenciamento de acessos. Como perfis de acessos entende-se que vários usuários estão sob as mesmas regras e podem ser gerenciados em conjunto.

Todos os perfis de acessos devem ter um Responsável nomeado. As funções do Responsável pelo perfil são:

- ✓ Determinar, em conjunto com a Diretoria de Tecnologia da Informação os direitos dos usuários;
- ✓ Aprovar o cadastro de novos usuários;
- ✓ Revisar e se responsabilizar pelas ações dos usuários, utilizando as permissões dadas pelas funções;
- ✓ Revisar periodicamente a validade dos direitos concedidos.

6.9.3. Proteção contra Acessos Indevidos

É recomendado a Diretoria de Tecnologia da Informação que seja definido um procedimento para o bloqueio dos usuários que não acessam os sistemas críticos (definidas na GED 14141) por um período determinado.

6.9.4. Revogação de Acessos

A Diretoria de Tecnologia da Informação deve revogar todos os direitos de acesso sempre que ocorrerem as seguintes situações:

- ✓ Aviso de desligamento de colaborador enviado pelo Departamento de Recursos Humanos;
- ✓ Solicitação de revogação enviada pelo Responsável do perfil ou grupo;
- ✓ Solicitação de revogação enviada pelo Gestor de Contratos ou Gestor imediato de terceiros.

Quando viável tecnicamente, poderá ser implantado um processo automatizado para detecção de desligamento e revogação automatizada de direitos dos colaboradores e/ou terceiros.

6.9.5. Segregação de Funções

Com o objetivo de prevenir oportunidades de uso não autorizado, dano ou perda de informações e riscos relacionados, deve haver mecanismos de segregação de funções em sistemas e operações que suportam informações financeiras da empresa para evitar fraudes

e perdas. As áreas envolvidas no processo devem analisar e remediar as situações de conflitos. Na impossibilidade de remediação, as áreas de negócio responsáveis pelo processo em conjunto com o *Responsável pelo ativo*, devem informar ação mitigatória (controle compensatório) para o risco, informando a Gerência de Controles Internos, para avaliação. Caberá à área de Gerência de Tecnologia da Informação, o cadastramento desta ação na respectiva matriz de segregação de função, orientar as áreas envolvidas sobre os conceitos, bem como realizar a gestão da matriz de segregação de função, visando assegurar a adequada disponibilidade das informações aos órgãos avaliadores.

6.10. Plano de Continuidade dos Negócios

O **Grupo CPFL** entende que garantir a continuidade dos negócios diante de situações adversas é extremamente importante, as diretrizes estabelecidas neste documento devem ser seguidas para guiar os responsáveis na elaboração dos planos de Continuidade e Contingência. É necessária a formalização e testes periódicos destes planos.

6.10.1. Condições Gerais

6.10.1.1. Identificação de Impacto

Um processo de gestão de continuidade dos negócios deve ser implementado para minimizar o impacto sobre a organização resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais, a um nível aceitável.

Para isto, é necessário que as consequências de uma indisponibilidade, perda de confidencialidade ou de integridade das informações sejam submetidas a uma análise de impacto no negócio.

O resultado desta análise deve identificar claramente os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as consequências para a segurança de informações.

6.10.2. Condições Específicas

6.10.2.1. Plano de continuidade de negócio

É responsabilidade do Gerente de Segurança da Informação desenvolver, implementar e manter um plano de contingência relativo à segurança de informações para a manutenção ou recuperação das operações e para garantir a disponibilidade das informações no tempo necessário após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

6.10.2.2. Estrutura do plano

O plano de continuidade deve especificar os planos de escalonamento e as condições para a sua ativação. O plano também deverá identificar as responsabilidades para a execução de cada atividade. Os procedimentos e os programas de gestão de mudança deverão fornecer as informações necessárias para que o plano esteja sempre atualizado.

6.10.2.3. Testes dos Planos

Os planos e procedimentos devem ser testados anualmente e os resultados registrados para análise futura. Estes testes visam garantir que o plano funciona e que todos os envolvidos têm a completa habilidade e ferramental para acioná-lo com sucesso. É responsabilidade do

Gerente de Segurança da Informação analisar criticamente os resultados dos testes e promover as mudanças necessárias. Além da elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

6.10.2.4. Revisão

O plano de continuidade deve ser revisado anualmente após o teste ou em caso de alteração no ambiente. Todos os testes realizados neste período devem ser documentados e mantidos para verificação futura.

6.11. Incidentes de Segurança da Informação

Promover um ambiente onde todos se comprometem com segurança da informação na empresa é extremamente importante e exige um processo contínuo de conscientização. É responsabilidade de todos informarem possíveis violações das Diretrizes de Segurança da Informação através dos canais disponibilizados pela Gerência de Segurança da Informação. A Gestão de Incidentes de Segurança da Informação tem apoio da Diretoria Executiva do **Grupo CPFL**. O objetivo desse documento é estabelecer a sistemática do Processo de Gestão de Incidentes de Segurança da Informação no **Grupo CPFL**.

6.11.1. Condições gerais

6.11.1.1. Incidentes de Segurança da Informação

São eventos que podem colocar em risco a confidencialidade, disponibilidade, integridade e/ou a autenticidade das informações da Organização (podendo envolver dados de negócio, dados de pessoa jurídica ou dados pessoais de pessoa física), que possam colocar em risco os ativos do **Grupo CPFL**
ou mesmo qualquer descumprimento das políticas, procedimentos e/ou orientações do Departamento de Segurança da Informação.
Abaixo alguns exemplos de incidente de segurança da informação;
(i) perda ou roubo de equipamentos da Empresa (celular ou notebook corporativo);
(ii) vazamento de dados pessoais de indivíduos reportado por um titular de dados no canal disponibilizado para atendimento de titulares;

Incidentes de segurança da informação/dados pessoais devem ser formalmente relatados ao Departamento de Segurança da Informação através dos canais de comunicação por ele disponibilizados.

Os incidentes devem ser investigados e registrados, gerando um relatório conclusivo. Em sendo concluída pela exposição de dados pessoais de indivíduos o Encarregado de Proteção de Dados do **Grupo CPFL** será acionado para realizar a análise de risco relevante nos termos da Lei Geral de Proteção de Dados (Lei Federal 13.853/2019)

Para casos de incidentes que envolvam a Alesta, será necessária a comunicação junto ao BACEN para compartilhamento de informações. Para tal ação, o departamento de segurança de informação deverá ser acionado para averiguar as informações que serão compartilhadas pelo departamento de compliance da Alesta. O compartilhamento também deve abranger informações sobre incidentes recebidas de empresas prestadoras de serviços a terceiros.

As informações sobre os incidentes devem ser consolidadas, apresentadas e discutidas, periodicamente, nas reuniões do Comitê de Segurança da Informação.

O **Grupo CPFL** manterá Plano de Resposta a Incidentes atualizado contendo papéis, responsabilidade, fases do processo e demais temas relevantes para que o processo seja registrado e auditável.

As ocorrências de segurança da informação devem ser registradas com seus artefatos e armazenados em repositório protegido.

Todos os incidentes de segurança devem ser comunicados às partes envolvidas tempestivamente, quando aplicável.
O registro de uma ocorrência de segurança da informação deve estar acessível, quando necessário e previamente autorizado pela Segurança da Informação, para funcionários, terceiros e entidades externas interessadas, e todos devem ser instruídos sobre a responsabilidade em notificar e registrar quaisquer fragilidades e falhas de segurança da informação.

Os incidentes de maior impacto devem ter o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, para as atividades do **Grupo CPF**L, abrangendo inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

6.11.1.2 Preparação

A etapa de Preparação visa capacitar a organização na adequada resposta a um incidente de segurança da informação, garantindo que sistemas, redes e aplicativos estejam suficientemente seguros, ativos de resposta a incidentes relacionados e equipes envolvidas devidamente treinadas.
Nesta fase, serão produzidos os seguintes documentos, não ficando restrito a esta lista:

- Lista de contatos da organização, atualizada periodicamente
- Inventário de procedimentos e tools para resposta a incidentes
- Procedimento para estabelecimento de war rooms
- Definição de categorização e criticidade de incidentes
- Treinamentos
- Simulações de cenários e ameaças para testes de resiliência, de análise das ferramentas e da capacidade e tempo de resposta;

6.11.2. Fases do Processo

6.11.2.1. Abertura de Incidente

Fase em que o incidente de segurança da informação é identificado e comunicado ao Departamento de Segurança da Informação através dos canais disponibilizados pelo **Grupo CPFL** (vide item 16.11.4 abaixo)

6.11.2.2. Impacto nos Negócios

O impacto nos negócios deve ser classificado de acordo com os seguintes parâmetros:

Impacto	Descrição
Alto	- Impacto Financeiro de valor acima de R$ 1.000.000,01; - Parada de mais de um processo de negócio; - Perda generalizada de credibilidade junto aos dados pessoais que são tratados pelo **Grupo CPFL.** - Quantidade significativa de dados pessoais e sensíveis comprometida; - Incidentes de privacidade que resultam em cobertura da mídia em territórios, on-line ou através de grandes notícias ou meios de comunicação com alta probabilidade de visibilidade pública; e/ou - Incidentes de privacidade que podem resultar em violação da LGPD e que represente risco ou dano relevante para os direitos e garantias fundamentais dos titulares de dados pessoais.
Médio	- Impacto Financeiro entre R$ 500.000,01 e R$ 1.000.000,00; - Parada de um processo de negócio; e/ou - Perda de disponibilidade junto aos dados pessoais que são tratados pelo **Grupo CPFL**.
Baixo	- Impacto Financeiro abaixo ou igual de R$ 500.000,00; - Atraso operacional em um ou mais processos de negócio; e/ou - Perda de disponibilidade temporária ou junto a uma pequena quantidade de dados pessoais tratados pelo **Grupo CPFL**.

Tendo sido classificado o incidente, os acionamentos necessários são realizados e as equipes que tratarão o incidente são convocadas.

6.11.2.3. Investigação

Após o devido registro, o incidente deve ser encaminhado para a fila de Segurança da Informação para análise e providências.

Os incidentes devem ser classificados de acordo com o nível do impacto ocorrido em Alto, Médio ou Baixo de acordo com a classificação de impacto descrita no Procedimento de Análise de Riscos do SGSI (Sistema de Gestão de Segurança da Informação). Na hipótese de exposição de dados pessoais de pessoa natural, o Encarregado de Dados da Organização é informado sobre tal ocorrência para realizar a avaliação de relevância do risco e os impactos a privacidade dos titulares nos termos da LGPD.

6.11.2.4. Ações Corretivas e Preventivas

Fase em que é identificada a causa raiz do incidente de forma a gerar plano de ação para implementação de controles e eliminação da causa raiz.

6.11.2.5. Encerramento

Fase em que o incidente de segurança da informação é fechado e comunicado às partes envolvidas.

6.11.2.6. Contatos Externos

É fundamental que sejam mantidos contatos apropriados com autoridades pertinentes e grupos de segurança externos, de forma a manter o **Grupo CPFL** a par das tendências e ameaças do ambiente. Esse contato pode ser através de fóruns, palestras seminários etc.

6.11.2.7. Punição e Processo disciplinar

Dependendo do impacto do incidente, é recomendável que exista um processo disciplinar definido relatando as devidas punições. A punição de infratores só pode ser efetuada se evidências forem corretamente coletadas e armazenadas de forma segura. A coleta de evidências nos casos em que houver a necessidade de punição interna deve contar com um representante do Departamento de Recursos Humanos e/ou Departamento Jurídico (quando aplicável) e/ou Departamento de Compliance (quando aplicável), e em se tratando de evidência digital de um representante de Segurança da Informação a fim de que sejam tomadas as medidas necessárias a fim de que seja preservada a integridade da evidência.

Dependendo da gravidade do incidente, o Gestor de Segurança pode optar também pela presença de um auditor externo independente.

Dependendo da gravidade do incidente, o Gestor de Segurança pode optar também pela presença de um auditor externo independente.

6.11.2.8. Canal de Notificação de Incidentes

O seguinte canal deve ser utilizado para notificação de incidentes de segurança da informação:

Canal	Detalhes
Notificação Interna via e-mail	seginfo@cpfl.com.br.

O **Grupo CPFL** deverá notificar a equipe de Coordenação Setorial designada para cuidar dos incidentes cibernéticos de maior impacto, os quais afetam de maneira significativa e substancial a segurança das instalações, a operação, os serviços aos usuários ou dados dos ambientes e estações, os resultados dos modelos de maturidade aplicados. Essa notificação de incidente cibernético de maior impacto incluirá a análise da causa e impacto, os riscos cibernéticos identificados, com a respectiva forma de tratamento bem como incluir as ações mitigatórias que deverão ser anotadas, referente a cada caso, conforme Resolução Normativa Aneel nº 964.

Assim que, o **Grupo CPFL** tiver ciência do incidente e de sua dimensão, deverá ser enviada a notificação de incidente cibernético. O envio dessa notificação não exclui a obrigatoriedade do **Grupo CPFL** ao atendimento e cumprimento das obrigações previstas em leis, normas e regulamentos.

Para maiores informações sobre prevenção, tratamento e resposta a incidentes cibernéticos e os dados das equipes de prevenção, tratamento e resposta a incidentes cibernéticos poderá ser verificado na GED 18851 - Plano de Resposta a Incidentes de Segurança da Informação.

6.12. Gestão de Vulnerabilidades

Para garantir níveis de proteção adequados aos sistemas e informações do **Grupo CPFL**, assim como para atendimento a regulamentações e normas, foram definidos um conjunto de regras para o gerenciamento de vulnerabilidades nos ativos da empresa.

6.12.1. Condições gerais

As análises de vulnerabilidades devem ser realizadas por ferramentas contratadas de propriedade da área de Tecnologia da Informação da **Grupo CPFL**, conforme cronograma definido.

Regularmente serão analisados os servidores com escopo de aplicação, infraestrutura e servidores.

6.12.2. Metodologia de Gestão de Vulnerabilidades

O **Grupo CPFL** adotou a seguinte metodologia para o gerenciamento de vulnerabilidades em seu ambiente:

6.12.2.1. Identificação

Etapa onde é definido quais ativos serão analisados.

6.12.2.2. Coleta

Por meio de varreduras automatizadas, são coletados dados do ambiente, para análise e identificação das vulnerabilidades existentes.

6.12.2.3. Validação

Etapa onde é realizada a validação dos dados coletados, para identificação de possíveis divergências.

6.12.2.4. Classificação / Priorização

Etapa onde é realizada a avaliação de quais vulnerabilidades x ambientes, na qual estas vulnerabilidades existentes precisam ser priorizadas de acordo com o risco que oferecem.

6.12.2.5. Correção

Etapa onde quais correção serão priorizadas, também onde ocorre a implantação de controles compensatórios e análise de causa raiz.

6.12.2.6. Evidências

Etapa onde são coletadas evidências, as que são identificadas e associadas aos itens de avaliação do ambiente.

6.12.2.7. Resultados

Por fim ocorre a elaboração de relatório e apresentação dos dados observados, bem como de orientação sobre a correção das vulnerabilidades identificadas e orientação de fortalecimento do ambiente.

O **Grupo CPFL** realiza anualmente aplicação de teste de modelo de maturidade em segurança cibernética.

6.13. Segurança Física e do Ambiente

O acesso ao escritório, sala de servidores ou outro local da empresa que contenha informações do **Grupo CPFL** seja de dados pessoais de pessoa natural, dados de pessoa jurídica, dados de negócio ou qualquer outro dado classificado como confidencial ou de uso interno devem ser mantidas em local seguro, e ter acesso restrito fisicamente. Os documentos

ou outras mídias que contenham informações sensíveis devem ser mantidos em local seguro (caixa forte, arquivo fechado) quando não estiverem em uso. As mesas devem estar limpas e organizadas ao final do expediente.

6.13.1. Perímetro de Segurança

Para evitar acesso não autorizado, maior restrição de acesso, rastreabilidade dos acessos e dano ou interferência aos sistemas de informação considerados críticos, um perímetro de segurança deve ser claramente definido. Barreiras físicas e sistemas de controle de acesso devem ser implementados para garantir o acesso físico apenas por usuários autorizados pelo responsável. O perímetro de segurança deve comtemplar as seguintes características:

- Paredes, portas e teto com solidez adequada;
- Um sistema de portaria ou recepção para controle do acesso;
- Monitoração e gravação em vídeo, circuito fechado de TV ou equivalente;
- Biometria
- Acesso controlado por crachás de identificação;
- Autorização de acesso apenas a pessoas autorizadas;
- A área deve permanecer trancada mesmo quando houver pessoas trabalhando.

Os controles e recursos de proteção relacionados ao perímetro de segurança, fazem parte das áreas seguras do **Grupo CPFL**, nas seguintes localidades:

- Data Center CPFL Sede;
- Data Center CPFL DR;
- Data Center São Leopoldo.

Os controles e recursos de proteção relacionados ao perímetro de segurança seguem as diretrizes da GED 18744 - Norma de Classificação da Informação.

A área de Infraestrutura de TI é a responsável por propor e implementar mecanismos e processos para restringir o acesso e monitorar o cumprimento das regras estabelecidas neste documento nas áreas consideradas como restritas e seguras.

6.13.1.1. Identificação

Por questões de segurança, todo o acesso ao ambiente do **Grupo CPFL** deve ser precedido de uma identificação na portaria ou recepção. O acesso ao ambiente interno do **Grupo CPFL**, só é permitido quando devidamente autorizado pelo colaborador contatado na portaria ou recepção.

Adicionalmente, a data e a hora da entrada e saída dos visitantes devem ser registradas, assim como dados pessoais mínimos e que proporcione a identificação do indivíduo.

6.13.1.2. Verificação de Identidade

Em área de circulação restrita os colaboradores/terceiros autorizados devem andar com seu crachá à mostra, a fim de que possam ser facilmente identificadas a sua permissão para acesso à área restrita. Os colaboradores devem ser encorajados a questionar outros

colaboradores, terceiros e/ou visitantes que circularem na área restrita e/ou crítica na hipótese de não ter certeza quanto a permissão.

6.13.1.3. Atividade dentro do Perímetro

Todas as atividades dentro do perímetro de segurança devem ser previamente autorizadas e monitoradas. Adicionalmente são necessários os seguintes controles:

- ✓ A área segura deve ser mantida fechada e trancada e se possível possuir um controle de acesso auditável;
- ✓ Terceiros ou contratados devem ser supervisionados constantemente, de preferência devem ser acompanhados por um responsável na empresa.
- ✓ Deve ter instalado um sistema de monitoração, alarme ou gravação em vídeo ou equivalente das atividades dentro do perímetro de segurança.
- ✓ As imagens e registros de acesso devem ser armazenados observada a tabela de temporalidade do **Grupo CPFL**.

6.13.2. Segurança de Escritórios, Salas e Instalações

O acesso a sala de escritórios ou outro local do **Grupo CPFL** que contenha informação sensível deve ser restrito fisicamente. Para estes ambientes devem ser utilizados controles adicionais de autenticação.

6.13.2.1. Áreas Restritas

Os locais determinados como áreas críticas são implementados controles adicionais de acesso e monitoramento, tais como:

- ✓ CFTV,
- ✓ Biometria,
- ✓ Acesso controlado por crachás de identificação,
- ✓ Autorização de acesso;

Esses locais determinados pelo **Grupo CPFL** são:

- ✓ Data Center CPFL Sede;
- ✓ Data Center CPFL DR;
- ✓ Data Center São Leopoldo.

6.13.2.2. Visitação Pública

A visitação pública às instalações do **Grupo CPFL** deve ser obrigatoriamente acompanhada e previamente autorizada pelo responsável.

6.13.2.3. Compartilhamento de informações do Grupo CPFL

Todas as informações e dados obtidas pelo Colaborador no exercício de suas atividades no **Grupo CPFL** são consideradas informações internas ou confidencial (deve-se observar a classificação da informação dada pelo Responsável pelo Ativo) do **Grupo CPFL** e somente podem ser utilizadas em benefício dos objetivos de negócio da companhia exclusivamente no exercício de sua atividade e somente durante o período em que o seu contrato de trabalho estiver ativo.

É vedado o acesso as informações do **Grupo CPFL** quando o Colaborador estiver em férias, afastado, aposentado ou em qualquer hipótese de suspensão do contrato de trabalho.

É proibido fotografar, filmar, copiar, desenhar, vender, compartilhar com terceiros não autorizados, compartilhar para e-mails particulares, utilizar para finalidades diversas ao exercício de suas atividades, praticar qualquer ação ou omissão que possa facilitar o uso ou deixá-las expostas.

6.13.3. Área de Entrega e Carregamento

O recebimento de cargas ou equipamentos deve ser efetuado em local próprio, controlado e isolado. Para isto, o acesso a uma área de entrega e carregamento deve ser restrito ao pessoal identificado e autorizado de maneira que não permita o acesso às demais instalações da empresa.

Os materiais entregues devem ser previamente inspecionados para detectar ameaças potenciais antes de serem encaminhados para as demais dependências da empresa.

6.13.4. Equipamentos e Instalações

Os servidores ou outros equipamentos considerados críticos devem ser protegidos contra as principais ameaças físicas como roubo, fogo, poeira, água, temperatura, efeitos químicos, radiação eletromagnética e vandalismo.

6.13.5. Controle de Alimentação e Temperatura

Os servidores e equipamentos devem ser protegidos contra interrupções de e de ventilação / calefação. Esta proteção normalmente é feita com a utilização de sistemas de “no- break” ou geradores auxiliares.

Da mesma forma o acesso aos quadros de manutenção de devem ser restritos e controlados e devem ser mantidos trancados.

As salas devem ser mantidas na temperatura recomendada pelos fabricantes dos equipamentos. A temperatura das salas deve ser monitorada constantemente e alertas devem ser disparados em caso de aumento brusco de temperatura.

6.13.6. Cabeamento

Os cabos de transmissão elétrica, dados e comunicações devem respeitar as normas técnicas vigentes bem como devem ser protegidos contra rompimentos acidentais ou não. Os cabos de elétrica devem ser segregados dos cabos de comunicação e devem ser claramente identificados.

6.13.7. Manutenção dos Equipamentos

Equipamentos ou sistemas que possuam informações classificadas como confidencial ou de uso restrito devem ser comunicadas pelo Responsável ao gestor da área de Segurança da Informação a fim de que possam alinhar as questões de segurança a serem observadas na manutenção seja ele preventiva ou corretiva.

Quando a manutenção for realizada por fornecedor, na hipótese de ele ter acesso a dados classificados como confidencial ou de uso interno este deverá ter um termo/clausula de

confidencialidade assinada com o **Grupo CPFL**. Na hipótese de poderem ter acesso a dados pessoais de pessoa natural identificada ou identificável o acesso somente será permitido se ele tiver assinado as cláusulas de proteção de dados da organização.

Adicionalmente, devem ser atendidas todas as exigências estabelecidas nas apólices de seguros.

As informações contidas nos equipamentos críticos devem ser apagadas de forma apropriada antes de serem retirados do **Grupo CPFL** ou ter o acesso liberado para terceiros.

6.13.8. Transporte de ativos

Equipamentos, mídias, informações ou qualquer outro ativo de propriedade do **Grupo CPFL** não pode ser retirados ou compartilhados sem autorização formal e conjunta do Responsável pelo Ativos e do Gestor de Segurança e/ou Gerente do Departamento, considerando a adoção das medidas de proteção para garantia das informações armazenas e em trânsito a seguir:

- ✓ A natureza da informação, bem como seu nível de sensibilidade e confidencialidade para o negócio;
- ✓ Declaração da finalidade de uso contendo os impactos do seu não compartilhamento, e em se tratando de compartilhamento externo a indicação do fornecedor (nome e nº do contrato no SAP) e destinatário da informação;
- ✓ O valor ou impacto relacionado a qualquer perda durante a transferência;
- ✓ Criptografia dos dados em trânsito;
- ✓ Anonimização/Pseudoanonimização dos dados (quando aplicável);
- ✓ Processo de dupla custódia para mídias em trânsito;
- ✓ Se o compartilhamento dos dados está registrado no Inventário de Dados (se informação pessoal de indivíduo);
- ✓ Se o contrato com o fornecedor tem regras de proteção de dados e clausula de confidencialidade e o resultado da avaliação de riscos de fornecedor relacionado a LGPD.

É recomendável que exista um processo para registro de retirada e devolução do equipamento/mídia/informação no momento do seu retorno identificando claramente quem autorizou a sua retirada das dependências da empresa.

- **Transporte de Propriedade da Empresa**

Equipamentos, mídias, informações ou qualquer outro ativo de propriedade do **Grupo CPFL** não pode ser retirado da mesma sem autorização formal do Responsável pelo Ativo e do Gestor de Segurança ou gerente do departamento.
É recomendável que exista um processo para registro de retirada e devolução do equipamento/mídia/ informação no momento do seu retorno identificando claramente quem autorizou a sua retirada das dependências da empresa.

6.14. Segurança nas Comunicações

É importante garantir que os recursos de processamento da informação sejam operados de forma correta e segura. As diretrizes e conceitos descritos neste documento devem ser observados, principalmente, pelo Departamento de Tecnologia da Informação e pelos usuários em geral.

6.14.1. Condições gerais

6.14.1.1. Documentação dos Procedimentos

É responsabilidade da Diretoria de Tecnologia da Informação documentar os procedimentos requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle dos processos de segurança da informação sob sua responsabilidade.

6.14.1.2. Inventário dos Recursos

A Diretoria de Tecnologia da Informação é responsável por manter um inventário de softwares e hardwares de propriedade do **Grupo CPFL** ou equipamento/ferramenta de terceiro por ele utilizada, identificando os proprietários.

6.14.2. Condições específicas

6.14.2.1. Padronização e Homologação de Recursos Tecnológicos

A(s) aplicação(ões) de mensageria homologada(s) pelo **Grupo CPFL**, embora disponível(s) 24hs por dia e 7 (sete) dias por semana, seu uso deve ser limitado às atividades e operações de trabalho executadas no **Grupo CPFL** e somente no horário de expediente do colaborador.

É vedada a utilização de ferramentas de comunicação não homologadas pelo **Grupo CPFL** em qualquer situação que exista o tratamento de dados pessoais ou dados pessoais sensíveis de qualquer origem (clientes, colaboradores, prestadores de serviços etc.).

Como forma de prevenir incidentes com dados pessoais por meio da utilização de ferramentas não homologadas (ex. WhatsApp, Telegram, ...) orientamos que:

- Compartilhe com seus contatos o comunicador oficial do **Grupo CPFL**, bem como os canais homologados pela Gerência de Segurança da Informação para compartilhamento de documentos confidenciais (dentre estes àqueles que contém dados pessoais/dados pessoais sensíveis).

- Caso receba algum documento de terceiros, tendo como destinatária ao **Grupo CPFL**, contendo dados pessoais, oriente o reenvio por ferramentas homologadas do **Grupo CPFL**, exclua imediatamente dos seus arquivos e permaneça no fluxo seguro para as demais tratativas.

- Se você possui celular corporativo, havendo a necessidade de compartilhamento de dados pessoais por WhatsApp Business (o que se admitirá tão somente se a comunicação não puder ser realizada por ferramentas homologadas pela Gerência de Segurança da Informação), é obrigatório, tão logo ele seja recebido pelo colaborador, salvá-lo em ambiente monitorado pela Gerência de Segurança da Informação e apagá-lo imediatamente dos arquivos do celular.

- Vedado tirar foto e gravar áudios relacionados a informações do **Grupo CPFL** e compartilhar através de grupos de aplicativos de mensagens instantâneas.
- Sempre que possível, havendo informação confidencial (nesta incluído dado pessoal/dado pessoal sensível), utilizar duplo fator de autenticação em aplicativos de mensageria e arquivar eventuais informações confidenciais em pasta criptografada.

6.14.2.2. Gestão de Mudanças

É responsabilidade da Diretoria de Tecnologia da Informação controlar as alterações no ambiente computacional. Como alteração se entende mudança em hardware, mudança em sistema operacional, substituição ou atualização de sistemas aplicativos.

No mínimo devem ser estabelecidos os seguintes controles:

- ✓ Identificação das alterações propostas;
- ✓ Registro das versões atuais e das novas versões implantadas;
- ✓ Avaliação e aprovação formal pelo Responsável;
- ✓ Comunicação antecipada aos usuários afetados;
- ✓ Identificação das responsabilidades e atualização do Inventário de Ativos.

6.14.2.3. Segregação de Tarefas

É responsabilidade da Diretoria de Tecnologia da Informação implementar a segregação de tarefas. As tarefas operacionais e de controle do sistema devem ser executadas por diferentes usuários sempre que possível.

6.14.2.4. Planejamento de Capacidade

É responsabilidade da Diretoria de Tecnologia da Informação monitorar a capacidade de processamento dos equipamentos e sistemas críticos. O objetivo desta monitoração é evitar que o sistema seja sobrecarregado e cause prejuízos e/ou mesmo perda de lucratividade.

6.14.2.5. Contas de Serviço

Nos casos em que sistemas necessitem de contas de serviço para qualquer finalidade, é responsabilidade da Diretoria de Tecnologia da Informação implantar os seguintes controles:

- ✓ As contas de serviço devem ser inventariadas, devendo constar no inventário, no mínimo:
- ✓ Nome da conta;
- ✓ Objetivo;
- ✓ Responsável;
- ✓ O acesso às contas deve ser controlado e restrito aos profissionais da Diretoria de Tecnologia da Informação que dela fazem uso;
- ✓ No caso de sistemas críticos, deve ser avaliada a guarda compartilhada da senha;
- ✓ Deve ser estabelecido um procedimento de substituição periódica ou sob demanda desta senha, como por exemplo, nos casos de desligamento do responsável pela conta de serviço;
- ✓ A criação das contas de serviço deve ser autorizada pelo Gestor de Tecnologia da Informação.

6.14.2.6. Controle de Mídias Removíveis

É responsabilidade da Diretoria de Tecnologia da Informação proteger adequadamente as mídias removíveis (CDs, DVDs, Flash Memories, etc.) que contenham informações confidenciais ou de uso interno e que estão em seu poder. Quando não mais necessárias ao uso empresarial, as mídias devem ser destruídas fisicamente de forma segura.

6.14.2.7. Armazenamento de Informações

Deve ser utilizada uma estrutura de armazenamento nos Servidores de Arquivo. Esta estrutura deve conter, no mínimo, uma estrutura de armazenamento departamental e segregação de privilégios para acessos a informações nele contidas.

6.14.2.8. Cópias de Segurança

É responsabilidade da Diretoria de Tecnologia da Informação implementar um processo para realização de cópias de segurança dos dados armazenados e processados, principalmente, nos servidores corporativos. Informações armazenadas, localmente, em estações de trabalho não fazem parte do escopo de cópias de segurança.

O processo deve contemplar as ações necessárias para a que as informações sejam recuperadas, em casos de emergências, no menor tempo possível.

6.14.2.9. Periodicidade

É responsabilidade da Diretoria de Tecnologia da Informação definir a frequência de execução do backup, critérios de extensão, tempo de retenção e testes de recuperação das cópias de segurança realizadas.

6.14.2.10. Necessidades adicionais

Caso a necessidade do responsável pela ferramenta não seja atendida pelo procedimento de backup oficial, este deverá solicitar a Diretoria de Tecnologia da Informação a adequação do backup para sua necessidade. Estas necessidades devem ser baseadas na classificação das informações (grau de sigilo), requisitos legais e de negócio do **Grupo CPFL**.

6.14.2.11. Segurança das Mídias em Trânsito

É responsabilidade da Diretoria de Tecnologia da Informação definir e implementar controles de proteção para as mídias em trânsito contra acesso não autorizado ou alteração indevida. Deve ser claramente definido quem são as pessoas autorizadas a enviar, transportar e receber as mídias. O transporte deve ocorrer em um período de tempo apropriado ao objetivo de tempo de recuperação para o ativo crítico.

Os seguintes cuidados adicionais devem ser considerados:

- ✓ As cópias de segurança devem ser armazenadas em locais protegidos, conforme padrões de segurança física e ambiental que assegurem a integridade, disponibilidade e confidencialidade dos dados contidos nestas mídias.

- ✓ Deve existir um controle centralizado e atualizado que contemple o inventário de todas as cópias de segurança realizadas no **Grupo CPFL**.

- ✓ Toda cópia de segurança de sistemas críticos deve ser realizada, no mínimo, em duas vias completas e recentes, armazenadas em locais distintos com os devidos controles de acesso e retiradas.

- ✓ Deve existir um processo de revisão periódica do procedimento de backup e processos de recuperação de cópias de segurança.

- ✓ Toda a recuperação e/ou restauração de uma cópia de segurança deve ser realizada em um ambiente diferente do original, sempre que tecnicamente possível, evitando danos aos dados atuais.

- ✓ Toda cópia de segurança deve ser testada periodicamente, assegurando a integridade e a possível restauração dos dados.

6.14.3. Segurança na documentação dos Recursos de TI

A documentação dos recursos de Tecnologia da Informação deve ser armazenada em local seguro e o acesso deve ser restrito apenas às pessoas que necessitem das informações.

6.14.4. Registros de Auditoria

É recomendável que o Diretoria de Tecnologia da Informação armazene os registros de auditoria, de todos os sistemas definidos como críticos, por um determinado período.

6.14.5. Sincronização de Relógio

É responsabilidade Diretoria de Tecnologia da Informação manter a sincronização de data e hora nos sistemas, de acordo com NTP.

6.14.6. Instalação Padrão

É responsabilidade da Diretoria de Tecnologia da Informação padronizar a instalação inicial dos sistemas. Um conjunto padrão de instalação de software deve ser preparado e mantido em local seguro. Estas cópias padrão deve ser usadas para a recuperação de infecções de vírus, falhas do disco rígido e outros problemas do equipamento.

É responsabilidade da Diretoria de Tecnologia da Informação implementar em todas as estações de trabalho um sistema de proteção contra programas maliciosos.

6.14.6.1. Gerenciamento e Controle

Toda estação de trabalho deve possuir software de gerenciamento e controle, para monitoramento de atividades e assistência ao usuário de forma remota.

O acesso à estação de trabalho do usuário, por meio do software de gerenciamento, deve ser previamente informado sobre o monitoramento.

6.14.6.2. Instalação padrão para Estação de Trabalho

Os dispositivos de armazenamento removíveis como portas USB (pen drive), gravador de CD, gravador de DVD, BlueTooth, não se limitando a estes, devem ser desabilitados antes da liberação da estação de trabalho para o usuário. Este item não se aplica a teclados, mouses, monitores e placas de rede,

Toda estação de trabalho, quando tecnicamente viável, deve possuir lacre de segurança, controlado e inventariado pela Diretoria de Tecnologia da Informação.

6.14.6.3. Instalação Padrão – Notebook

É recomendável que todo notebook seja protegido por um sistema de Firewall local. As configurações do Firewall devem obedecer aos critérios de segurança estabelecidos pela Diretoria de Tecnologia de Informação.

Todo notebook, quando tecnicamente viável, deve possuir sistema de criptografia e autenticação. As configurações do sistema de criptografia e autenticação devem obedecer aos critérios de segurança estabelecidos pela Diretoria de Tecnologia de Informação.

6.14.7. Dos endereços de Rede (IP)

O endereçamento dos equipamentos conectados à rede é dinâmico e atribuído automaticamente. A utilização de endereços fixos deve ser solicitada pelo usuário a Diretoria de Tecnologia da Informação.

6.14.8. Serviços de Rede Terceirizados

Os serviços de rede de terceiros devem ser documentados e verificados sob o ponto de vista de segurança. Novos sistemas ou redes de acesso a redes externas ao **Grupo CPFL** devem, obrigatoriamente, ser aprovados pelo gestor da Diretoria de Tecnologia da Informação.

6.14.9. Acesso Remoto

É responsabilidade da Diretoria de Tecnologia da Informação garantir que todo acesso remoto aos sistemas do **Grupo CPFL** seja feito através de VPN, Citrix Access Gateway ou Citrix Secure Gateway.

6.14.9.1. VPN

Toda solicitação de acesso remoto através da ferramenta VPN (Virtual Private Network) deve ser previamente autorizada pelo superior imediato, e encaminhada a Diretoria de Tecnologia da Informação conceder o acesso solicitado.

Todo equipamento que necessite acessar a rede do **Grupo CPFL** remotamente deve possuir software cliente de VPN homologado pela da Diretoria de Tecnologia da Informação.

As configurações do software cliente de VPN devem obedecer aos critérios de segurança estabelecidos pela Diretoria de Tecnologia da Informação.

6.14.9.2. CITRIX

Toda solicitação de acesso remoto através da ferramenta Citrix Access Gateway e Citrix Secure Gateway deve ser previamente autorizada pelo gestor e encaminhada a Diretoria de Tecnologia da Informação para análise e aprovação.

Todo equipamento que necessite acessar a rede do **Grupo CPFL** remotamente deve possuir software cliente de Citrix homologado pela Diretoria de tecnologia da Informação.

As configurações do software cliente de Citrix devem obedecer aos critérios de segurança estabelecidos pela Diretoria de Tecnologia da Informação.

6.14.9.3. Perfil de Acesso

É responsabilidade da Diretoria de Tecnologia da Informação implementar controles que evitem a visibilidade, por parte de usuários com acesso remoto, de todo o ambiente de rede ou sistemas do **Grupo CPFL**.

6.14.9.4. Acesso remoto para fiscalizações nos sistemas do Grupo CPFL

O acesso remoto para fiscalizações será concedido mediante ao preenchimento do "Termo de confidencialidade" conforme anexo II.

Este termo deverá ser renovado anualmente.

6.14.10. Manutenção Periódica

Os recursos listados no inventário de ativos tecnológicos devem ser mantidos em condições adequadas de funcionamento. É responsabilidade da Diretoria de Tecnologia da Informação, e de acordo com as orientações do fornecedor, implementar um processo de manutenção periódica.

6.14.11. Transferências de Informações

A troca de informações com terceiros: envio ou recebimento de arquivos, ordens de compra, recebimento ou outra forma de transferência de informações como B2B ou B2C, devem ser previamente autorizados pelo Responsável pela Informação. É responsabilidade da Diretoria de Tecnologia da Informação verificar as implicações e definir padrões de segurança adequados.

No mínimo, devem ser verificados e definidos:

- ✓ Responsabilidades em caso de erro, alteração ou perda das informações;
- ✓ Padrões técnicos e ferramentas utilizadas;
- ✓ Procedimentos de proteção, verificação de envio, recebimento e rastreamento das mensagens.

6.14.12. Meios de Acesso à Internet

É responsabilidade da Diretoria de Tecnologia da Informação, responsável pelo suporte ao usuário, configurar o browser para que os acessos à internet dos colaboradores somente sejam permitidos quando por meio do proxy da rede corporativa do **Grupo CPFL**.

6.14.13. Meios de acesso à informação

O uso de dispositivos de armazenamento removíveis como portas USB (pen drive), gravador de CD, gravador de DVD, não se limitando a estes, não são permitidos e estão desabilitados.

Estes recursos para a gravação de dados não serão aprovados em nenhum momento. Alguma necessidade eventual, após justificativa será encaminhado ao Comitê de Segurança da Informação e passara por avaliação.

Após a avaliação o Diretor da área deverá aprovar o "Termo de Responsabilidade para utilização dispositivos de armazenamento removíveis" onde será descrito o risco que a empresa está exposta em deixar o dispositivo em aberto, e sempre que possível conterá orientações necessárias para mitigação dos riscos.

6.15. Acesso Remoto e Computadores Portáteis

Definir regras de segurança para acesso remoto ao ambiente do **Grupo CPFL** e para uso de equipamentos portáteis é extremamente importante. As regras objetivam minimizar o risco aos quais esses tipos de recurso estão expostos, como alteração, roubo ou destruição de informações armazenadas.

6.15.1. Condições gerais

O **Grupo CPFL** implementa medidas técnicas, incluindo aquelas de rastreabilidade da informação, que busquem garantir a segurança das informações críticas utilizando ferramentas de Siem, e adota as práticas conforme Norma 18758 - Gestão de Logs e Eventos.

6.15.1.1. Proteção das Informações

As informações do **Grupo CPFL** armazenadas em equipamentos portáteis devem ser protegidas de forma proporcional ao seu valor e criticidade. Isto significa que os usuários têm que proteger toda e qualquer informação sob sua guarda, não importando se eles estejam nas dependências da empresa ou em outro local.

6.16. Acesso Remoto

Todo o acesso remoto aos sistemas do **Grupo CPFL** deve ser feito, obrigatoriamente, através de VPN (Virtual Private Network) ou CITRIX. Este acesso deve ser analisado e aprovado pela Diretoria de Tecnologia da Informação.

6.16.1. Condições específicas

6.16.1.1. Treinamento

Antes de ser concedido um equipamento portátil ou acesso remoto, o usuário deve estar informado dos requisitos de Segurança.

6.16.1.2. Comunicação de Perda ou Dano

É responsabilidade do usuário informar prontamente a Diretoria de Tecnologia da Informação em caso de dano, roubo, furto ou perda de qualquer equipamento sob sua guarda. Igualmente importante é informar imediatamente qualquer suspeita de quebra de segurança. A omissão da perda ou dano implicará em responsabilização do usuário.

Adicionalmente deve ser aberto um incidente de segurança através dos canais de comunicação disponibilizados pela Diretoria de Tecnologia da Informação.

6.16.2. Proteção de Informações

É responsabilidade da Diretoria de Tecnologia da Informação implementar ferramentas de criptografia, quando viável tecnicamente, em todos os equipamentos portáteis que contenham informações do **Grupo CPFL**.

6.16.3. Cópia de Segurança

É responsabilidade dos usuários certificar-se de que tenham sido feitas cópias de segurança das informações armazenadas em equipamentos portáteis sob sua responsabilidade e armazenar suas informações em locais apropriados. Em caso de dúvida com relação a padrões ou procedimentos, deve ser consultado pela Diretoria de Tecnologia da Informação.

6.16.4. Programas Antivírus

Quando aplicável, deve ser instalado em todos os equipamentos portáteis um aplicativo antivírus aprovado pela Diretoria de Tecnologia da Informação. Este aplicativo deverá ser configurado para permitir a atualização das definições de vírus sempre que o equipamento for conectado em alguma rede pública.

Da mesma forma que as demais estações de trabalho da empresa, o sistema de antivírus deverá ser configurado para fazer a verificação de arquivos, quando viável, sempre que novas mídias são inseridas (CD-ROM, DVD-ROM, pen-drives ou similares).

6.16.5. Outras formas de Acesso e troca de Informações

A informação deve ser protegida seja qual for a forma de transmissão ou armazenamento.

6.16.5.1. Exposição pública

Informações classificadas como de uso interno ou confidencial do **Grupo CPFL** não deve ser lida, manuseada ou discutida em elevadores, restaurantes, aviões, trens ou em outros lugares de acesso público.

6.16.5.2. Sistema de Mensagem

Os usuários não devem deixar mensagens ou informações confidenciais ou de uso interno do **Grupo CPFL** em dispositivos como secretária eletrônica, SMS e aplicativos de mensageria (ex WhatsApp, Telegram...).

6.16.5.3. Proteção contra Acesso Físico

Os equipamentos portáteis, quando não utilizados, devem ser fisicamente protegidos contra acesso não autorizado. Desta forma, ao se afastarem do equipamento, os usuários devem utilizar recursos de proteção de acesso físico contra roubo de cabos de proteção antifurto, quando possível, ou guardar os equipamentos em armários com chave, principalmente quando estiverem fora das dependências da empresa. Cuidados devem ser tomados em lugares como salas de reuniões vazias, quartos de hotel e centros de treinamento.

6.16.5.4. Transporte de Equipamento Portátil

Os equipamentos do tipo portátil como notebooks, e outros computadores transportáveis que contenham informação sensível não podem ser despachados como bagagem.

Para evitar danos e roubo, estes computadores devem permanecer na posse do viajante como bagagem de mão. Quando transportados em automóveis particulares ou em táxi, estes equipamentos devem ser transportados no bagageiro para evitar furtos quando o veículo estiver parado no trânsito. É fundamental nestes casos que o equipamento não possa ser visto por outras pessoas de fora do veículo.

6.16.6. Protocolo de Recebimento de Equipamento

Computadores portáteis, telefones celulares, Pdas, Smartphones ou similares, de propriedade da empresa, não podem deixar as dependências do **Grupo CPFL** sem que o portador assine o protocolo de recebimento de equipamento de informática que deverá permanecer em posse da Diretoria de Tecnologia da Informação.

6.17. Correio Eletrônico

É necessário estabelecer regras e definir de forma clara que o correio eletrônico é uma ferramenta de trabalho, fornecida ao colaborador para melhor execução de suas funções. O uso e as informações trafegadas devem estar em conformidade com as regras definidas neste documento.

6.17.1. Condições gerais

6.17.1.1. Propriedade da Companhia

O uso de sistemas de comunicações eletrônicas, e todas as mensagens geradas ou transmitidas através do mencionado sistema, são considerados propriedade do **Grupo CPFL**. O acesso à caixa de Correio Eletrônico se dará através de software específico, cuja configuração será feita pela Diretoria de Tecnologia da Informação.

O acesso a caixa de Correio Eletrônico no celular está restrito aos cargos de liderança e especialistas. O acesso também poderá ser disponibilizado aos terceiros para realizarem a prestação de serviços.

6.17.1.2. Uso Autorizado

Os sistemas de comunicações eletrônicas devem ser utilizados exclusivamente para atividades relacionadas aos negócios do **Grupo CPFL**. O uso pessoal ocasional é permissível desde que:

- ✓ Não interfira com a produtividade do colaborador;
- ✓ Não mantenha prioridade sobre nenhuma atividade da Empresa;
- ✓ Não esteja proibido pelas Diretrizes de Segurança da Informação.

6.17.2. Condições específicas

6.17.2.1. Identidade de Usuário

Não é permitido falsear, obscurecer, suprimir ou substituir a identidade de um usuário no sistema de correio eletrônico. O nome do usuário, endereço de correio eletrônico e afiliação organizacional devem corresponder à realidade.

6.17.2.2. Mensagens Monitoradas

Os equipamentos são de propriedade do **Grupo CPFL** e fornecidos ao colaborador para o exercício de suas atividades de trabalho e por esta razão são monitorados para apoiar as atividades de manutenção, segurança, auditoria e outras investigações. Orientamos não salvar documentos com informações pessoais e não utilizar as ferramentas disponibilizadas com outra finalidade que não o exercício de sua atividade. Os usuários devem utilizar as comunicações eletrônicas tendo em mente o fato de que o **Grupo CPFL** se reserva o direito de examinar o conteúdo destas.

6.17.2.3. Revelação Incidental

Pode ser necessário que a equipe de apoio técnico revise o conteúdo das comunicações de um usuário individualmente durante o curso de resolução de problemas. A equipe de apoio técnico, no entanto, não pode revisar o conteúdo das comunicações de um usuário, movida

por curiosidade pessoal ou qualquer outro motivo não relacionado ao suporte de usuário, sem autorização específica do Gestor de Tecnologia da Informação.

6.17.2.4. Conteúdos de Mensagens

Não é permitido utilizar o correio eletrônico para transmitir os conteúdos abaixo:

- ✓ Termos obscenos ou observações pejorativas;
- ✓ Arquivos contendo vírus, jogos, pornografia, músicas/vídeos ou similares;
- ✓ Mensagens de propaganda ou venda de produtos com fins particulares;
- ✓ Cartas de corrente ou “spam”;
- ✓ Conteúdo ou atividades ilegais.

6.17.2.5. Armazenamento

O armazenamento de mensagens de correio eletrônico em diretórios de rede ou discos locais só é permitido quando previamente autorizado pelo Gestor de Tecnologia da Informação.

6.17.2.6. Mensagem para Fora da Empresa

Os usuários de comunicações eletrônicas devem usar de toda precaução ao remeter mensagens. Enviar informações confidenciais ou de uso interno para pessoas fora do **Grupo CPFL** sem a aprovação do Responsável não é permitido.

A área de infraestrutura de Tecnologia da Informação fica encarregada de configurar no ambiente uma Assinatura Padrão pré-definida conforme o ANEXO I.

6.17.2.7. Manutenção de Espaço

É responsabilidade da Diretoria de Tecnologia da Informação definir a capacidade de armazenamento das mensagens bem como o tipo e tamanho do anexo, de acordo com as funções desempenhadas pelo colaborador.

6.17.2.8. Informação sobre Segurança

É responsabilidade do usuário, ao receber mensagens de origem desconhecida ou que contenham arquivos anexos duvidosos, não abrir ou executar tais anexos e encaminhar tal mensagem imediatamente para a Diretoria de Tecnologia da Informação.

6.17.2.9. Uso de Conta de E-mail Particular

A utilização de correio eletrônico de terceiros, tais como Gmail, Hotmail, Bol, Yahoo ou qualquer outro não é permitida.
Necessidades específicas devem ser justificadas no “termo de responsabilidade” para uso dos recursos de informática ou regime de exceção.

6.18. Acesso à Internet

Todos que tem permissão a este recurso devem se atentar aos detalhes desse documento, para que o uso do recurso seja feito de maneira segura, produtiva e somente na execução de tarefas empresariais.

6.18.1. Condições gerais

6.18.1.1. Software de Acesso à Internet

O acesso à Internet se dará através de software específico (browser). A configuração deste software deve ser feita pela Diretoria de Tecnologia da Informação.

6.18.2. Condições específicas

6.18.2.1. Confiabilidade da Informação

Não há nenhum processo do controle de qualidade da informação disponível na Internet. Antes de utilizar uma informação recebida via Internet para finalidades de tomada de decisão, os usuários devem confirmar validade desta informação em pelo menos mais uma fonte.

6.18.2.2. Verificação de Vírus

Todos os arquivos (bases de dados, código de objeto do software, planilhas, documentos de textos etc.) recebidos através da Internet devem ser verificados através das ferramentas adequadas, fornecidas pelo **Grupo CPFL**. Esta verificação visa evitar a infecção dos computadores por vírus ou outros programas maliciosos.

6.18.2.3. Falsificação de Identidade

Exceto que ferramentas como assinatura ou certificado digital sejam empregadas, antes que os usuários forneçam informações, contratem serviços ou efetuem qualquer outra transação, a identidade dos indivíduos e das organizações contatadas deve ser confirmada.

6.18.2.4. Divulgação de Informações Internas

Não é permitido divulgar informações de Uso Interno e Confidenciais através da Internet. Antes de divulgar uma informação o usuário deve se certificar de que esta esteja classificada como pública.

6.18.2.5. Compartilhamento de arquivos na Internet através de discos virtuais

Só é permitido o uso de compartilhadores de arquivos na internet por ferramentas homologadas pela Diretoria de Tecnologia da Informação.

6.18.2.6. Senhas de Acesso

As senhas não podem ser gravadas em programas navegadores ("browser"), ou similares. Esta atitude pode permitir que qualquer um, presente em suas estações de trabalho, tenha acesso à Internet com sua identidade.

6.18.2.7. Autenticação do Usuário

O acesso à Internet local do **Grupo CPFL** só é permitido após a autenticação do usuário.

6.18.2.8. Uso Autorizado

Os sistemas de comunicações instantâneas devem ser utilizados exclusivamente para atividades relacionadas aos negócios do **Grupo CPFL**. O uso pessoal ocasional é permissível desde que:

- ✓ Não interfira com a produtividade do colaborador;
- ✓ Não mantenha prioridade sobre nenhuma atividade da Empresa;

- ✓ Não esteja proibido pelas Diretrizes de Segurança da Informação.

6.18.2.9. Mensagens Monitoradas

O conteúdo e o uso de sistemas de comunicações eletrônicas são monitorados para apoiar as atividades de manutenção, segurança, auditoria e outras investigações. Os usuários devem utilizar as comunicações eletrônicas tendo em mente o fato de que o **Grupo CPFL** se reserva o direito de examinar o conteúdo destas.

6.18.2.10. Conteúdos de Mensagens

Não é permitido utilizar o sistema de mensagem instantânea para transmitir os conteúdos abaixo:

- ✓ Termos obscenos ou observações pejorativas;
- ✓ Arquivos contendo vírus, jogos, pornografia, músicas/vídeos ou similares;
- ✓ Mensagens de propaganda ou venda de produtos com fins particulares;
- ✓ Cartas de corrente ou “spam”;
- ✓ Conteúdo ou atividades ilegais.

6.18.2.11. Permissões de acesso à rede Internet

Os usuários não devem utilizar a Internet ou outros sistemas de informação interna para uso pessoal, de maneira que a sua produtividade ou de outros usuários seja prejudicada.

A permissão ou proibição de acesso a categorias de sites na Internet deve ser uma decisão de alto nível do Comitê de Segurança Empresarial e da Diretoria de Tecnologia da Informação, com base nos quesitos de produtividade, segurança e alinhamento com os objetivos de negócio.

A solicitação de liberação de sites, para atendimento a necessidades de negócio, deve ser formalizada junto a Diretoria de Tecnologia da Informação. Necessidades específicas devem ser justificadas no “termo de responsabilidade” para uso dos recursos de informática ou regime de exceção.

Os sites, que na opinião da Diretoria de Tecnologia da Informação, coloquem em riscos os Ativos do **Grupo CPFL**, somente serão liberados após análise e aprovação do Gestor de Tecnologia da Informação.

6.18.2.12. Acessos Proibidos

O acesso a sites que veiculem os conteúdos abaixo listados não é permitido:

- ✓ Vírus, jogos, pornografia, músicas/vídeos, download e upload de arquivos ou outros conteúdos que não estejam relacionadas ao objetivo do **Grupo CPFL** e a atividade profissional do colaborador;
- ✓ Conteúdo ou atividades ilegais.

6.18.2.13. Registros

O **Grupo CPFL** se reserva o direito de registrar o histórico de navegação do Usuário tais como sites visitados, o tempo de acesso e a informação consultada, para apoiar as atividades de manutenção, segurança, auditoria e outras investigações, em caso de acesso realizado a internet local do **Grupo CPFL**.

6.18.2.14. Acesso à Internet em Áreas Públicas

Independente dos meios onde a informação esteja armazenada, ou seja, transmitida, cada Colaborador deve assumir um comportamento seguro e proativo impedindo seu vazamento para pessoas ou meios externos do **Grupo CPFL**.

Caso seja necessário utilizar quaisquer redes de acesso público, assegure que o acesso a quaisquer informações do **Grupo CPFL** seja feito através de conexões VPN e/ou SSL.

Após o uso de quaisquer redes de acesso público, o colaborador deve desconectar-se dessa rede e desligar o sinal do WI-FI do seu dispositivo.

6.19. Uso de Equipamentos

Este documento apresenta as regras de uso dos equipamentos e sistemas de propriedade do **Grupo CPFL**. O objetivo é orientar os colaboradores sobre como utilizar os equipamentos de forma produtiva e segura na execução de suas tarefas.

6.19.1. Condições gerais

6.19.1.1. Sistemas envolvidos

Esta diretriz se aplica a todo equipamento e/ou sistema de informação de propriedade ou administrado pelo **Grupo CPFL**.

6.19.1.2. Equipamentos

Não é permitida a conexão física de nenhum equipamento à rede de dados do **Grupo CPFL** sem prévio conhecimento da Diretoria de TI.

Qualquer equipamento conectado à rede de dados do **Grupo CPFL**, que não é de propriedade e não é administrado pela Diretoria de Tecnologia da Informação, será retirado pela equipe técnica de TI sem prévia autorização do usuário, sendo acionada a gerência do proprietário do equipamento, caso identificado, notificando a infração.

Exemplo de equipamentos: Roteador Wireless, Hubs, Switches, etc.

Toda e qualquer necessidade de aquisição de equipamentos de TI, deve ser informada à Diretoria de Tecnologia da Informação.

6.19.1.3. Uso autorizado

Os sistemas de informação e computadores de propriedade do **Grupo CPFL** são destinados para atividades empresariais. Uso pessoal ocasional é permissível desde que:

- ✓ Não interfira na produtividade do colaborador;
- ✓ Não mantenha prioridade sobre alguma atividade empresarial;

- ✓ Não contrarie outros itens das Diretrizes de Segurança da Informação.

6.19.1.4. Termos de Compromisso (colaboradores e/ou dirigentes)

O acesso aos Recursos de Tecnologia da Informação do **Grupo CPFL** só é permitido após a assinatura dos Termos de Compromisso que evidenciem o comprometimento do colaborador com os cuidados para com os ativos de informação do **Grupo CPFL**.

6.19.2. Condições específicas

6.19.2.1. Identificação e autenticação

O acesso aos recursos de Tecnologia da Informação do **Grupo CPFL** só é permitido após uma identificação e autenticação de acordo com as Diretrizes de Controle de Acesso.

6.19.2.2. Uso de Senhas

É de responsabilidade dos usuários manter sigilo da senha de acesso aos recursos e sistemas do **Grupo CPFL** e zelar por todas as informações acessadas.

Todos os usuários devem obrigatoriamente escolher senhas fáceis de lembrar, porém, que sejam de difícil identificação. Isto significa que não devem ser utilizadas senhas relacionadas ao trabalho ou vida pessoal, como por exemplo, um número de placa de carro, nome do cônjuge ou data de nascimento.

Os requisitos de complexidade de senhas devem ser observados no item 8. (Documentos Relacionados) das Diretrizes de Segurança da Informação.

6.19.2.3. Padrões Repetidos

Os usuários não podem utilizar senhas compostas de uma sucessão básica de caracteres que são alterados parcial e periodicamente, baseados em data ou algum outro fator previsível. Por exemplo: empregar senhas com sequência alfabética “ABCDE” ou numérica “12345” e sequências lógicas como "A34JAN" em janeiro, por "A34FEV" em fevereiro, etc.

6.19.2.4. Armazenamento de Senha

As senhas não podem ser escritas em locais de fácil acesso a terceiros como: “Mouse Pad”, teclado, blocos de nota, “post it” ou assemelhados. Adicionalmente não é permitido armazenar senhas em arquivos gravados nos discos locais.

6.19.2.5. Compartilhamento de Senhas

O uso da senha de acesso aos recursos e sistemas do **Grupo CPFL** é de caráter pessoal e intransferível.

É responsabilidade do usuário manter as senhas em sigilo. Compartilhar uma senha, ou qualquer outro mecanismo que permita a autenticação, expõe o usuário autorizado à responsabilidade pelas ações de outra pessoa que venha a utilizar seus acessos indevidamente.

6.19.2.6. Troca de Senhas

É responsabilidade do usuário trocar as suas senhas periodicamente e não utilizar as últimas senhas já cadastradas.

6.19.2.7. Configurações de Software e Hardware

O usuário não tem permissão para alterar configurações de software ou hardware da estação de trabalho, nem de instalar ou remover programas. Se houver tal necessidade, estas deverão ser executadas pela Diretoria de Tecnologia da Informação, que é responsável pelo suporte ao usuário.

6.19.2.8. Transporte de Equipamentos

O usuário não tem permissão para alterar a localização física dos equipamentos, exceto equipamentos portáteis. É responsabilidade do usuário solicitar a Diretoria de Tecnologia da Informação que desligue, embale e transporte quaisquer equipamentos considerados Recursos de Tecnologia da Informação.

6.19.3. Monitoração

O uso dos recursos de Tecnologia da Informação é monitorado para apoiar as atividades de manutenção, segurança, auditoria e outras investigações. Os usuários devem utilizar os recursos tendo em mente o fato de que o **Grupo CPFL** se reserva o direito de examinar o conteúdo destes.

6.19.4. Erradicação de vírus

A erradicação de vírus é responsabilidade da Diretoria de Tecnologia da Informação. No caso de suspeita de infecções por vírus, o usuário deve, obrigatoriamente, desligar o equipamento e informar a Diretoria de Tecnologia da Informação que deverá proceder com as medidas cabíveis.

6.19.5. Compartilhamento de recursos

Não é permitido compartilhar recursos, como disco ou outro dispositivo de armazenamento que compõe o computador de uso diário. Se os usuários, para executarem suas tarefas, necessitam compartilhar dados entre si, devem usar diretórios restritos em servidores de rede ou correio eletrônico.

6.19.6. Armazenamento de Informações

Não é recomendável a gravação de informações em discos locais de equipamentos desktop quando conectados à rede corporativa, pois não são feitas cópias de segurança de arquivos armazenados localmente. As informações do **Grupo CPFL** devem ser armazenadas em locais da rede (diretórios ou pastas), ou base de dados, onde serão devidamente protegidas contra acesso indevido. O armazenamento de informações confidenciais ou estratégicas em estruturas de armazenamento compartilhadas não é permitido.

6.19.7. Mídias removíveis

Não é recomendável armazenar informações sensíveis em mídias removíveis como pen drives, CDs, DVDs ou similares.

6.19.8. Modems

É proibido o uso de modems e conexões discadas (dial-up), em equipamentos conectados à rede corporativa do **Grupo CPFL**.

6.19.9. Guarda do Equipamento

O usuário que utiliza sempre ou na maior parte do tempo o mesmo computador para executar suas tarefas é o responsável pelo equipamento. Em caso de falha ou dano o fato deve ser imediatamente comunicado a Diretoria de Tecnologia da Informação.

6.19.10. Comida e Bebida

Não é permitido comer, fumar ou beber utilizando os computadores. Normalmente estes equipamentos são sensíveis e podem sofrer danos em caso de um acidente.

6.19.11. Proteção do Equipamento

É responsabilidade do colaborador efetuar logout ou acionar a proteção de tela sempre que se ausentar de seu local de trabalho.

6.19.12. Impressão

O recurso de impressão disponibilizado para o uso dos colaboradores é destinado unicamente para fins empresariais. Devem ser seguidos os seguintes padrões:

- ✓ É responsabilidade do usuário verificar se foram recolhidos todos os documentos enviados para impressão;
- ✓ É responsabilidade do usuário acompanhar a impressão de informações do **Grupo CPFL.**
- ✓ Quando tecnicamente viável, é obrigatório o uso de senhas para impressão de documentos confidenciais ou estratégicos.

6.19.13. FAX ou similares

É responsabilidade do colaborador garantir a segurança de informações sigilosas quando transmitidas por meios eletrônicos como FAX ou similares.

6.19.14. Mesa Limpa

É responsabilidade do colaborador manter as informações sigilosas adequadamente protegidas contra acesso indevido durante o seu uso diário. É responsabilidade do colaborador, ao final do turno de trabalho, guardar as informações de acordo com as definições das Diretrizes de Privacidade e Classificação de Informações.

6.20. Aquisição, Desenvolvimento e Manutenção de Sistemas

Neste documento estão, objetivamente, descritos controles e conceitos, conforme boas práticas de segurança da informação, para garantir que os processos de aquisição, desenvolvimento e implantação de sistemas, são executados com o objetivo de mitigar os riscos relacionados ao uso de informações, códigos de programação e disponibilidade dos sistemas de propriedade do **Grupo CPFL**. Quando necessário estas Diretrizes serão detalhadas em procedimentos e/ou padrões específicos. Os procedimentos e os controles de gestão de vulnerabilidades, classificação da informação, gestão de riscos deve ser aplicados

no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas em suas atividades.

6.20.1. Condições gerais

6.20.1.1. Papéis e responsabilidades

6.20.1.1.1. Líder Técnico

O líder técnico tem a responsabilidade de interagir com a Diretoria de Tecnologia da Informação e/ou agentes de serviços externos, para certificar-se de que todas as definições de segurança tenham sido implantadas quando da aquisição, desenvolvimento ou manutenção de sistemas.

Quando necessário, a Diretoria de Tecnologia da Informação pode consultar empresas especializadas em Segurança da Informação para avaliar se controles implantados estão de acordo com as boas práticas de Segurança da Informação.

6.20.1.1.2. Líder de projeto

O líder de projeto executa a análise crítica das mudanças de software, considerando requisitos de qualidade e Segurança da Informação, quando necessário o líder de projeto pode obter auxílio da Diretoria de Tecnologia da Informação em relação aos requisitos de Segurança da Informação.

6.20.1.2. Produtos de terceiros

No caso de sistemas adquiridos externamente já completos, conhecidos como “software de prateleira”, é responsabilidade do líder técnico seguir o processo de homologação de software que deve contemplar os requisitos de Segurança da Informação cabíveis. Os registros e documentos fiscais relacionados ficam sob responsabilidade da Diretoria de Tecnologia da Informação.

6.20.1.3. Padrões de nomenclatura

Quando possível, novos sistemas devem ser desenvolvidos adotando uma nomenclatura padronizada, seja de tabelas, campos ou outros componentes necessários.

6.20.2. Condições específicas

6.20.2.1. Validação de dados

É responsabilidade do líder técnico definir controles de verificação de entrada e saída. O líder técnico deve indicar qual parte do processamento lidará com os ativos de informações. Para estes casos, a Diretoria de Tecnologia da Informação deve avaliar a necessidade de controles adicionais.

6.20.2.2. Dados de entrada

Devem ser definidos padrões de verificação de consistência para os dados de entrada. Normalmente os controles de consistência tratam de, entre outros:

- ✓ Verificação de faixa de valores;
- ✓ Verificação de falta de dados ou valores incompletos;
- ✓ Alterações indevidas, no caso de formulário em papel;

- ✓ Identificação de responsabilidades e autorização para entrada de dados.

6.20.2.3. Dados de saída

Devem ser implementados controles de verificação para identificar erros de processamento; recomenda-se a implantação de controles para, entre outros:

- ✓ Verificação de erros de processamento, teste de validação;
- ✓ Verificação e reconciliação caso necessário;
- ✓ Atribuição de responsabilidades de acordo com verificação periódica dos dados de saída.

6.20.3. Controle de processamento interno

A metodologia de desenvolvimento deve possibilitar a identificação de partes do sistema que sejam considerados pontos críticos em termos de integridade, disponibilidade, confidencialidade e performance.

6.20.3.1. Trilhas de auditoria

Operações críticas realizadas pelos sistemas devem conter mecanismos para rastreamento das ações realizadas.

6.20.4. Autenticação e Segurança dos Dados

6.20.4.1. Controle de Acesso

É responsabilidade do líder técnico certificar-se que o novo sistema possua, no mínimo, as seguintes funcionalidades:

- ✓ Possibilidade de integração com os mecanismos de autenticação em uso no **Grupo CPFL**;
- ✓ Possibilidade de troca de senha por parte do usuário;
- ✓ Segurança no armazenamento de informações sensíveis de acordo com os padrões de segurança e criptografia definidos pelo **Grupo CPFL**;

6.20.4.2. Autenticação de mensagens

É responsabilidade do líder técnico incluir controles de proteção e verificação aprovados pela Diretoria de Tecnologia da Informação, sempre que a especificação do sistema incluir a troca de dados ou mensagens sigilosas com outro sistema.

6.20.5. Verificação de requisitos

É responsabilidade do líder técnico definir um plano de teste e homologação. Somente após conclusão, com êxito, das fases de teste e homologação o sistema poderá ser colocado em produção.

6.20.5.1. Segregação de ambientes

Os ambientes de desenvolvimento, testes e produção, devem ser ambientes totalmente distintos. Não é permitido efetuar desenvolvimentos e testes de sistemas em equipamentos de uso pessoal ou estações de trabalho conectadas à rede corporativa.

6.20.5.2. Segregação de funções

As tarefas de desenvolvimento, teste e passagem de sistemas para produção devem ser executadas por equipes diferentes ou, no mínimo, por usuários diferentes.

6.20.5.3. Dados para teste de sistemas

Durante o desenvolvimento e teste dos sistemas não podem ser utilizados dados reais dos sistemas em produção, sem a autorização do responsável pelo Ativo.

6.20.6. Controle de acesso às fontes e base de dados

É responsabilidade do líder técnico definir mecanismos de proteção das bibliotecas de programas contra alterações não autorizadas. Em se tratando de bases de dados de produção, o acesso deve ser restrito ao menor número possível de profissionais e verificado periodicamente pelo responsável.
Caso seja comprovada a necessidade do acesso por outros profissionais, este deve ser liberado por um período determinado, necessário à execução da tarefa, e retirado em seguida. Durante o uso, o acesso deve ser monitorado pelo Responsável.

6.20.7. Controle de alteração de software

Para toda alteração de software deve ser definido um procedimento de requisição e aprovação formal pelos responsáveis. Os controles e procedimentos devem conter no mínimo:

- ✓ Registro da requisição de alteração;
- ✓ Registro da versão em uso e da versão alterada;
- ✓ Plano de instalação que leve em conta o tempo de paradas e possíveis perdas de produtividade;
- ✓ Plano de reversão que leve em conta o tempo de paradas e possíveis perdas de produtividade;
- ✓ Registro dos testes e aprovação da alteração pelos responsáveis.

6.20.8. Controle de versão

A metodologia de desenvolvimento deve prever mecanismos para controle de versão de todos os softwares desenvolvidos ou customizados no **Grupo CPFL**.

6.20.9. Controle contra Ameaças Internas

A metodologia de desenvolvimento deve prever controles que ofereçam proteção contra ameaças tipo “bomba relógio”, “cavalo de tróia” ou similares. Deve ser considerada, no mínimo, a adoção dos seguintes controles:

- ✓ Auditoria, mesmo que por amostragem, das fontes dos sistemas;
- ✓ Verificação dos registros (logs) dos sistemas à procura de atividades incomuns;
- ✓ Rígido controle de mudança quando o sistema operacional puder ser alterado.

6.20.10. Documentação dos sistemas

A metodologia de desenvolvimento de sistemas deve exigir a criação e manutenção de documentação formal que descreva a funcionalidade e os componentes do sistema.

No mínimo devem ser considerados os seguintes pontos:

- ✓ Os manuais devem ser revisados como forma de garantir sua didática e aplicabilidade;
- ✓ A documentação deve ser atualizada de forma a refletir as alterações efetuadas nos sistemas;
- ✓ A documentação deve conter informações de instalação e configuração dos sistemas nas estações, quando aplicável.

6.20.11. Treinamento

A capacitação dos colaboradores na administração e uso dos sistemas é essencial para a segurança e produtividade. O treinamento dos administradores e usuários deve ser parte da fase de implantação dos novos sistemas. Adicionalmente, sempre que os sistemas forem alterados, os administradores e usuários devem ser treinados nas novas funcionalidades.

6.20.12. Controles Criptográficos

Os dados sigilosos de transferência bancária são criptografados e é recomendável que os dados sensíveis enviados ou recebidos através de redes de comunicação devem ser criptografados.

6.21. Proteção de Dados Pessoais de Indivíduos

O **Grupo CPFL** manterá Programa de Governança em Proteção de Dados sob a gestão da Gerência de Proteção de Dados, onde estará alocado o Encarregado de Proteção de Dados nomeado pelo **Grupo CPFL** e que atuará de forma corporativa para todas as empresas com governança direta.

O **Grupo CPFL** tem como valor inegociável a segurança e, portanto, está comprometido com a proteção de dados e buscará cumprir todas as regras legais e regulatórias a ela aplicáveis com o propósito de assegurar aos titulares de dados pessoais que o tratamento das informações seja realizado de forma segura, ética, responsável e informada ao seu real proprietário.

Os compromissos do **Grupo CPFL** com a proteção de dados pessoais de forma resumida são:

•Respeitar a privacidade e a proteção de dados pessoais dos indivíduos que realiza o tratamento de dados pessoais em suas atividades de negócio;
•Assegurar o tratamento de dados pessoais de forma transparente, ética, segura e responsável;
•Tomar medidas técnicas e organizacionais visando assegurar o tratamento de dados de acordo com as leis e regulamentações que regem o tema;
•Promover a cultura de Proteção de Dados nas empresas com governança direta no **Grupo CPFL;**
•Influenciar de forma positiva as empresas do **Grupo CPFL** com governança própria na adoção dos parâmetros de privacidade e proteção de dados do Grupo
•Realizar o monitoramento contínuo do Programa de Governança em Proteção de Dados com o propósito de reduzir os riscos a privacidade dos titulares de dados
•Assegurar os direitos dos titulares de dados com relação a sua privacidade;

•Manter atualizado o inventário de dados pessoais das áreas que realizam o tratamento de dados pessoais de indivíduos na execução de suas atividades;
•Promover canal para atendimento aos direitos dos titulares.

A Gerência de Proteção de Dados atuará na orientação do **Grupo CPFL** quanto a adoção das regras de proteção de dados para execução das operações de tratamento, apoiando inclusive na classificação da categoria de dados e titulares de informação nos termos das leis e regulamentações de proteção de dados.

No atendimento dos requisitos de privacidade e proteção de dados para atendimento das leis e regulamentações relacionadas a Proteção de Dados as Gerências de Proteção de Dados, Segurança da Informação e Tecnologia atuarão em conjunto cada qual em suas competências técnicas e observando as funções e tarefas de suas responsabilidades definidas pelo **Grupo CPFL.**

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Política de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8. ANEXOS

ANEXO I – Mensagem padrão de e-mail externo

Esta mensagem (incluindo anexos, se houver) pode conter dados e informações confidenciais, e/ou confidenciais para o destinatário e é protegida pelas leis aplicáveis. Caso tenha recebido esta mensagem erroneamente, por favor notifique o remetente e providencie imediata exclusão da original e de qualquer cópia, sendo estritamente proibida qualquer divulgação, cópia ou distribuição desta mensagem.

This message (including any attachments) may contain confidential information and data, and/or confidential to the recipient, and is protected by applicable laws. If you have received this message in error, please notify the sender and promptly delete the original message and any copy, is strictly prohibited any disclosure, copying or distribution of this message.

--
---

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
CPFL Paulista	EIQS	Rafael Fedozzi
CPFL Paulista	EIS	Mateus Rocha
CPFL Piratininga	IJC	Michel Franco de Carvalho Ribeiro
CPFL Piratininga	IJC	Vanessa Oliveira Batista
CPFL Piratininga	SBE	Cassio Henrique Florido
Renováveis	PAP	Denise Ramos de Lima
Renováveis	EIS	Everton Duarte

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
1.0	01/07/2022	Criação do documento.

Summary

1. SCOPE

CPFL Group, through its Information Security department, and in line with the purposes and requirements of the business, establishes in this policy the rules and guidelines to be complied with and applied to people, processes and technology in order to protect information owned by **CPFL Group** or held by them and establish the rules for classifying data and information as to their relevance and the adequate level of protection of **CPFL Group**'s information assets according to their value, legal requirements, sensitivity and criticality for preventing unauthorized modification or disclosure.

This document reassures the commitment of **CPFL Group** to business security and good market practices.

The Executive Board of **CPFL Group** has established and supports the Information Security Guidelines in order to protect the information assets and ensure the continuance of business in case of adverse events that may affect the confidentiality, integrity and availability of data and systems and information assets owned by **CPFL Group** and/or under its custody.

The guidelines set out in this document provide a comprehensive view of Information Security (including cybersecurity) applied to the company's business and high-level concepts that must be observed by everyone who somehow uses technological resources, information and/or physically accesses the premises of **CPFL Group** companies.

When necessary, the provisions of this Policy will be detailed in specific rules, procedures or standards.

2. SCOPE OF APPLICATION

2.1. Company

This Policy is applicable to **CPFL Group** and all its subsidiaries and/or affiliates, including those operating in the generation, transmission, distribution and sale of electricity.

2.2. Department

All areas of **CPFL Group**.

3. DEFINITIONS

3.1. Basic Concepts

All technological resources, information systems and business processes have a value and must be protected according to their importance and criticality for the business. The Information Security Management System aims to protect the assets of **CPFL Group**, whether in a physical or digital environment, ensuring the continuance of business by minimizing possible losses and mitigating the risks to which the assets are exposed, always considering the following requirements:

- **CONFIDENTIALITY:** The assurance that the information is accessed only by duly authorized users. This can be ensured through encryption of stored and transmitted data, access controls, data classification, and procedures with adequate training.

- **INTEGRITY:** The assurance that the information is complete, entire and full at the time it is accessed, without any change in its content in relation to when it was stored. Compliance with this security attribute ensures that intruders or errors made by users will not jeopardize the accuracy and integrity of the information, as well as authenticity (certainty as to authorship or origin of the information), non-repudiation (impossibility of denying liability for the acts performed) and auditability (ease of reaching the origin and consistency of the information). This can be maintained through encryption techniques, recording user logs, review processes and approval by different levels of changes in systems and information.

- **AVAILABILITY:** Assurance that the information is available to the user (who has such access authorization) and to the information system at the time required by **CPFL Group**, even in the event of a disaster. This can be maintained through backup procedures and respective storage management.

- **INFORMATION SECURITY:** Protection of information against threats, whether in a physical or digital environment, to ensure the continuity of **CPFL Group**'s core activities, minimize risks and maximize the efficiency and effectiveness of the actions carried out by **CPFL Group**.

- **INFORMATION SECURITY INCIDENT:** Occurrence that compromises or may potentially compromise the availability, integrity, confidentiality or authenticity, adverse, unwanted or unexpected, confirmed or suspected event that may compromise the confidentiality, integrity or availability of information, whether they are in the physical or logical environment **CPFL Group**.

- **MAJOR IMPACT INCIDENT:** It is established based on the severity rating included in **CPFL Group**'s information security risk management process.

- **PERSONAL DATA INCIDENT:** Security incident that accidentally or illicitly causes the destruction, loss, alteration, disclosure or unauthorized access to personal data of individuals transmitted, preserved or subject to any other type of handling by **CPFL Group**.

- **CONFIDENTIAL INFORMATION:** Information that if compromised may negatively impact the provision of services to people and adversely affect the business of CPFL Group and third parties.
- **CYBERSECURITY:** subclass of Information Security, since its purpose is to protect information security in a digital environment, that is, protects assets against cyber threats and malicious attacks.

- **CPFL GROUP:** CPFL Energia S.A., and all its subsidiaries and/or affiliates, except for companies with their own governance and management standards the control of which is shared with other companies.

- **SUBSIDIARIES:** Companies directly or indirectly controlled by CPFL Energia.

- **AFFILIATES:** Companies in which CPFL Energia holds a 50% or less interest, directly or indirectly.

- **INFORMATION NETWORK:** The Company's corporate data network comprising all its own and third-party telecommunications infrastructure intended for Information Technology assets.

3.2. General Concepts

- **Good Information Security Practices**
  The recommendations contained in standards and bodies such as those listed below are considered good information security practices: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) and others internationally recognized;

- **Security Settings (Baselines)**
  Information security configuration requirements, recommendations, and best practices for resources/assets. These are the minimum settings acceptable by **CPFL Group** for assets/resources within each context;

- **Control**
  Any resource or measure that ensures ways to handle risks, including reduction, elimination or transfer. Information security is materialized by implementation and proper maintenance of controls. Controls may be understood as: policies, processes, organizational structures, standard techniques, software, hardware and others;

- **Manager**
  Employee in a leadership role, such as: president, vice president, officer, manager, coordinator, leader or section chief;

- **Information**
  Any organized set of data that has some purpose and value for **CPFL Group**, its customers, partners and employees. The information may be owned by the company, or be directly in its custody (filing and internal processing) or in the custody of third parties (suppliers, partners and service providers that support **CPFL Group**'s activities), such as, for example, cloud stored information

- **Least Privilege and Need to Know principles**
  These principles should govern the authorization of any access to systems and information. According to them, only the minimum level of access (Least Privilege) should be granted to those who really need access (Need to Know). That is, access must be granted to the minimum necessary extent to the performance of the work, taking into accounting what is needed for the duty to be performed;

- **Resources**
  Any resource, tangible or intangible, belonging to, at the service of or under the responsibility of **CPFL Group**, which has value for the company. Resources will include: physical environments, technologies, contracted services, cloud services, systems and processes;

- **Critical Resources**
  Essential resources for the operation of **CPFL Group** and that have critical or sensitive information, also known as critical assets. Resources can be typified as: people, technology, and data/information. In which regards technology, we have the infrastructure elements, information systems and tools;

- **Risk (s)**
  Any uncertainty in relation to events or situations to which the institution is exposed and which may impact business results.

- **Threat**
  Any potential cause of an unwanted incident that could impact the business purposes. Threats can be internal or external, intentional or unintentional;

- **Vulnerability**
  Weakness of an asset or control that can be exploited by one or more threats. It means the absence or weakness of a preventive measure that can be exploited.

- **Security Controls**
  Preventive measures or countermeasures used to mitigate potential risks

3.3. Specific Concepts

- **Categories of Responsibilities**
  CPFL Group adopts the system of categories and responsibilities to operationalize the control of security-related rights and duties.

- **Person in Charge of the Asset**
  Every application, system or critical information shall have a designated Person in Charge. The Person in Charge shall define the classification of information and the access profile per user (including privileges) in order to ensure compliance with information security requirements (confidentiality, integrity and availability), as well as guarantee the retention of evidence of the execution of their controls for submission in case of audits or if it is required to comply with regulations;

- **Asset Depositary**
  The Depositaries have physical or logical possession of the information. Depositaries are responsible for the custody of information, and also for the implementation of access control systems and backups. The Depositaries are also responsible for the implementation, operation and maintenance of security measures in accordance with the classification of information carried out by the Persons in Charge;

- **User**
  Users are responsible for familiarizing themselves and complying with all applicable Information Security items. Questions about the proper handling of a specific type of information should be addressed to the Asset Depositary, the Person in Charge of the Asset, or the Information Security Management;

4. REFERENCE DOCUMENTS

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- ABNT/ISO 27032-2013;
- ABNT/ISO 31000-2009;
- GED 18744 - **CPFL Group** Information Classification
- GED 13307 - **CPFL Group**'s Risk Management Policy
- GED 14634 - Use of **CPFL Group**'s Email
- GED 18744 - **CPFL Group** Information Classification
- GED 19127 - **CPFL Group**'s Safe Disposal Standard
- GED 18928 - **CPFL Group**'s General Data Protection Standard
- GED 14141 - **CPFL Group**'s Access Management Standard
- GED 18851 - **CPFL Group**'s Information Security Incident Response Plan;
- GED 19232 - **CPFL Group**'s Code of Ethical Conduct;
- This Policy is supplemented by other **CPFL Group**'s Standards and Procedures.

5. RESPONSIBILITIES

Every Employee, regardless of position, function or place of work, is responsible for the security of **CPFL Group**'s information and shall comply with the provisions of this policy and the standards and procedures related to it. The obligations and responsibilities of those involved are set out below:

- **Employee:**

  ✓ To safely, responsibly, morally and ethically use all information, data, systems and technology tools made available by **CPFL Group**;

  ✓ To protect information against access, disclosure, modification or destruction not authorized by **CPFL Group**;

  ✓ Ensure that equipment and technological resources available to him/her are used only for the purposes approved by **CPFL Group**;

  ✓ To properly dispose of printed/logical documents and information according to their degree of classification and in compliance with the Information Security guidelines;

  ✓ To notify the Information Security department about violations of the Information

Security Policy and/or other standards and procedures, as well as about security and personal data incidents that they become aware of;

- ✓ To ensure the confidentiality of the information to which he/she has gained access as an Employee of **CPFL Group**, even after leaving the company;
- ✓ To actively participate in the Information Security Awareness and Disclosure Program.

- **Manager:**
  - ✓ To inform, at the stage of hiring and execution of individual employment contracts, the responsibility for complying with policies, standards and procedures related to information security;
  - ✓ To comply with and enforce this Policy, the Information Security Standards and Procedures;
  - ✓ To require partners, service providers and other external entities to execute the confidentiality agreement regarding the information to which they will have access;
  - ✓ To develop, with the support of the Information Security Management, information security procedures related to their areas, providing the necessary information and keeping it updated;
  - ✓ To inform, whenever necessary, updates regarding processes and/or data records of employees so that permissions can be granted or revoked as necessary;
  - ✓ To ensure that their subordinates have access to and get knowledge of this Policy and information security standards;
  - ✓ To periodically assess the degree of secrecy and security necessary to protect the information under his/her responsibility and that of his/her team;
  - ✓ To designate more than one person as responsible for acting in processes and operations susceptible to fraud and take due care to preserve the division of duties;
  - ✓ To call the relevant departments for application of penalties applicable to Employees who violate the information security guidelines provided for in the **CPFL Group**'s Code of Conduct, in this document and in other related standards and procedures;
  - ✓ To authorize his/her employees to access systems and environments only when such access is really necessary and according to the concepts of “least privilege” and “need to know” that must be essentially related to the duties and tasks performed by them;
  - ✓ To encourage his/her teams and employees to participate in actions related to the Information Security Awareness and Disclosure Program.

- **Information Security Management:**

  - ✓ To seek alignment with the organization's guidelines;
  - ✓ To propose methodologies and processes related to information security, such as information classification, risk assessment, vulnerability analysis, etc.;
  - ✓ To guide and coordinate information security actions, enforcing execution in compliance with what has been established;
  - ✓ To perform all activities inherent in the vulnerability handling cycle;
  - ✓ To seek the safe use of networks and services of electric power stations;
  - ✓ To engage the areas in charge of corrections in the timely handling of vulnerabilities;
  - ✓ To identify new threats, monitor existing ones, and track fixes;
  - ✓ To update this document whenever applicable;
  - ✓ To conduct and monitor vulnerability tests;
  - ✓ To create simulations of scenarios and threats for resilience tests, analysis of tools and capacity and response time;
  - ✓ To create procedures and controls to reduce vulnerability to incidents and meet other cybersecurity objectives;
  - ✓ To define the rules for installing software and hardware in **CPFL Group**;
  - ✓ To approve personal equipment (smartphones and notebooks) for use on the **CPFL Group**'s network;
  - ✓ To keep an updated record and control of all access releases granted, promptly suspending and altering such releases whenever it is requested in writing;
  - ✓ To develop, disseminate and establish programs for awareness and dissemination of the Information Security Policy and cybersecurity culture;
  - ✓ To implement, monitor and report the performance of programs for the training and periodic evaluation of personnel and actions of the annual awareness program;
  - ✓ To disseminate the cybersecurity culture;
  - ✓ To create measures to raise awareness and educate **CPFL Group** employees on cybersecurity aspects;

- ✓ To conduct the Information Security Risk Management process;
- ✓ To conduct the Management of Information Security Incidents, including investigations to determine the causes and persons responsible and the communication of the facts that occurred;
- ✓ To identify, protect, diagnose, respond to and recover from cyber incidents and prevent, detect, respond to and reduce vulnerability to cyber incidents;
- ✓ To identify, assess, classify and handle cyber risks within the structure established by **CPFL Group**;
- ✓ To seek cooperation between the various agents involved with the aim of mitigating cyber risks, observing the information confidentiality rules set out in GED 18744 - Information Classification;
- ✓ To conduct the monitoring and security processes of information and technology assets (systems, databases, network resources), with reference to the Information Security Policy, standards and procedures;
- ✓ To define mechanisms to prevent, mitigate and recover cyber incidents on the Information Network or on the premises network, and to prevent incidents from affecting the operation
- ✓ To define controls for handling risks, vulnerabilities, threats and non-conformities identified by the IS processes;
- ✓ To define and provide Information Security training and awareness programs;
- ✓ To assist the other areas, including the legal department, in the analysis of information security requirements in contracts entered into with **CPFL Group**, when applicable;
- ✓ To propose projects and initiatives to improve the level of security of **CPFL Group**'s information; and
- ✓ To act with responsibility, care and transparency;

- **CISO:**
  - ✓ To Approve the Information Security documents/standards/procedures/guidelines;
  - ✓ To designate a person as responsible for approving Information Security documents, standards, procedures and guidelines in his/her absence;

- **Information Technology Executive Board:**
  - ✓ To keep the technological infrastructure up to date, as recommended by hardware

and software manufacturers;

- ✓ To handle the risks and vulnerabilities identified in assets, systems or processes under his/her responsibility or custody;
- ✓ To conduct the management of access to systems and information of **CPFL Group**;
- ✓ To implement and maintain functional controls and security standards defined for technology assets;
- ✓ To immediately inform the Information Security area of violations, failures, anomalies and other conditions that may put **CPFL Group**'s information and assets at risk;
- ✓ To control changes in IT assets and ensure that they are critically analyzed and tested so that there are no adverse impacts on the company's operation or security;
- ✓ To ensure the continuity of technological services in order to meet essential business requirements; and
- ✓ To ensure that all critical Information Technology assets are installed in specialized environments known as Datacenters. Such centers shall be equipped with all the necessary protections and contingencies to protect them.

- **Information Security Committee:**

- ✓ To propose improvements, changes and adjustments to the Information Security Policy;
- ✓ To propose investments related to information security in order to minimize risks (including legal and regulatory risks);
- ✓ To classify and reclassify the level of access to information, whenever necessary;
- ✓ To evaluate security incidents and propose corrective actions;

- **Legal Executive Board:**

- ✓ To support and assist the Information Security Management on legal issues involving the application of disciplinary measures to the internal staff member responsible for violations of the Information Security Guidelines and other related standards and procedures;
- ✓ To advise on legal, regulatory or contractual obligations relevant to information security and any legal security requirements in order to meet business requirements;
- ✓ To adopt, with the support of the Information Security Management, clauses relevant to information security in the legal transactions carried out with **CPFL Group** in order to ensure that the information security guidelines, standards and procedures are observed by suppliers, partners and third party contractors.

- **Suppliers and Business Partners:**

  ✓ To comply with the provisions of **CPFL Group**'s information security and data protection Policy, standards and procedures (when applicable);

  ✓ To comply with the confidentiality agreement entered into with **CPFL Group**;

  ✓ To instruct its employees, agents, third parties and any subcontractors to comply with the provisions of **CPFL Group**'s information security and data protection Policy, Standards and Procedures; and

  ✓ To adopt, in the fulfillment of the purpose of the contract/partnership, security measures consistent with the criticality of the information used, according to the classification of the information and other processing and confidentiality rules determined by **CPFL Group**.

- **Service Providers/Third Parties:**

  ✓ If they handle data or Confidential Information or other information that is relevant to the conduct of operating activities at levels of complexity, scope and accuracy compatible with those used by **CPFL Group**, they shall comply with this Policy, or the **CPFL Group**'s Information Security Incident Response Plan, or have procedures and controls for preventing and handling incidents.

- **Data Protection Management:**

  ✓ To provide guidance on data protection rules applicable to information identifying or rendering identifiable individuals whose data is handled by **CPFL Group**.
  ✓ To make an assessment of the impact in terms of data protection of the handling of personal data on the business activities of **CPFL Group.**
  ✓ To carry out the risk or damage assessment relevant to the data subjects in the event of a data incident, and provide guidance on the giving of notice to the National Data Protection Authority and the data subjects relating to the event.

- **Senior Management:**

  ✓ To commit to the continuous improvement of procedures related to information and cyber security;
  ✓ To provide resources for the implementation, maintenance and improvement of information security and data protection management;
  ✓ To provide the Information Security and Data Protection Managements with guidance, support and recommendations, pointing out any restrictions when necessary.

6. BASIC RULES

Information is an essential asset for an organization's business and, as such, must be properly protected. This is especially important in an increasingly interconnected business environment.

The protection of **CPFL Group** assets takes into account the criticality of information and systems in the business processes, that is, the importance, indispensability and ability to recover information and systems in operational processes through the BIA (Business Impact Assessment) method.

Information security is the protection of information against various types of threats in order to minimize the company's exposure to risks, ensuring that the fundamental characteristics of the information are preserved, namely: confidentiality, integrity, availability and compliance. This means protecting the company against information leakage and fraud, ensuring privacy, protecting employees in the event of an incident that directly involves them, assuring that systems and information are available when necessary, and ensuring the protection of the company's image and brands.

CPFL Group, through its Information Security Management and in line with the purposes and requirements of the business, establishes in this policy rules and guidelines to be followed by and applied to people, processes and technology in order to protect the Company's information, its employees, customers, suppliers and business partners.

In general, following the provisions of this policy means preventing fraud, protecting the company against information leakage, ensuring privacy and availability of systems and information when necessary, as well as ensuring the protection of **CPFL Group**'s image and brand.

6.1. Policy Management General Aspects

The Information Security area is responsible for reviewing/updating the Information Security Policy periodically every 12 months, whenever necessary or in the event of a significant change in the **CPFL Group**'s information security context as result of new laws, systems or incidents.

After the periodic updating of this policy, the Board of Directors of **CPFL Group** shall be responsible for its written approval.

The policy shall have protective measures against any unwanted and unauthorized changes, such as access control.

6.2. Compliance

Compliance with and adherence to the laws, regulations, Information Security Policy, rules, contractual obligations and security standards are mandatory and shall be enforced by all Employees of CPFL Group.

Persons responsible for critical resources of **CPFL Group** shall ensure the retention of evidence of the performance of their controls to be provided in cases of audits or in need of compliance with the regulations.

6.3. Information Security Committee

CPFL Group designates the Information Security Committee as the highest authority for evaluating policies, standards and procedures relating to Information Security. Since total security is impossible to achieve in practice, the committee shall follow the GED 13307 Standard, which sets acceptable risk levels for **CPFL Group**.

The Information Security Committee is a multidisciplinary body preferably consisting of representatives from the Information Technology, Legal, Human Resources and Internal Audit departments. The members of the committee shall be chosen by **CPFL Group**.

The Ethics Committee of **CPFL Group** shall be responsible for enforcing disciplinary measures against non-compliance with the rules set forth in this policy.

6.22. Information Classification

All information must have an owner (Information Manager) and shall be properly classified according to the business need and the legal requirements for sharing or restricting such information.
Physical assets, in addition to information assets, shall also be classified according to the label assigned to the information stored, processed, handled or protected by it and be compatible with the sensitivity of data and information. **CPFL Group** adopts the following categories for classifying information, as described in the following subsections:

6.22.1. Public Information

Public access to this information does not cause any damage to **CPFL Group**, its employees or business partners. Any information can only be disclosed to the public if it is classified as such, as defined by the Person in Charge, according to 3.3. Specific Concepts.

6.22.2. Internal Use Information

This information is understood to be for access and use by CPFL Group and, in some cases, by its business partners, and public access to it (on the Internet, for example) is prohibited. Access by others to this information may harm the company, its employees and its business partners. Information classified as Internal Use may be in emails (for email classification see GED 14634 - Use of Email, reports, control spreadsheets, telephone list, among others.

6.22.3. Confidential Information

Confidential information is information that, due to its criticality to the business, must have restricted and controlled access and distribution. Therefore, this information should only be accessed by those who really need to know it in order to perform their activities in the organization. This category is related to sets of information, such as banking information, information about customers or specific contracts, information about Human Resources or other information whose unauthorized disclosure could cause serious damage to the organization. **Information that is not classified shall be deemed as Internal Use Information.**

Every employee is responsible for ensuring the security of confidential information that is under his/her custody or within his/her reach, in order to prevent such information from being read or copied by an unauthorized person.

6.23. Handling of Information

The information shall have (i) rules clearly defined by its owner to protect it against loss, alteration and/or undue access, regardless of the medium in which it is stored; and (ii) explicitly defined user, with the respective types of access rights determined.

6.23.1. Information Reclassification

The information shall be reclassified whenever the Person in Charge identifies that it is necessary. When making any reclassification, the Person in Charge shall properly notify all interested parties.

6.23.2. Information Destruction

When the information loses its usefulness or value it must be destroyed or, in the case of personal data of individuals or a group of individuals, anonymized (to be used only for statistical purposes).

The Person in Charge of the assets has the power to decide on the destruction or anonymization of the information, unless there is a law, regulation or internal rule determining on the allocation of the information. For more information, see GED 18744 - Information Classification, and/or 19127 - Safe Disposal Standard.

When disposed, documents printed with the confidential label shall be completely destroyed using equipment such as shredders, so that reproduction will not be possible after disposal.

6.23.3. Information Storage

The storage of information shall be made with security controls appropriate to the level of confidentiality of the information.

6.23.4. Information Transmission

It is desirable that the information be transmitted through appropriate means that ensure the level of confidentiality of the asset.

For more information, see the Information Classification Standard (GED 18744).

6.23.5. Sharing

All information shared with third parties shall be classified according to established labels. The sharing of information is not restricted to companies of the same corporate group. **CPFL Group** adopts a procedure for sharing information on threats/vulnerabilities and other information related to cybersecurity in a confidential and non-discriminatory manner. The sharing of information does not include information classified by CPFL Group as confidential or that may compromise its own security. When sharing information with third parties via email, the title of the email and the title of the attached document shall be labeled. If the email contains an attachment with confidential information, the file shall be password protected. And when it comes to sharing personal/sensitive/under 12 data, the area shall meet the privacy requirements set out in the General Data Protection Standard (GED 18928).

The sharing of personal information of individuals shall only occur if necessary to fulfill the purpose set out in a legal instrument/data handling document, with registration of the sharing

is assured in a way that renders it possible to ensure the enforcement of the rights of the data subjects guaranteed under the General Data Protection Law.

In case of sharing personal data of any category, the information shall be masked, whenever possible, by removing any data that refers or can be related to the data subject. The lower the possibility of identifying the individual or group of individuals, the lower the risk in case of improper access/data leakage.

The sharing of any information classified as Confidential may only be made in an encrypted form. In case of personal data, sensitive personal data and/or data belonging to minors under the age of 12, it is mandatory that there is a record of the activity in the personal data inventory identifying at least: location/date/time/sharing tool/authorized addressee/list of shared information.

Important: If sharing is necessary involving sensitive personal data and/or data of children under 12 (i) if internally, such sharing shall be made according to the access management rules defined by the person responsible for the database that will be impacted by such sharing; and (ii) if externally, the person responsible for extracting the information shall (a) ensure that the sharing of data to a third party is registered in the area's "data mapping" (see Privacy Ambassador), otherwise the data will not be able to be shared; (b) ensure that there is a current contract containing data protection rules; (c) keep the list of shared information registered so that it is possible to confirm, in fulfillment of the rights of data subjects, what was shared, about whom, and who the recipient is (the statute of limitations for maintaining the information shall be observed); (d) follow data protection standards and procedures, as well as information security rules applicable to data protection.

6.24. Human Resources Security

It is extremely important to ensure that employees, suppliers and third parties have prior and duly documented knowledge of their responsibilities for the protection of **CPFL Group** assets and compliance with relevant laws and regulations, and the concepts described in this section shall be observed from pre-contract to termination or end of contract.

6.24.1. Assignment of Responsibility

Employees, suppliers and third parties shall be clearly informed of their responsibility from an Information Security point of view, and they shall comply with **CPFL Group**'s Information Security Guidelines, and the agreements, training and awareness records shall be registered in proper document and/or stored in specific software.

6.24.2. Specific Conditions

The following conditions described in the subsections below shall be complied with by Human Resources managers.

6.24.3. Contract Terms and Conditions

The Human Resources Department shall cause employees and/or officers of the **CPFL Group** companies to sign a Commitment Agreement at the time of hiring the employees. The Commitment Agreement is a guarantee that the people agree with their responsibilities related to the protection and proper use of **CPFL Group** assets.

6.24.4. Onboarding Training

New employees and third parties shall receive information security training, focusing on the Information Security Guidelines. This training can be given together with the onboarding training for new permanent employees and for third parties when they start their activities at **CPFL Group** or in the following month.

6.24.5. Periodic Training

It is extremely important to ensure that employees and **Third Parties** have prior and duly documented knowledge of their responsibilities related to protection, use of information and information assets of **CPFL Group**. For such purpose, awareness campaigns and materials as well as training shall be made available and properly disclosed.
Training and awareness records shall be created in an appropriate document and/or stored in specific software;
Information Security Training shall be provided at least annually, with training refresher available at the **CPFL Group** University;
Information Security training shall be supplemented by dissemination campaigns with awareness materials to be disseminated, interspersed with training schedules, as needed. These materials can be disseminated in different formats: email, banners, intranet, paper documents, and websites, among others.
The content of Information Security training and awareness shall address the topics contained in **CPFL Group**'s Information Security Guidelines and regulatory documentation, including, but not limited to:

- Privacy and classification of information;
- Logical access control;
- Physical access control;
- Continuity of Business;
- Information Security Incidents;
- Remote Access and mobile devices;
- Email, internet and corporate instant messaging applications;
- Acquisition, development and maintenance of systems.

Periodic tests and simulated drills

Periodically, the IT Security Management area performs tests and simulated drills to measure the level of awareness of the employees. Such activity aims to guide and train, as well as increase the company's level of protection with an increased safety maturity gained by the employees.
The tests can be taken through various communication channels, such as email, instant messaging, etc.

- **Phishing Test**

This exercise is carried out by sending emails that simulate malicious messages aimed at stealing information or access credentials. The purpose is to test the employee's attention and perception to identify the scam.
At the end of each test, when the employee is not successful, there will be an automatic route to a mandatory course to reinforce the applied concepts. The immediate manager will be notified to monitor the progress of his/her team member. When the course is not taken, the area officer will be involved to assist in the guidance towards it.

The Human Resources Managers and the Information Security Management Department are responsible for developing and promoting information security training and awareness programs, disseminating the cybersecurity culture in the institution and implementing training programs and periodic assessment of personnel.

6.24.6. Safe Behavior

Regardless of the means where the information is stored or transmitted, each Employee shall have a safe and proactive behavior preventing it to be accessed by unauthorized third parties, both in relation to employees, third parties, suppliers and business partners of **CPFL Group**.

Employees are prohibited from giving opinions on behalf of **CPFL Group** when their function does not allow them to do it, or from using confidential or information for internal use by the Organization in: emails, websites, social networks, printed publications, discussion forums, Internet services and other public environments, given the possibility of inadvertent disclosure, see Code of Conduct.

You shall not make connections in public areas such as shopping malls and airports; avoid accessing, viewing or editing any information or page that requires the input of confidential data, such as passwords, banking information or data relating to **CPFL Group**.

6.24.7. Disciplinary Process

Failure to comply with the rules set out in **CPFL Group**'s Information Security Guidelines may, without prejudice to compensation for damages caused, result in:

- ✓ Verbal warning;
- ✓ Written warning;
- ✓ Temporary suspension of access rights;
- ✓ Contract termination without payment of fines by **CPFL Group**;
- ✓ Dismissal.

The Human Resources and Information Technology Departments shall maintain formal procedures to ensure the handling of security incidents and provide a gradual response that considers the following factors:

- ✓ Nature of the violation;
- ✓ Severity of the violation;
- ✓ Business impact;
- ✓ Number of violations by the violator.

6.24.8. Communication of Change of Positions

For proper access management, the Human Resources Department shall send notice to the Information Technology Department in the event of any change of position or activity.

6.24.9. Blocking Access Rights

In the event of temporary absence of employees or third parties as a result of vacations, health or maternity leave, the Human Resources Department is responsible for notifying the Information Technology Executive Board so that the necessary measures can be taken. The Information Technology Executive Board shall analyze each case according to the permissions granted to the employee. In which regards Third Parties, the contract manager and/or the area with which the third party works, shall notify the Information Technology Executive Board.

6.24.10. Revocation of Access Rights

The Human Resources Department shall notify the Information Technology Executive Board of terminations so that the necessary measures can be taken. As regards Third Parties, the contract manager and/or the area with which the third party works shall notify the Department.

6.25. Access Control

To ensure an adequate level of protection for CPFL Group's systems and information, as well as to comply with regulations, it was determined that all user accesses shall be duly registered, approved by those responsible and periodically reviewed. Where technically feasible, the provision of access rights shall be automated and error detection methods shall be established.

6.25.1. General Conditions

The general conditions set out in the following subsections shall be satisfied especially by the Information Technology Executive Board and the areas that in some way perform tasks related to access in the information technology environment.

6.25.2. User Registration

Every user who accesses the **CPFL Group**'s Technology environment shall be logically and uniquely identified by their account (“user-ID” and password) for exclusive use.

6.25.3. Registration and exclusion

The Information Technology Executive Board shall implement and control procedures for the approval, creation, blocking and exclusion of users in the systems. When technically feasible, the employee information contained in the Human Resources database shall be used as a source for employee registration in other systems.

6.25.4. Privilege Control

The Information Technology Executive Board shall control access rights as “super user”, administrator or any other denomination that means additional powers to install, change or delete information. The controls shall observe, at least:

- ✓ Use of a user different than the normal user, when performing “super user” tasks;
- ✓ Clear identification of which users have access to “privileged accounts”;
- ✓ When technically feasible, keep records of account usage.

Only users authorized and approved by the Information Security Management and the manager in charge may have ADM privileges for the environment.
Exceptions will be analyzed and shall be approved by the manager of the person in charge, informing the risk of such type of access, filling out the “Statement of Liability concerning the Local ADM privilege”, and making access by using the Password Vault tool.

6.25.5. Privileges in Specific Equipment

The Information Technology Executive Board shall set up the rights of domain users so that they have minimum access rights on the workstation, but sufficient to perform their tasks.

Specific needs shall be justified in the "Statement of Liability concerning the Local ADM privilege” and approved by the applicant's superior (at least Manager) and by the Information Security Manager, and attached to the open access release call on the Portal of Shared Services.

6.25.6. Access Password Setup

The Information Technology Executive Board, whenever technically feasible, shall customize the systems to match at least the following rules:

- ✓ Use at least eight characters;
- ✓ Use of alphanumeric characters;
- ✓ Password expiration time: sixty days;
- ✓ Do not allow repeated patterns, such as: alphabetical sequence “ABCDE” or numeric sequence “12345”;
- ✓ Require exchange periodically;
- ✓ Do not allow the use of the last twenty-four passwords;
- ✓ Require the change of the default password on the user's first access;
- ✓ Blocking access after five unsuccessful attempts.

The Information Technology Executive Board, in specific cases and in order to protect **CPFL Group**'s assets, may define a period different from the standards set above.

6.26. Password Storage

The passwords registered to access the **CPFL Group**'s environments and systems are personal and non-transferable, and they shall be kept and used exclusively by the authorized user. Thus, they cannot be stored legibly in files, databases, software macros, function keys, terminals or in other places to which unauthorized persons may have access.

6.26.1. Default Passwords

The Information Technology Executive Board shall change the password of equipment or systems that use a default password at the time of installation or receipt before start-up. The new password default shall according to the definitions of specific procedures and/or the Information Security Guidelines.

6.27. Use of Privileged User

Standard user accounts with privileged access, such as “root”, “administrator” and others cannot be used in tasks that are not specific to the administration of technology environments.

6.27.1. Access Review

Those responsible for access profiles shall review the rights granted to users according to the frequency of each environment. A joint effort by the Person in Charge and the Human Resources is recommended to revoke redundant or unnecessary rights.

Users with special privileges to access critical systems shall have their rights reviewed periodically as defined in the periodicity of each environment. Special privileges mean functions of administrators or operators with the right to write or change systems and/or Databases.

6.27.2. Usage Profiles and Rights

Access profiles shall be created for users in order to reduce risks related to access management. Access profiles mean that several users are under the same rules and can be managed together.

All access profiles shall have a designated Person in Charge. The Person in Charge of the profiles shall:

- ✓ Determine, jointly with the Information Technology Executive Board, the rights of users;
- ✓ Approve the registration of new users;
- ✓ Review and be responsible for the actions of users, using the permissions conferred by the functions;
- ✓ Periodically review the validity of the rights granted.

6.27.3. Protection against Undue Access

The Information Technology Executive Board is recommended to define a procedure for blocking users who do not access critical systems (defined in GED 14141) for a specified period.

6.27.4. Revocation of Access

The Information Technology Executive Board shall revoke all access rights in any of the following events:

- ✓ Employee termination notice sent by the Human Resources Department;
- ✓ Revocation request sent by the Person in Charge of the profile or group;
- ✓ Revocation Request submitted by Contract Manager or Immediate Third Party Manager.

When technically feasible, an automated process may be implemented to detect termination and automated revocation of rights of employees and/or third parties.

6.27.5. Segregation of Duties

In order to prevent opportunities for unauthorized use, damage or loss of information and related risks, there shall be mechanisms for segregation of duties in systems and operations that support the company's financial information to prevent fraud and loss. The areas involved in the process shall analyze and remedy conflicts. If remediation is not possible, the business areas responsible for the process, together with the *Person in Charge of the asset*, shall inform a mitigating action (compensatory control) for the risk, notifying the Internal Controls Management, for evaluation. The Information Technology Management area shall register such

action in the respective function segregation matrix, instruct the areas involved on the concepts, and carry out the management of the function segregation matrix, in order to ensure that the information will be properly available to the evaluating bodies.

6.28. Business Continuity Plan

CPFL Group understands that ensuring business continuity in the event of adverse situations is extremely important, and the guidelines established in this document shall be followed to guide those responsible for preparing the Continuity and Contingency plans. Such plans shall be formalized and tested periodically.

6.28.1. General Conditions

6.28.1.1. Impact Identification

A business continuity management process shall be implemented to minimize to an acceptable level the impact on the organization resulting from, for example, acts of God, accidents, equipment failures and intentional actions.

For such purpose, it is necessary that the consequences of an unavailability, loss of confidentiality or integrity of the information are submitted to a business impact analysis.

The result of such analysis shall clearly identify the events that can cause disruptions to business processes, along with the probability and impact of such disruptions and the consequences for information security.

6.28.2. Specific Conditions

6.28.2.1. Business continuity plan

The Information Security Manager shall develop, implement and maintain a contingency plan related to information security for the maintenance or recovery of operations and to ensure the availability of information in the necessary time after the occurrence of interruptions or failures of the critical processes of the business.

6.28.2.2. Plan Structure

The continuity plan shall specify the escalation plans and the conditions for their activation. The plan shall also identify responsibilities for carrying out each activity. Change management procedures and programs shall provide the necessary information so that the plan is always up to date.

6.28.2.3. Plan Tests

Plans and procedures shall be tested annually and the results recorded for future analysis. The purpose of such tests is to ensure that the plan works and that everyone involved has the complete skill and tooling to successfully implement it. The Information Security Manager shall critically analyze the test results and make the necessary changes. And he/she shall also prepare the incident scenarios considered in the business continuity tests;

6.28.2.4. Review

The continuity plan shall be reviewed annually after the test or if the environment changes. All tests performed during that period shall be documented and kept for future verification.

6.29. Information Security Incidents

Promoting an environment where everyone is committed to information security in the company is extremely important and requires a continuous process of awareness. Everyone is responsible for reporting possible violations of the Information Security Guidelines through the channels provided by the Information Security Management. The Management of Information Security Incidents is supported by the Executive Board of **CPFL Group**. The purpose of this document is to establish the systematics of the Process of Management of Information Security Incidents in **CPFL Group**.

6.29.1. General Conditions

6.29.1.1. Information Security Incidents

Events that may jeopardize the confidentiality, availability, integrity and/or authenticity of the Organization's information (which may involve business data, corporate or personal data), which may pose a risk to the assets of **CPFL Group**.
or even any non-compliance with the policies, procedures and/or guidelines of the Information Security Department.
Some examples of information security incidents are given below;
(i) loss or theft of Company equipment (corporate cell phone or notebook);
(ii) leakage of personal data of individuals reported by a data subject in the service channel made available to data subjects;

Information security/personal data incidents shall be formally reported to the Information Security Department through the communication channels made available by said Department.

Incidents shall be investigated and recorded, generating a conclusive report. Upon completion of the exposure of personal data of individuals, **CPFL Group**'s Data Protection Officer shall be called upon to make the relevant risk analysis under the terms of the General Data Protection Law (Federal Law No. 13853/2019)

In cases of incidents involving Alesta, communication with BACEN will be required to share information. For such action, the information security department shall be called to verify the information that will be shared by Alesta's compliance department. Sharing shall also include incident information received from companies providing services to third parties.

Information on incidents shall be consolidated, submitted and discussed periodically at the meetings of the Information Security Committee.

CPFL Group shall maintain an updated Incident Response Plan containing roles, responsibilities, process phases and other relevant topics for the process to be registered and auditable.

Information security occurrences shall be recorded with their artifacts and stored in a protected repository.

All security incidents shall be reported to the parties involved in a timely manner, where applicable.
The record of an information security event shall be available to be accessed, when necessary and as previously authorized by the Information Security, by employees, third parties and interested external entities, and everyone shall be instructed on the responsibility to notify and record any information weaknesses and security failures.

The highest impact incidents shall be recorded and the cause and impact thereof shall be analyzed and the incident effects controlled for the activities of **CPFL Group**, including information received from companies providing services to third parties.

6.29.1.2. Preparation

The Preparation stage aims to enable the organization to properly respond to an information security incident, ensuring that systems, networks and applications are sufficiently secure and ready to respond to related incidents, and that the teams involved are properly trained.
At this stage, the following documents shall be provided, but without limitation:

- Organization contact list updated periodically
- Inventory of procedures and tools for incident response
- Procedure for establishing war rooms
- Definition of incident categorization and criticality
- Training
- Scenario and threat simulations for resilience testing, analysis of tools and capacity and response time;

6.29.2. Process Phases

6.29.2.1. Incident Opening

Phase in which the information security incident is identified and notified to the Information Security Department through the channels provided by **CPFL Group** (see section 16.11.4 below)

6.29.2.2. Business Impact

The business impact shall be classified according to the following parameters:

Impact	Description
High	- Financial Impact in an amount above R$ 1,000,000.01; - Stoppage of more than one business process; - Generalized loss of credibility in relation to the personal data handled by **CPFL Group**. - Significant amount of personal and sensitive data compromised; - Privacy incidents that result in media coverage in territories, online or through big news or media outlets with a high probability of public visibility; and/or - Privacy incidents that may result in a violation of the LGPD and that represent a relevant risk or damage to the fundamental rights and guarantees of the personal data subjects.
Medium	- Financial impact between R$ 500,000.01 and R$ 1,000,000.00; - Stoppage of one business process; and/or - Loss of availability in respect of personal data handled by **CPFL Group**.
Low	- Financial impact below or equal to R$ 500,000.00; - Operational delay in one or more business processes; and/or - Temporary loss of availability or in respect of a small amount of personal data handled by **CPFL Group**.

Once the incident has been classified, the necessary actions are carried out and the teams that will deal with the incident are called up.

6.29.2.3. Investigation

After proper registration, the incident shall be sent to the Information Security and will wait in line for analysis and action.

Incidents shall be classified according to the level of impact occurred as High, Medium or Low, according to the impact classification set out in the SGSI Risk Analysis Procedure (Information Security Management System). In the event of exposure of personal data of a natural person, the Data Officer of the Organization is informed about such occurrence to make an assessment of the relevance of the risk and the impacts on the privacy of data subjects according to the LGPD.

6.29.2.4. Corrective and Preventive Actions

Phase in which the root cause of the incident is identified in order to generate an action plan for implementing controls and eliminating the root cause.

6.29.2.5. Closing

Phase in which the information security incident is closed and notified to the parties involved.

6.29.2.6. External Contacts

It is essential that appropriate contacts are maintained with relevant authorities and external security groups in order to keep **CPFL Group** posted on the trends and threats in the environment. Such contact can be through forums, lectures, seminars, etc.

6.29.2.7. Punishment and Disciplinary Process

Depending on the impact of the incident, it is recommended that there is a defined disciplinary process in place reporting appropriate punishments. Punishment of offenders can only be applied if evidence is correctly collected and stored securely. The collection of evidence in cases where there is a need for internal punishment shall have a representative of the Human Resources Department and/or Legal Department (when applicable) and/or Compliance Department (when applicable), and in the event of digital evidence, of representative of the Information Security department, so that the necessary measures are taken in order to preserve the integrity of the evidence.

Depending on the severity of the incident, the Security Manager may also request the presence of an independent external auditor.

Depending on the severity of the incident, the Security Manager may also request the presence of an independent external auditor.

6.29.2.8. Incident Notification Channel

The following channel shall be used for notification of information security incidents:

Channel	Details
Internal Notification by email	seginfo@cpfl.com.br

CPFL Group shall notify the Sector Coordination team designated to deal with cyber incidents of greater impact, which significantly and substantially affect the security of facilities, operation, services to users or data from environments and stations, the results of applied maturity models. Such notification of cyber incident of higher impact will include the analysis of the cause and impact, the cyber risks identified, with the respective form of handling, and shall also include the mitigating actions that shall be noted, in respect of each case, according to Aneel Normative Resolution No. 964.

As soon as **CPFL Group** becomes aware of the incident and its dimension, a cyber incident notification shall be sent. The sending of such notification does not release **CPFL Group** from its liability to comply with the obligations under the laws, rules and regulations.

For further information on prevention, handling and response to cybernetic incidents and on the details of the cybernetic incidents prevention, handling and response teams, see GED 18851 - Information Security Incident Response Plan.

6.30. Vulnerability Management

To ensure adequate levels of protection for **CPFL Group**'s systems and information, as well as to comply with regulations and standards, a set of rules were defined for managing vulnerabilities in the company's assets.

6.30.1. General Conditions

Vulnerability analyzes shall be carried out by contracted tools owned by the **CPFL Group**'s Information Technology area, according to a defined time schedule.

Application servers, infrastructure and servers will be regularly analyzed.

6.30.2. Vulnerability Management Methodology

CPFL Group has adopted the following methodology for managing vulnerabilities in its environment:

6.30.2.1. Identify

Phase where the assets to be analyzed are determined.

6.30.2.2. Collect

Through automated scans, data from the environment is collected for analysis and identification of existing vulnerabilities.

6.30.2.3. Validation

Phase where the validation of the collected data is carried out for identification of possible discrepancies.

6.30.2.4. Classification / Prioritization

Phase where the types of vulnerabilities x environments are assessed, and the existing vulnerabilities need to be prioritized according to the risk they pose.

6.30.2.5. Correction

Phase to determine which correction shall be given priority, where the implementation of compensatory controls and root cause analysis takes place.

6.30.2.6. Evidence

Phase where evidence is collected, which are identified and associated with the environment assessment items.

6.30.2.7. Results

Finally, a report is prepared and the observed data submitted, and recommendation is given on the correction of identified vulnerabilities and instruction on strengthening the environment.

CPFL Group administers a cybersecurity maturity model test every year.

6.31. Physical and Environmental Security

Access to the office, server room or other company location that contains information of CPFL Group, whether personal data of natural persons, corporate data, business data or any other data classified as confidential or for internal use shall be kept in safe place with restricted physical access. Documents or other media containing sensitive information shall be kept in a safe place (safe, closed file) when not in use. Tables shall be cleaned and organized at the end of the day.

6.31.1. Security Perimeter

A security perimeter shall be clearly defined to avoid unauthorized access, greater access restriction, access traceability and damage or interference /to information systems considered critical. Physical barriers and access control systems shall be implemented to ensure physical access only by users authorized by the person in charge. The security perimeter shall include the following characteristics:

- Walls, doors and ceiling with adequate solidity;
- A doorman/gatehouse or reception system to control access;
- Video monitoring and recording, closed circuit TV or equivalent;
- Biometry
- Access controlled by identification badges;
- Authorization of access only to authorized persons;
- The area shall remain locked even when people are working.

The controls and protection resources related to the security perimeter are part of the **CPFL Group**'s safe areas in the following locations:

- CPFL Data Center Headquarters;
- CPFL DR Data Center;
- São Leopoldo Data Center.

The controls and protection features related to the security perimeter follow the guidelines under GED 18744 - Information Classification Standard.

The IT Infrastructure area is responsible for proposing and implementing mechanisms and processes to restrict access and monitor compliance with the rules established in this document in areas considered to be restricted and safe.

6.31.1.1. Identification

For security reasons, all access to the **CPFL Group**'s environment shall be preceded by identification at the door/gate or reception. Access to the **CPFL Group**'s internal premises is only allowed when duly authorized by the employee at the door, gate or reception desk.

Additionally, the date and time of entry and exit of visitors shall be recorded, as well as minimum personal data to identify the individual.

6.31.1.2. Identity Verification

In a restricted circulation area, authorized employees/third parties shall use their badge on a visible place in order to be easily identified and allowed to enter the restricted area. Employees shall be encouraged to question other employees, third parties and/or visitors walking across the restricted and/or critical area if they are not sure whether the other person is authorized to be there.

6.31.1.3. Activity within the Perimeter

All activities within the security perimeter shall be previously authorized and monitored. Additionally, the following controls are required:

- ✓ The secure area shall be kept closed and locked and, if possible, have an auditable access control;
- ✓ Third parties or contractors shall be constantly supervised, preferably accompanied by a responsible person in the company.
- ✓ A monitoring, alarm or video recording system or equivalent equipment shall be installed to track the activities carried out within the security perimeter.

- ✓ The images and access records shall be stored according to the table of temporality of **CPFL Group**.

6.31.2. Security of Offices, Rooms and Facilities

Access to an office room or other premise of **CPFL Group** containing sensitive information shall be physically restricted. Additional authentication controls shall be used to access those areas.

6.31.2.1. Restricted Areas

Additional access and monitoring controls shall be used in locations identified as critical areas, such as:

- ✓ CCTV,
- ✓ Biometry,
- ✓ Access controlled by ID badges,
- ✓ Access authorization;

The locations determined by **CPFL Group** as such are the following:

- ✓ CPFL Data Center Headquarters;
- ✓ CPFL DR Data Center;
- ✓ São Leopoldo Data Center.

6.31.2.2. Public Visitation

Public visits to **CPFL Group** facilities shall be accompanied and previously authorized by the person in charge.

6.31.2.3. Sharing of CPFL Group information

All information and data obtained by the Employee in the performance of his/her duties in **CPFL Group** are considered internal or confidential information (subject to the classification of the information by the Person in Charge of the Asset) of **CPFL Group** and may only be used for the fulfillment of the scope of the company's business exclusively in the performance of his/her duty and only during the effective term of his/her employment contract.

Access to **CPFL Group** information is prohibited when the Employee is on vacation, on leave, retired or in any event of suspension of his/her employment contract.

Taking pictures of information or image, or filming, copying, drawing or selling it, or sharing it with unauthorized third parties is prohibited, as well as sharing it on private emails, using it for purposes other than the performance of the Employee's duties, or performing or not performing any act that could facilitate the use thereof or leave it exposed.

6.31.3. Delivery and Loading Area

Cargo or equipment shall be received at a proper, controlled and isolated location. Accordingly, access to a delivery and loading area shall be restricted to identified and authorized personnel in a way that does not allow access to other facilities of the company.

The delivered materials shall be previously inspected to detect potential threats before being forwarded to the other premises of the company.

6.31.4. Equipment and Facilities

Servers or other critical equipment shall be protected against major physical threats such as theft, fire, dust, water, temperature, chemical effects, electromagnetic radiation and vandalism.

6.31.5. Power and Temperature Control

Servers and equipment shall be protected against power outages and ventilation/heating interruptions. Such protection is normally provided with the use of “no-break” systems or auxiliary generators.
Likewise, access to maintenance boards shall be restricted and controlled, and they shall be kept locked.

Rooms shall be kept at the temperature recommended by the equipment manufacturers. The temperature of the rooms shall be constantly monitored and alerts shall be triggered in case of a sudden increase in temperature.

6.31.6. Cabling

Electrical, data and communication transmission cables shall comply with the current technical standards and be protected against rupture, whether or not by accident. Electrical cables shall be separated from communication cables and be clearly identified.

6.31.7. Equipment Maintenance

Equipment or systems containing information classified as confidential or of restricted use shall be informed by the person in charge to the manager of the Information Security area so that they can align the security measures to be observed in preventive or corrective maintenance.

When maintenance is performed by a supplier, in the event that it has access to data classified as confidential or for internal use, it shall sign a confidentiality agreement/clause with **CPFL Group**. If it may have access to the personal data of an identified or identifiable natural person, access will only be allowed if it has signed the organization's data protection clauses.

Additionally, all requirements under the insurance policies shall be met.

The information contained in critical equipment shall be properly deleted before being removed from **CPFL Group** or having access released to third parties.

6.31.8. Asset transport

Equipment, media, information or any other asset owned by **CPFL Group** cannot be removed or shared without written and joint authorization from the Responsible for Assets and the Security Manager and/or Department Manager, considering the adoption of measures to protect the information stored and in transit as follows:

- ✓ The nature of the information, as well as its level of sensitivity and confidentiality to the business;
- ✓ Declaration of the purpose of use containing the impacts of not sharing it, and in the case of external sharing, the identification of the supplier (name and contract number in SAP) and recipient of the information;
- ✓ The amount or impact related to any loss during the transfer;
- ✓ Encryption of data in transit;

- ✓ Anonymization/Pseudonymization of data (when applicable);
- ✓ Dual custody process for media in transit;
- ✓ Whether the sharing of data is recorded in the Data Inventory (in case of individual's personal information);
- ✓ Whether the contract with the supplier has data protection rules and confidentiality clause, and the result of the supplier risk assessment related to the LGPD.

A process is recommended for recording the removal and return of the equipment/media/information at the time of its return, clearly identifying the person who authorized its removal from the company's premises.

- **Transport of Company Property**

Equipment, media, information or any other asset owned by **CPFL Group** cannot be removed from it without formal authorization from the Person in Charge of the Asset and the Security Manager or department manager.
A process is recommended for recording the removal and return of the equipment/media/information at the time of its return, clearly identifying the person who authorized its removal from the company's premises.

6.32. Communications Security

It is important to ensure that information processing facilities are operated correctly and securely. The guidelines and concepts described in this document shall be observed, especially by the Information Technology Department and by users in general.

6.32.1. General Conditions

6.32.1.1. Documentation of Procedures

The Information Technology Executive Board shall document the procedures required by the organization to ensure the effective planning, operation and control of the information security processes under its responsibility.

6.32.1.2. Resource Inventory

The Information Technology Executive Board is responsible for maintaining an inventory of software and hardware owned by **CPFL Group** or third-party equipment/tools used by it, identifying the owners.

6.32.2. Specific conditions

6.32.2.1. Standardization and Approval of Technological Resources

The use of messaging application(s) approved by **CPFL Group**, although available 24 hours a day and seven (7) days a week, shall be limited to the activities and work operations carried out at **CPFL Group** and only during the employee's working hours.

The use of communication tools not approved by **CPFL Group** is prohibited in any situation in which personal data or sensitive personal data from any source (clients, employees, service providers, etc.) are handled.

In order to prevent incidents with personal data through the use of non-approved tools (e.g. WhatsApp, Telegram etc.), we instruct you as follows:

• Share **CPFL Group**'s official means of communication with your contacts, as well as the channels approved by the Information Security Management for sharing confidential documents (including those containing personal data/sensitive personal data).

• If you receive from a third party any document addressed to **CPFL Group** containing personal data, re-sent it through the approved tools of **CPFL Group**, immediately delete it from your files and remain in the safe flow for further processing.

• If you have a corporate cell phone and there is need to share personal data via WhatsApp Business (which will only be admitted if the communication cannot be carried out using tools approved by the Information Security Management), it is mandatory that, as soon as the data is received, you save it in an environment monitored by the Information Security Management and immediately delete it from the cell phone files.

• It is forbidden to take photos and record audios related to CPFL Group information and share them in groups of instant messaging applications.
• Whenever possible, with confidential information (including personal data/sensitive personal data), use two-factor authentication in messaging applications and file any confidential information in an encrypted folder.

6.32.2.2. Change Management

The Information Technology Executive Board shall control changes in the computing environment. Change means a change in hardware, change in operating system, replacement or update of application systems.

At least the following controls shall be established:

- ✓ Identification of proposed changes;
- ✓ Registration of current versions and new versions deployed;
- ✓ Formal evaluation and approval by the Person in Charge;
- ✓ Early communication to affected users;
- ✓ Identification of responsibilities and updating of the Asset Inventory.

6.32.2.3. Segregation of Tasks

The Information Technology Executive Board shall implement the segregation of tasks. Operational and system control tasks should be performed by different users whenever possible.

6.32.2.4. Capacity Planning

The Information Technology Executive Board shall monitor the processing capacity of critical equipment and systems. The purpose of this monitoring is to prevent the system from being overloaded and causing losses and/or even loss of profitability.

6.32.2.5. Service Accounts

In cases where systems require service accounts for any purpose, the Information Technology Executive Board shall implement the following controls:

- ✓ Service accounts shall be inventoried, and the inventory shall include at least:
- ✓ Account name;
- ✓ Objective;
- ✓ Person in Charge;
- ✓ Access to accounts shall be controlled and restricted to professionals from the Information Technology Executive Board who use them;
- ✓ In the case of critical systems, the shared custody of the password shall be evaluated;
- ✓ A procedure shall be established for periodic or on-demand replacement of the password, as in the case of termination of the person responsible for the service account;
- ✓ The creation of service accounts shall be authorized by the Information Technology Manager.

6.32.2.6. Removable Media Control

The Information Technology Executive Board shall adequately protect removable media (CDs, DVDs, Flash Memories, etc.) containing confidential or internal information that are in its possession. Media shall be physically destroyed safely when no longer needed for business use.

6.32.2.7. Information Storage

A storage structure shall be used on the File Servers. Such structure shall include at least a departmental storage structure and segregation of privileges for access to the information contained therein.

6.32.2.8. Backups

The Information Technology Executive Board shall implement a process to make backups of stored and processed data, especially on corporate servers. Information stored locally on workstations is outside the scope of backups.

The process shall include the necessary actions to retrieve information as soon as possible in the event of emergencies.

6.32.2.9. Frequency

The Information Technology Executive Board shall define the backup execution frequency, extension criteria, retention time and recovery tests of the backups performed.

6.32.2.10. Additional needs

If the need of the person in charge of the tool is not met by the official backup procedure, he/she shall ask the Information Technology Executive Board to adapt the backup to his/her needs. Those needs shall be based on the classification of information (degree of secrecy), and on the legal and business requirements of **CPFL Group**.

6.32.2.11. Security of Media in Transit

The Information Technology Executive Board shall define and implement protection controls for media in transit against unauthorized access or improper alteration. The persons authorized to send, transport and receive the media shall be clearly identified. Transport shall occur in a time period appropriate to the recovery time objective for the critical asset.

The following additional precautions should be considered:

- ✓ Backup copies shall be stored in protected locations, according to physical and environmental security standards that ensure the integrity, availability and confidentiality of the data contained in these media.
- ✓ There shall be a centralized and up-to-date control of the inventory of all backups made in **CPFL Group**.
- ✓ Every backup of critical systems shall be made at least in two complete and recent copies, stored in different places with the appropriate access and withdrawal controls.
- ✓ There must be a process for periodically reviewing the backup procedure and backup recovery processes.
- ✓ All recovery and/or restoration of a backup shall be performed in an environment different from the original one, whenever technically possible, avoiding damage to current data.
- ✓ Every backup shall be tested periodically, ensuring data integrity and possible restoration.

6.32.3. Security in IT Resource Documentation

Documentation of Information Technology resources shall be stored in a safe place, and access to it shall be restricted only to people who need the information.

6.32.4. Audit Records

The Information Technology Executive Board is recommended to store the audit records of all systems defined as critical for a certain period.

6.32.5. Clock Synchronization

The Information Technology Executive Board shall ensure the synchronization of date and time in the systems, in accordance with the NTP.

6.32.6. Default Installation

The Information Technology Executive Board shall standardize the initial installation of the systems. A standard software installation set shall be prepared and kept in a safe place. These standard copies should be used for recovery from virus infections, hard drive failures and other equipment problems.

The Information Technology Executive Board shall implement a protection system against malicious programs on all workstations.

6.32.6.1. Management and Control

Every workstation shall have management and control software to monitor activities and assist the user remotely.

The monitoring of the access to the user's workstation through the management software shall be previously informed.

6.32.6.2. Default Installation for Workstation

Removable storage devices such as USB ports (pen drive), CD writer, DVD writer, BlueTooth, among others, shall be disabled before the workstation is released to the user. This item does not apply to keyboards, mouses, monitors and network cards,

Every workstation, when technically feasible, shall have a security seal controlled and inventoried by the Information Technology Executive Board.

6.32.6.3. Default Installation - Notebook

It is recommended that every notebook is protected by a local Firewall system. Firewall settings shall comply with the security criteria established by the Information Technology Executive Board.

Every notebook, when technically feasible, shall have an encryption and authentication system. The encryption and authentication system settings shall
comply with the security criteria established by the Information Technology Executive Board.

6.32.7. Network (IP) addresses

The addressing of equipment connected to the network is dynamic and automatically assigned. The use of fixed addresses shall be requested by the user to the Information Technology Executive Board.

6.32.8. Outsourced Network Services

Third party network services shall be documented and verified from a security point of view. New systems or networks for accessing networks external to **CPFL Group** shall be approved mandatorily by the manager of the Information Technology Executive Board.

6.32.9. Remote Access

The Information Technology Executive Board shall ensure that all remote access to the **CPFL Group**'s systems is made through VPN, Citrix Access Gateway or Citrix Secure Gateway.

6.32.9.1. VPN

Any request for remote access through the VPN (Virtual Private Network) tool shall be previously authorized by the immediate superior, and forwarded to the Information Technology Executive Board for the requested access to be granted.

All equipment that needs to access the **CPFL Group**'s network remotely shall have VPN client software approved by the Information Technology Executive Board.

VPN client software configurations shall comply with the security criteria established by the Information Technology Executive Board.

6.32.9.2. CITRIX

Every request for remote access through the Citrix Access Gateway and Citrix Secure Gateway tool shall be previously authorized by the manager and forwarded to the Information Technology Board for analysis and approval.

All equipment that needs to access the **CPFL Group**'s network remotely shall have Citrix client software approved by the Information Technology Executive Board.

Citrix client software configurations shall meet the security criteria established by the Information Technology Executive Board.

6.32.9.3. Access Profile

The Information Technology Executive Board shall implement controls that prevent the visibility, by users with remote access, of the entire network environment or systems of **CPFL Group**.

6.32.9.4. Remote access for inspections on CPFL Group systems

Remote access for inspections will be granted upon completion of the “Confidentiality Agreement”.

Such agreement shall be renewed annually.

6.32.10. Periodic Maintenance

The resources listed in the inventory of technological assets shall be kept in good working order. The Information Technology Executive Board shall implement a periodic maintenance process according to supplier's guidelines.

6.32.11. Information Transfers

The exchange of information with third parties: sending or receiving files, purchase orders, receipt or other form of transfer of information such as B2B or B2C, shall be previously authorized by Person in Charge of the Information. The Information Technology Executive Board shall verify the implications and define appropriate security standards.

At least the following items shall be verified and defined:

- ✓ Responsibilities in case of error, alteration or loss of information;
- ✓ Technical standards and tools used;
- ✓ Protection procedures, verification of sending, receiving and tracking of messages.

6.32.12. Internet Access Means

The Information Technology Executive Board shall give support to user and set up the browser so that the employees' internet access is only allowed when using the **CPFL Group**'s corporate network proxy.

6.32.13. Means of access to information

The use of removable storage devices such as USB ports (pen drive), CD writer, DVD writer, among others, is not allowed and is disabled.

Such data recording features will not be approved at any time. If need may be for such use, and after justification, a request shall be sent to the Information Security Committee for evaluation.

After the assessment, the Officer of the area shall approve the "Statement of Liability for using removable storage devices" where the risk that the company is exposed to in leaving the device open will be described, and whenever possible, it will contain the necessary guidelines for risk mitigation.

6.33. Remote Access and Laptops

Defining security rules for remote access to the **CPFL Group**'s environment and for the use of portable equipment is extremely important. The rules aim to minimize the risk to which these types of resources are exposed, such as alteration, theft or destruction of stored information.

6.33.1. General Conditions

CPFL Group implements technical measures, including those of information traceability, which seek to ensure the security of critical information using Siem tools, and adopts practices in accordance with Standard 18758 - Management of Logs and Events.

6.33.1.1. Information Protection

CPFL Group information stored on portable equipment shall be protected in proportion to its value and criticality. This means that users have to protect any and all information in their custody, whether they are on company premises or elsewhere.

6.34. Remote Access

All remote access to **CPFL Group** systems shall be through VPN (Virtual Private Network) or CITRIX. This access shall be analyzed and approved by the Information Technology Executive Board.

6.34.1. Specific conditions

6.34.1.1. Training

Users shall be informed of the Information Security requirements at the beginning of their activities at **CPFL Group**.

6.34.1.2. Communication of Loss or Damage

The user shall promptly report the Information Technology Executive Board any damage, robbery, theft or loss of any equipment under their custody. Equally important is to immediately report any suspected breach of security. The user will be held liable if he/she doesn't report such loss or damage.

Additionally, a security incident shall be opened through the communication channels made available by the Information Technology Executive Board.

6.34.2. Information Protection

The Information Technology Executive Board shall implement encryption tools, when technically feasible, in all portable equipment containing **CPFL Group** information.

6.34.3. Backup

The users shall make a backup of the information stored on portable equipment under their responsibility and shall store their information in proper locations. In case of doubt regarding standards or procedures, the Information Technology Executive Board shall be contacted.

6.34.4. Antivirus Programs

When applicable, an antivirus application approved by the Information Technology Executive Board shall be installed on all portable equipment. Such application shall be configured to allow updating the virus definitions whenever the equipment is connected to a public network.

Likewise other workstations of the company, the antivirus system shall be configured to scan files, when feasible, whenever new media are inserted (CD-ROM, DVD-ROM, pen-drives or similar devices).

6.34.5. Other ways of accessing and exchanging Information

Information shall be protected in any form of transmission or storage.

6.34.5.1. Public exhibition

CPFL Group's information classified as Internal Use or Confidential shall not be read, handled or discussed in elevators, restaurants, airports, airplanes, trains or other places of public access.

6.34.5.2. Message System

Users shall not leave messages or confidential information or information for internal use by the **CPFL Group** on devices such as answering machines, SMS and messaging applications (e.g. WhatsApp, Telegram...).

6.34.5.3. Physical Access Protection

Portable equipment, when not in use, shall be physically protected from unauthorized access. Thus, when moving away from the equipment, users shall use physical access protection features against theft of anti-theft protection cables, when possible, or store the equipment in lockers, especially when they are outside the company's premises. Care shall be taken in places like empty meeting rooms, hotel rooms and training centers.

6.34.5.4. Transport of Portable Equipment

Portable equipment such as notebooks and other portable computers that contain sensitive information cannot be checked in as baggage.

To prevent damage and theft, those computers shall be carried by traveler as hand luggage. When transported in private cars or taxis, said equipment shall be placed in the luggage compartment to prevent theft when the vehicle is stopped in traffic. It is essential in such cases that the equipment is not seen by other people from outside the vehicle.

6.34.6. Equipment Receipt Protocol

Laptops, cell phones, Smartphones or similar equipment owned by the company cannot leave **CPFL Group**'s premises without the holder signing the equipment receipt protocol that shall remain in the possession of the Information Technology Executive Board.

6.35. Email

It is necessary to establish rules and clearly define that email is a work tool provided to the employee for better performance of his/her duties. The use and the information transmitted shall be according to the rules set out in this document.

6.35.1. General Conditions

6.35.1.1. Company Property

The use of electronic communications systems, and all messages generated or transmitted through the aforementioned system, is considered property of **CPFL Group**. Access to the Electronic Mailbox shall be through specific software that shall be configured by the Information Technology Executive Board.

Access to the Electronic Mailbox on the cell phone is restricted to leadership positions and specialists. Access may also be made available to third parties for them to provide their services.

6.35.1.2. Authorized Use

Electronic communications systems shall be used exclusively for activities related to the business of **CPFL Group**. Occasional personal use is permitted so long as:

- ✓ It does not interfere with employee productivity;
- ✓ It is not used with priority over any activity of the Company;
- ✓ It is not prohibited by the Information Security Guidelines.

6.35.2. Specific conditions

6.35.2.1. User Identity

It is not allowed to falsify, obscure, suppress or substitute the identity of a user in the electronic mail system. Username, email address and organizational affiliation shall correspond to reality.

6.35.2.2. Monitored Messages

The equipment is owned by **CPFL Group** and provided to the employee to carry out his work activities and, for this reason, is monitored to support maintenance, security, auditing and other investigations. We advise you not to save documents with personal information and not to use the tools available for any purpose other than the performance of your activity. Users shall use electronic communications bearing in mind that **CPFL Group** reserves the right to examine their content.

6.35.2.3. Incidental disclosure

It may be necessary for technical support team to review the content of an individual user's communications during the course of troubleshooting. The technical support team, however, cannot review the content of a user's communications out of personal curiosity or for any other reason unrelated to user support without specific authorization from the Information Technology Manager.

6.35.2.4. Message Contents

The use of electronic mail to transmit the contents below is not permitted:

- ✓ Obscene terms or derogatory remarks;
- ✓ Files containing viruses, games, pornography, music/videos or the like;
- ✓ Messages for advertising or selling products for private purposes;
- ✓ Chain letters or "spam";
- ✓ Illegal content or activities.

6.35.2.5. Storage

The storage of email messages in network directories or local disks is only allowed when previously authorized by the Information Technology Manager.

6.35.2.6. Message Outside the Company

Users of electronic communications shall use all caution when sending messages. Sending confidential or internal information to people outside **CPFL Group** without the approval of the Person in Charge is not allowed.

The Information Technology infrastructure area is in charge of configuring a pre-defined Standard Signature in the environment according to ATTACHMENT I.

6.35.2.7. Space Maintenance

The Information Technology Executive Board shall define the message storage capacity and the type and size of the attachment, according to the duties performed by the employee.

6.35.2.8. Safety Information

When receiving messages of unknown origin or containing dubious attachments, the user shall not open or execute such attachments and forward such message immediately to the Information Technology Executive Board.

6.35.2.9. Use of Private Email Account

The use of third-party electronic mail, such as Gmail, Hotmail, Bol, Yahoo or any other is not allowed.
Specific needs shall be justified in the “statement of liability” for the use of computer resources or exception regime.

6.36. Internet Access

Everyone who has permission to use this feature shall pay attention to the details of this document in order to use such feature in a safe and productive way, and only in the performance of business tasks.

6.36.1. General Conditions

6.36.1.1. Internet Access Software

Internet access shall be through specific software (browser). The said software shall be configured by the Information Technology Executive Board.

6.36.2. Specific conditions

6.36.2.1. Information Reliability

There is no information quality control process available on the Internet. Before using information received via Internet for decision-making purposes, users shall confirm the validity of the information with at least one more source.

6.36.2.2. Virus Scan

All files (databases, software object code, spreadsheets, text documents, etc.) received via Internet shall be verified using the appropriate tools provided by **CPFL Group**. This scan is intended to prevent computers from being infected by viruses or other malicious programs.

6.36.2.3. Identity Forgery

Unless tools such as a digital signature or certificate are used, before users provide information, take out services or carry out any other transaction, the identity of the individuals and organizations contacted shall be confirmed.

6.36.2.4. Disclosure of Internal Information

Disclosure of Confidential and Internal Use information over the Internet is not permitted. Before disclosing information, the user shall make sure that it is classified as public.

6.36.2.5. Internet file sharing via virtual disks

The use of file sharing services on the internet is only allowed with tools approved by the Information Technology Executive Board.

6.36.2.6. Access Passwords

Passwords cannot be recorded in browser programs ("browser"), or similar. Such attitude can allow anyone present at your workstations to have access to the Internet with your identity.

6.36.2.7. User Authentication

Access to **CPFL Group**'s local Internet is only allowed after user authentication.

6.36.2.8. Authorized Use

Instant communication systems shall be used exclusively for activities related to the **CPFL Group**'s business. Occasional personal use is permitted so long as:

- ✓ It does not interfere with employee productivity;
- ✓ It is not used with priority over any activity of the Company;
- ✓ It is not prohibited by the Information Security Guidelines.

6.36.2.9. Monitored Messages

The content and use of electronic communications systems are monitored to support maintenance, security, auditing and other investigation activities. Users shall use electronic communications bearing in mind that **CPFL Group** reserves the right to examine their content.

6.36.2.10. Message Contents

The instant messaging system may not be used to transmit the contents below:

- ✓ Obscene terms or derogatory remarks;
- ✓ Files containing viruses, games, pornography, music/videos or the like;
- ✓ Messages for advertising or selling products for private purposes;
- ✓ Chain letters or "spam";
- ✓ Illegal content or activities.

6.36.2.11. Internet access permissions

Users shall not use the Internet or other internal information systems for personal use in such a way that their productivity or that of other users is impaired.

The permission or prohibition of access to categories of websites on the Internet shall be a high-level decision of the Corporate Security Committee and the Information Technology Executive Board, based on productivity, security and alignment with business purposes.

The request to release websites to meet business needs shall be formalized with the Information Technology Executive Board. Specific needs shall be justified in the “statement of liability” for the use of computer resources or exception regime.

Sites that, in the opinion of the Information Technology Executive Board, put **CPFL Group** Assets at risk will only be released after analysis and approval by the Information Technology Manager.

6.36.2.12. Prohibited Access

Access to websites that display the contents listed below is not allowed:

- ✓ Viruses, games, pornography, music/videos, downloading and uploading of files or other content that is not related to CPFL Group's business purposes and the employee's professional activity;
- ✓ Illegal content or activities.

6.36.2.13. Records

CPFL Group reserves the right to record the User's browsing history, such as websites visited, access time and information searched in support of maintenance, security, auditing and other investigations, in case access to the local Internet of **CPFL Group**.

6.36.2.14. Internet Access in Public Areas

Regardless of the means where the information is stored, that is, transmitted, each Employee shall assume a safe and proactive behavior, preventing its leakage to people or means outside **CPFL Group**.

If access to any public access networks is necessary, ensure that access to any **CPFL Group** information is made through VPN and/or SSL connections.

After using any public access networks, the employee shall disconnect from that network and turn off the WI-FI signal of his/her device.

6.37. Use of Equipment

This document presents the rules for the use of equipment and systems owned by **CPFL Group**. The purpose is to guide employees on how to use the equipment in a productive and safe way in the performance of their tasks.

6.37.1. General Conditions

6.37.1.1. Systems involved

This guideline applies to all equipment and/or information systems owned or managed by **CPFL Group**.

6.37.1.2. Equipment

The physical connection of any equipment to the **CPFL Group**'s data network is not permitted without the prior knowledge of the IT Executive Board.

Any equipment connected to the **CPFL Group**'s data network that is not owned and managed by the Information Technology Executive Board will be removed by the IT technical team without the user's prior authorization, and the equipment owner's manager will be notified of such breach, if identified.

Equipment example: Wireless Router, Hubs, Switches etc.

Any and all IT equipment acquisition shall be reported to the Information Technology Executive Board.

6.37.1.3. Authorized use

The information systems and computers owned by **CPFL Group** are intended for business activities. Occasional personal use is permitted so long as:

- ✓ It does not interfere with employee productivity;
- ✓ It is not used with priority over any business activity;
- ✓ It is not contrary to the other provisions of the Information Security Guidelines.

6.37.1.4. Terms of Commitment (employees and/or officers)

Access to the **CPFL Group**'s Information Technology Resources is only allowed after execution of Commitment Agreements evidencing the employee's commitment to use care with the **CPFL Group**'s information assets.

6.37.2. Specific conditions

6.37.2.1. Identification and authentication

Access to **CPFL Group**'s Information Technology resources is only allowed after identification and authentication in accordance with the Access Control Guidelines.

6.37.2.2. Use of Passwords

Users shall keep secret the access password to the **CPFL Group**'s resources and systems and protect all information accessed.

All users shall choose passwords that are easy to remember, but that are difficult to identify. This means that passwords related to work or personal life, such as a license plate number, spouse's name or date of birth, should not be used.

Password complexity requirements shall be observed in section 8. (Related Documents) of the Information Security Guidelines.

6.37.2.3. Repeated Patterns

Users may not use passwords consisting of a basic sequence of characters that change partially and periodically, based on date or some other predictable factor. For example: passwords with alphabetical sequence “ABCDE” or numerical sequence “12345”, and logical sequences such as "A34JAN" in January, by "A34FEV" in February, etc.

6.37.2.4. Password Storage

Passwords cannot be written in places that are easily accessible to third parties such as: “Mouse Pad”, keyboard, notepads, “post it” or similar items. Besides, passwords shall not be stored in files recorded on local disks.

6.37.2.5. Password Sharing

The use of the password to access the **CPFL Group**'s resources and systems is personal and non-transferable.

The user shall keep passwords confidential. Sharing a password or any other mechanism that allows authentication, exposes the authorized user to responsibility for the actions of another person who may misuse their access.

6.37.2.6. Password change

Users shall change their passwords periodically and not use the last passwords already registered.

6.37.2.7. Software and Hardware Settings

The user is not allowed to change the workstation's software or hardware settings, or to install or remove programs. If there is such a need, the change shall be made by the Information Technology Executive Board, which is responsible for supporting the user.

6.37.2.8. Equipment Transport

User is not allowed to change the physical location of equipment, except portable equipment. Users shall request the Information Technology Executive Board to turn off, pack and transport any equipment considered to be Information Technology Resources.

6.37.3. Monitoring

The use of Information Technology resources is monitored to support maintenance, security, auditing and other investigation activities. Users shall use the resources bearing in mind the fact that **CPFL Group** reserves the right to examine their content.

6.37.4. Virus eradication

Virus eradication is the responsibility of the Information Technology Executive Board. In the event of suspected virus infections, the user shall mandatorily turn off the equipment and inform the Information Technology Executive Board, which shall proceed with the appropriate measures.

6.37.5. Resource sharing

Resources such as disk or other storage device that are used with the computer on a daily basis may not be shared. If users may need to share data with each other in order to perform their duties, they shall use restricted directories on network servers or email.

6.37.6. Information Storage

Information is recommended to be recorded on local disks of desktop equipment when connected to the corporate network, since files stored locally are not backed up. **CPFL Group** information shall be stored in network locations (directories or folders) or databases, where they will be properly protected against undue access. Storing confidential or strategic information on shared storage structures is not allowed.

6.37.7. Removable media

It is not recommended to store sensitive information on removable media such as flash drives, CDs, DVDs or similar.

6.37.8. Modems

The use of modems and dial-up connections in equipment connected to the **CPFL Group**'s corporate network is prohibited.

6.37.9. Equipment Custody

The user who always or most of the time uses the same computer to perform his duties is responsible for the equipment. In case of failure or damage, the fact shall be immediately notified to the Information Technology Executive Board.

6.37.10. Food and Drink

Eating, smoking or drinking using the computers is not permitted. Such equipment is usually sensitive and can be damaged in the event of an accident.

6.37.11. Equipment Protection

The employee shall log out or activate the screen saver whenever he/she leaves his/her workplace.

6.37.12. Printing

The print resource made available for use by employees is intended solely for business purposes. The following standards shall be followed:

- ✓ The user shall verify that all documents sent for printing have been collected;
- ✓ The user shall monitor the printing of **CPFL Group** information.
- ✓ When technically feasible, the use of passwords for printing confidential or strategic documents is mandatory.

6.37.13. FAX or similar

The employee shall ensure the security of confidential information when transmitted by electronic means such as FAX or similar equipment.

6.37.14. Clean Table

The employee shall keep confidential information properly protected against undue access during its daily use. The employee shall, at the end of the work shift, save the information as set out in the Privacy and Information Classification Guidelines.

6.38. Acquisition, Development and Maintenance of Systems

In this document, controls and concepts are objectively described in accordance with good information security practices to ensure that the processes of acquisition, development and implementation of systems are carried out with in order to mitigate the risks related to the use of information, codes of programming and availability of systems owned by **CPFL Group**. When necessary, these Guidelines will be detailed in specific procedures and/or standards. The procedures and controls for vulnerability management, information classification and risk management shall be applied in the development of secure information systems and in the adoption of new technologies used in their activities.

6.38.1. General Conditions

6.38.1.1. Roles and responsibilities

6.38.1.1.1. Technical Leader

The technical leader is responsible for interacting with the Information Technology Executive Board and/or external service agents to ensure that all security settings have been implemented when acquiring, developing or maintaining systems.

When necessary, the Information Technology Executive Board may consult companies specialized in Information Security to assess whether implemented controls are in accordance with the good Information Security practices.

6.38.1.1.2. Project Leader

The project leader is responsible for the critical analysis of software changes, considering quality and Information Security requirements, and, when necessary, the project leader can obtain assistance from the Information Technology Executive Board regarding Information Security requirements.

6.38.1.2. Third party products

In the case of systems acquired externally that are already complete, known as “off-the-shelf software”, the technical leader shall follow the software approval procedure that must meet the applicable Information Security requirements. The Information Technology Executive Board is responsible for the records and related tax documents.

6.38.1.3. Naming standards

When possible, new systems should be developed adopting a standardized nomenclature, whether of tables, fields or other necessary components.

6.38.2. Specific conditions

6.38.2.1. Data validation

The technical leader shall define inbound and outbound verification controls. The technical lead shall specify which part of the processing will deal with the information assets. For such cases, the Information Technology Executive Board shall assess the need for additional controls.

6.38.2.2. Input data

Consistency checking standards shall be defined for input data. Consistency controls typically deal with, among others:

- ✓ Value range verification;
- ✓ Checking for missing data or incomplete values;
- ✓ Undue alterations, in the case of a paper form;
- ✓ Identification of responsibilities and authorization for data entry.

6.38.2.3. Output data

Verification controls shall be implemented to identify processing errors; Controls are recommended to be implemented for, among others:

- ✓ Verification of processing errors, validation testing;
- ✓ Verification and reconciliation if necessary;
- ✓ Assignment of responsibilities according to periodic verification of output data.

6.38.3. Internal processing control

The development methodology shall allow for identification of parts of the system that are deemed critical points in terms of integrity, availability, confidentiality and performance.

6.38.3.1. Audit trails

Critical operations performed by the systems shall have mechanisms for tracking the actions performed.

6.38.4. Authentication and Data Security

6.38.4.1. Access Control

The technical leader shall ensure that the new system has at least the following functionalities:

- ✓ Possibility of integration with the authentication mechanisms in use at **CPFL Group**;
- ✓ Possibility of changing the password by the user;
- ✓ Security in storage of sensitive information in accordance with the security and encryption standards defined by **CPFL Group**;

6.38.4.2. Message Authentication

The technical leader shall include protection and verification controls approved by the Information Technology Executive Board, whenever the system specification includes the exchange of data or confidential messages with another system.

6.38.5. Requirements verification

The technical leader shall define a test and approval plan. The system can only be put into production after successful completion of the testing and approval phases.

6.38.5.1. Segregation of environments

The development, testing and production environments shall be completely different environments. System development and testing on personal equipment or workstations connected to the corporate network are not permitted.

6.38.5.2. Segregation of Functions

The tasks of developing, testing and moving systems to production shall be performed by different teams or at least by different users.

6.38.5.3. Data for systems testing

During the development and testing of the systems, real data from the systems in production cannot be used without authorization of the person in charge of the Asset.

6.38.6. Sources and database access control

The technical leader shall define mechanisms to protect program libraries against unauthorized changes. In the case of production databases, access shall be restricted to the smallest possible number of professionals and periodically checked by the person in charge.
If access by other professionals is proven to be necessary, such access shall be released for a specified period as necessary for the performance of the task, and then withdrawn. Access shall be monitored by the Person in Charge during use.

6.38.7. Software change control

For any software change, a formal request and approval procedure shall be defined by those responsible. The controls and procedures shall contain at least:

- ✓ Registration of change request;
- ✓ Registration of the version in use and the changed version;
- ✓ Installation plan that takes into account downtime and possible productivity losses;
- ✓ Reversal plan that takes into account downtime and possible productivity losses;
- ✓ Registration of tests and approval of the change by those responsible.

6.38.8. Version control

The development methodology shall provide mechanisms for version control of all software developed or customized by **CPFL Group**.

6.38.9. Control against Internal Threats

The development methodology shall provide controls that offer protection against “time bomb”, “trojan horse” or similar threats. Adoption of at least the following controls should be considered:

- ✓ Audit, even if by sampling, of the sources of the systems;
- ✓ Checking system logs for unusual activity;
- ✓ Tight change control in the event of any change in the operating system.

6.38.10. Systems documentation

The systems development methodology shall require the creation and maintenance of written documentation that describes the functionality and components of the system.

At least the following points should be considered:

- ✓ Manuals shall be revised to ensure their didactics and applicability;
- ✓ Documentation shall be updated to reflect changes made to systems;
- ✓ The documentation shall contain information on installation and configuration of the systems at the stations, when applicable.

6.38.11. Training

Training of employees in the administration and use of systems is essential for safety and productivity. Training of administrators and users shall be part of the implementation phase of new systems. Additionally, whenever systems are changed, administrators and users shall be trained in the new features.

6.38.12. Cryptographic Controls

Sensitive bank transfer data is encrypted and it is recommended that sensitive data sent or received over communication networks should be encrypted.

6.39. Protection of Personal Data of Individuals

CPFL Group shall maintain a Data Protection Governance Program to be managed by the Data Protection Department, where the Data Protection Commissioner appointed by **CPFL Group** will be assigned, acting in a corporate manner for all companies with direct governance.

CPFL Group looks at security as a non-negotiable value and, therefore, is committed to data protection and will seek to comply with all legal and regulatory rules applicable to it with the purpose of assuring the personal data subjects that the information is handled in a safe, ethical, responsible and informed manner in respect of its real owner.

CPFL Group's commitments to the protection of personal data are summarized below:

- To respect the privacy and protection of personal data of individuals whose personal data are handled in its business activities;
- To ensure that personal data will be handled in a transparent, ethical, safe and responsible manner;
- To take technical and organizational measures to ensure the handling of data in accordance with the laws and regulations governing the issue;
- To promote the Data Protection culture in companies with direct governance in **CPFL Group**;
- To positively influence **CPFL Group** companies with their own governance to adopt the Group's privacy and data protection parameters;
- To carry out continuous monitoring of the Data Protection Governance Program in order to reduce the risks to the privacy of data subjects;
- To ensure the rights of data subjects with regard to their privacy;
- To keep the personal data inventory of the areas that handle personal data of individuals up to date in the performance of their activities;
- To provide a channel for meeting the rights of data subjects.

The Data Protection Management will guide **CPFL Group** on the adoption of data protection rules for the execution of handling operations, including supporting the classification of the category of data and data subjects under the terms of data protection laws and regulations.

In the fulfillment of the privacy and data protection requirements of compliance with the laws and regulations related to Data Protection, the Data Protection, Information Security and Technology Managements will act together, each one within the scope of their technical competences and according to the duties and tasks assigned to them by **CPFL Group.**

7. CONTROL OF RECORDS

Identification	Storage and Preservation	Protection (access)	Recovery and use	Retention	Disposal
IS Policy	Electronic (GED)	Access restriction	By theme or title	Until the next document update	Substitution

8. ATTACHMENT

ATTACHMENT I – Standard external email message

Esta mensagem (incluindo anexos, se houver) pode conter dados e informações confidenciais, e/ou confidenciais para o destinatário e é protegida pelas leis aplicáveis. Caso tenha recebido esta mensagem erroneamente, por favor notifique o remetente e providencie imediata exclusão da original e de qualquer cópia, sendo estritamente proibida qualquer divulgação, cópia ou distribuição desta mensagem.
---

9. REGISTRATION OF CHANGES

9.1. Employees

Company	Department	Name
CPFL Paulista	EIQS	Rafael Fedozzi
CPFL Paulista	EIS	Mateus Rocha
CPFL Piratininga	IJC	Michel Franco de Carvalho Ribeiro
CPFL Piratininga	IJC	Vanessa Oliveira Batista
CPFL Piratininga	SBE	Cassio Henrique Florido
Renewables	PAP	Denise Ramos de Lima
Renewables	EIS	Everton Duarte

9.2. Changes

Previous Version	Previous Version Date	Changes from the Previous Version
1.0	01/07/2022	Document creation.