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	03/11/2010	Criação do documento.
1.1	30/11/2010	Acerto do Cabeçalho e Rodapé e adicionado o item fragmentadora no capítulo de destruição de informações
1.2	30/06/2011	Atualização do documento
1.3	16/08/2011	Atualização do documento
1.4	30/08/2011	Atualização do documento
1.5	21/03/2012	Atualização do documento (Documentos de referência e Perfis de uso e direitos)
1.6	12/04/2012	Atualização do documento (Inclusão de itens específicos sobre Citrix)
1.7	18/07/2012	Atualização do documento (Documentos de referência e proibição de acesso a e- mail externo)
1.8	28/08/2012	Atualização do documento (Meios de acesso à Informação)
1.9	09/11/2012	Atualização do documento (Comitê de Segurança da Informação/ Segregação de Função)

1.10	27/03/2013	Atualização do documento (Inclusão do termo de confidencialidade para fiscalizações - anexo)
1.11	06/03/2015	Revisão geral do documento
1.12	18/08/2015	Revisão do item 17.14. Controles Criptográficos
1.13	20/08/2015	Revisão do item 12.9.1 VPN e documentos de referência
1.14	20/06/2016	Revisão do item 12.2.1. Padronização e Homologação de Recursos Tecnológicos. (Proibição da instalação e utilização do WhatsApp Web, remoção do item 15.2.8,
1.15	29/12/2021	Revisão geral do documento
1.16	21/03/2022	Revisão geral do documento
1.17	13/04/2022	Revisão geral do documento
1.18	08/06/2022	Revisão geral do documento