 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA	2
5.	RESPONSABILIDADES.....	2
6.	REGRAS BÁSICAS.....	3
7.	CONTROLE DE REGISTROS	6
8.	ANEXOS.....	6
9.	REGISTRO DE ALTERAÇÕES.....	6

1.OBJETIVO

O propósito deste documento é o de definir as regras básicas para o desenvolvimento seguro de software e sistemas.

Este documento é aplicado a todo o desenvolvimento e manutenção de todos os serviços, arquitetura, software e sistemas que fazem parte do Sistema de Gestão de Segurança da Informação (SGSI).

Os usuários deste documento são todos os funcionários que trabalham em desenvolvimento e manutenção no **Grupo CPFL Energia**, internas ou terceirizadas.

2.ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas com participação direta da CPFL Energia e sistemas considerados críticos e para SOX.

2.2. Área


Todas as áreas da CPFL Energia.

3.DEFINIÇÕES

SISTEMAS: Ativos de software como sistemas operacionais, sistemas gerenciadores de banco de dados, sistemas embarcados em roteadores e switches, aplicativos comerciais ou desenvolvidos internamente.

HARDENING: Processo de “fortalecimento” das configurações dos ativos, de uma determinada infraestrutura para diminuir de forma controlada as vulnerabilidades do ambiente e consequentemente ocasionando a mitigação de riscos.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18872	Instrução	1.0	Emerson Cardoso	13/08/2021	1 de 7

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

ESPECIFICAÇÃO FUNCIONAL: Conjunto de definições realizadas pela área de responsável visando o entendimento da necessidade do sistema.

ESPECIFICAÇÃO TÉCNICA: Detalhamento da Especificação Funcional realizada pela área de Tecnologia, visando o desenvolvimento ou aquisição do sistema.

4.DOCUMENTOS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001:2013 – Gestão da Segurança da Informação
- ABNT NBR ISO/IEC 27001:2013 – Controles de Segurança da informação
- ABNT/ISO 27002-2013 - 14.2.1 Política de desenvolvimento seguro

5.RESPONSABILIDADES

Líder Técnico

O líder técnico tem a responsabilidade de interagir com o departamento 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, o departamento 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.

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 do departamento de tecnologia da informação em relação aos requisitos de segurança da informação.

Gestores

Fornecer os recursos necessários para a configuração segura dos sistemas sob sua responsabilidade.

Infraestrutura


Propor mecanismos e processos relacionados à configuração segura dos sistemas. Implementar os controles tecnológicos e processos para manter os sistemas seguros.

Segurança da Informação

Elaborar os procedimentos de configuração segura dos sistemas, de acordo com as melhores práticas do mercado.

Avaliar e aprovar as propostas de controles para reforçar a segurança dos sistemas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18872	Instrução	1.0	Emerson Cardoso	13/08/2021	2 de 7

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

6. REGRAS BÁSICAS

Todas as aplicações utilizadas no ambiente do **Grupo CPFL Energia** precisam receber suporte do fornecedor ou da equipe de desenvolvimento para correção de possíveis falhas.

Desenvolvimento

Todas as aplicações desenvolvidas pelo **Grupo CPFL Energia**, precisam seguir um processo de desenvolvimento seguro, com requisitos de segurança especificados desde o início do projeto e revisões de segurança ao longo de todo o processo de desenvolvimento.

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 do Departamento de Tecnologia da Informação.

Padrões de Nomenclatura

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

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 informações sensíveis. Para estes casos, o Departamento de Tecnologia da Informação deve avaliar a necessidade de controles adicionais.

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

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;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18872	Instrução	1.0	Emerson Cardoso	13/08/2021	3 de 7

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

- Atribuição de responsabilidades de acordo com verificação periódica dos dados de saída.

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.

Trilhas de Auditoria

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

Autenticação e Segurança dos Dados

O controle de acesso é responsabilidade do Líder Técnico, ele tem que 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 Energia**;
- 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 Energia**.

É responsabilidade do líder técnico incluir controles de proteção e verificação aprovados pelo Departamento de tecnologia sempre que a especificação do sistema incluir a troca de dados ou mensagens sigilosas com outro sistema.

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.

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

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

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18872	Instrução	1.0	Emerson Cardoso	13/08/2021	4 de 7

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

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.

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.

Controle de versão

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

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.


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.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18872	Instrução	1.0	Emerson Cardoso	13/08/2021	5 de 7

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

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.

Avaliação de risco para o processo de desenvolvimento

Além da avaliação de risco executada de acordo com a Metodologia de avaliação de riscos e tratamento de riscos, o Líder Técnico precisa periodicamente executar a avaliação do seguinte:

- Os riscos relativos ao acesso não autorizado ao ambiente de desenvolvimento.
- Os riscos relativos às mudanças não autorizadas ao ambiente de desenvolvimento.
- As vulnerabilidades técnicas dos sistemas de TI usados na empresa.
- Os riscos que uma nova tecnologia pode trazer se for usada na empresa.

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.

7.CONTROLE DE REGISTROS

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

8.ANEXOS


Não se aplica

9.REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
NAVA	Segurança da Informação	Mateus Rocha

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18872	Instrução	1.0	Emerson Cardoso	13/08/2021	6 de 7

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento para o Desenvolvimento Seguro

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
-	-	Criação do documento