 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

## Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO .....	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA.....	3
5.	RESPONSABILIDADES .....	3
6.	REGRAS BÁSICAS .....	3
7.	CONTROLE DE REGISTROS.....	10
8.	ANEXOS.....	10
9.	REGISTRO DE ALTERAÇÕES.....	11

### 1. OBJETIVO

Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte do **Grupo CPFL Energia**.

### 2. ÂMBITO DE APLICAÇÃO

#### 2.1. Empresa

Todas as empresas com participação direta do **Grupo CPFL Energia** e sistemas considerados críticos e para SOX.


#### 2.2. Área

Todas as áreas do **Grupo CPFL Energia**.

### 3. DEFINIÇÕES

- **ACESSO:** É a capacidade de se realizar uma operação sobre algum recurso computacional;
- **AUTORIZAÇÃO:** Trata-se do que o usuário pode utilizar;
- **LAN:** Local Area Network ou mais conhecida como rede local é o nome que se dá a uma rede de caráter local, e cobrem uma área geográfica pequena, costumeiramente um escritório ou uma empresa, e interligam um número mediano de entidades. São de costume redes de domínio privado;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	1 de 11


 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

- **MAN:** Metropolitan Area Network ou mais conhecida como rede metropolitana é utilizada numa área geográfica maior que a da LAN. Usada tipicamente em um campus ou uma cidade, podem ser redes de domínio público ou privado;
- **WAN:** Wide Area Network ou mais conhecida como rede de longa distância integra equipamentos em diversos locais geograficamente, abrangendo países e continentes como a Internet. As WAN normalmente são de caráter público, geridas por um operador de telecomunicações;
- **SEGMENTAÇÃO DE REDE:** A segmentação é uma técnica que se pode quebrar uma rede em porções menores e conectar estas porções com o equipamento de interconexão apropriado, dessa forma é possível aumentar a largura de banda pois reduz-se o número de usuários que usufruem daquela segmentação;
- **REDE CORPORATIVA:** São computadores e outros dispositivos interligados que compartilham informações ou recursos do **Grupo CPFL Energia**;
- **DISPOSITIVO:** Equipamento e/ou acessório utilizado para acessar, transmitir, compartilhar, visualizar, editar, fazendo-se uso do meio eletrônico para tal;
- **INCIDENTE DE SEGURANÇA DA INFORMAÇÃO:** Indicação de eventos, indesejados ou inesperados, que podem ameaçar os pilares da Segurança da Informação;
- **FIREWALL:** Os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade deles.

Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino.

Os firewalls em forma de hardware são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais. A vantagem de usar equipamentos desse tipo é que o hardware é dedicado em vez de compartilhar recursos com outros aplicativos. Dessa forma, o firewall pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	2 de 11

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

#### 4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- Política de Segurança da Informação do **Grupo CPFL Energia**;
- Norma de Classificação da Informação do **Grupo CPFL Energia**;
- Código de Ética e de Conduta Empresarial do **Grupo CPFL Energia**;
- Esta Norma é complementada pela Política, e demais Normas e Procedimentos do **Grupo CPFL Energia**.

#### 5. RESPONSABILIDADES

##### • Usuários do Grupo CPFL Energia

O usuário titular das credenciais de acesso terá total responsabilidade pelo seu uso, além disso é o responsável pela sua senha sendo pessoal e intransferível. É importante que o usuário utilize suas credenciais somente para fins designados e para os quais estiver devidamente autorizado (de acordo com as suas funções e responsabilidades), além disso se faz necessário substituir a senha inicial gerada pelo sistema e alterá-la periodicamente.

Por fim, reportar imediatamente ao superior imediato e/ou ao setor responsável pela segurança da informação os casos de violação das credenciais, acidental ou não e, providenciar sua substituição, notificando imediatamente ao departamento de Segurança da Informação sobre qualquer uso não autorizado de seu e-mail, conta de acesso ou qualquer outra quebra de segurança de seu conhecimento. e não menos importante, ler e praticar as normas descritas neste documento.

##### • Diretoria de Tecnologia da Informação

Propor mecanismos e processos para restringir o acesso e monitorar o cumprimento das regras contidas neste documento, implementando os controles tecnológicos e processos para manter controle e monitoração de toda a rede do **Grupo CPFL Energia**.


##### • Departamento de Segurança da Informação

O departamento de Segurança da Informação é responsável por prover e manter o sistema de guarda, criação e alteração das credenciais dos usuários, bloquear ou desabilitar as credenciais após tentativas de troca de senhas sem sucesso, notificando o usuário, além disso é responsável por reportar as irregularidades/incidentes detectados. Liberar o acesso de acordo com as normas previstas, implementar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a Internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser utilizada para identificar usuários e respectivos acessos efetuados, bem como o material que foi manipulado e instalar sistemas de proteção, prevenção e detecção, para garantir a segurança das informações e dos perímetros de acesso.

#### 6. REGRAS BÁSICAS

As regras desta norma se aplicam a todos os dispositivos de rede do **Grupo CPFL Energia**, estando on-line e offline.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	3 de 11

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

## 6.1 Hardening

Hardening são ajustes finos efetuados no sistema após uma instalação. É o processo de proteger um sistema contra ameaças desconhecidas. Os administradores de sistema devem fortalecer uma instalação contra o que eles acham que poderia ser uma ameaça. Uma instalação padrão de qualquer sistema que tenha a finalidade de servidor, o administrador tem por obrigação de melhorar a segurança ativando controles nativos ou implementando-os, esse processo é conhecido como Hardening.

Em computação, hardening é o processo de customizar um sistema em busca de maior segurança proativo, para que ele se torne o mais resistente possível a ataques de crackers. Isso tipicamente inclui remoção dos usuários que não serão usados e da desativação ou remoção dos serviços e programas desnecessários.

Esta técnica não deve ser implementada somente em servidores que ficam conectados diretamente a Internet, muitas vezes fornecendo serviços como, por exemplo servidores web, mas também em máquinas que provêm serviços internos de rede como servidores de arquivos e de impressão.

Com a blindagem de sistemas é possível aumentar o desempenho do hardware, liberando recursos que estão sendo utilizado por aplicativos desnecessários, implementando configurações específicas em alguns serviços, além de gerar um ambiente mais seguro.


Hardening pode ser utilizado para evitar que usuários mal-intencionados aproveitem da ausência do administrador e implantem scripts maliciosos em servidores infectando toda a rede, bloquear que o usuário administrador faça login diretamente no terminal, efetuar logout por tempo de inatividade, remover pacotes que não são utilizados, remover permissões especiais de binários executáveis, dentre outras técnicas.

A seguir são listadas algumas vantagens de se utilizar técnicas de hardening:

- ✓ Em geral, utilizar técnicas de hardening é mapear ameaças e evitar que ocorram falhas e invasões em um sistema;
- ✓ Evitar que scripts maliciosos sejam executados;
- ✓ Proteger a conta do usuário root/admin de acessos indevidos;
- ✓ Liberar apenas serviços que estejam realmente ativos no sistema;
- ✓ Aplicar controles aos serviços disponíveis na rede;
- ✓ Aplicar limite de acesso aos usuários.

A tarefa de deixar a rede corporativa segura é complexa e requer sempre o planejamento da área de TI com a área de gestão, pois impacta diretamente o trabalho dos profissionais dentro da empresa.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	4 de 11

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes


Pensando nisso o **Grupo CPFL Energia** decidiu criar esse procedimento de hardening para sua rede corporativa e assim proteger os seus principais ativos, este processo consiste em remover todos os acessos desnecessários no firewall, tanto no sentido “outbound” (de dentro para fora), como no sentido “inbound” (de fora para dentro), de forma a diminuir as possibilidades que um usuário mal-intencionado teria para fazer um ataque.

Além do bloqueio dos acessos desnecessários, é necessário atentar também para a circulação de senhas no modo “texto”, ou seja, de um modo que facilite sua captura. A maioria dos protocolos tem uma versão SSL que deve ser utilizada sempre. Sendo assim, se faz necessário ações para proteger a rede no acesso “inbound”, regras que servem para manter os atacantes Mal-intencionados do lado de fora, como boas práticas podemos citar:

Nunca disponibilize um serviço que use autenticação sem que este seja criptografado: SMTP, POP, IMAP devem ser disponibilizados apenas por SSL. O HTTP, dos websites deve ser SSL sempre que houver alguma autenticação envolvida;

- ✓ Não deixe mais portas abertas do que o necessário para a sua operação. Se os seus funcionários não podem acessar o e-mail de casa, não deixe a conexão para os serviços POP, SMTP e IMAP abertos;
- ✓ Restrinja, sempre que possível, a origem dos acessos a um determinado serviço. Supondo que haja apenas um parceiro de negócios que precise acessar o seu servidor web, então tente fechar o acesso para este parceiro. Se este tiver um IP fixo, configure o acesso por IP. Caso contrário, configure outro tipo de autenticação;
- ✓ Mudar as portas-padrão dos serviços é uma boa prática para diminuir o número de ataques externos à sua rede. Mesmo quando configurado em uma porta diferente, é necessário o mesmo cuidado para bloquear os acessos indevidos;
- ✓ Utilize conexões VPN para dar acesso à sua rede, como servidores de disco e impressoras. Evite criar muitos acessos de entrada no seu firewall.
- ✓ Agora é proposto algumas ações em que protegendo a rede no acesso “outbound”, ações estas que servem para evitar que os seus colaboradores abusem da estrutura de rede da empresa, como boas práticas podemos citar:
- ✓ Tudo que não precisa ser permitido deve ser bloqueado. Comece bloqueando tudo e vá liberando especificamente o que é necessário. Basta uma porta aberta sem controle para que programas como o Ultrasurf ou o Tor funcionem e furem o controle de acesso;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	5 de 11

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes


- ✓ Usuários internos também podem atacar a sua rede. Embora menos importante, procure utilizar criptografia nos protocolos que exigem autenticação. Para não ter que pagar um certificado SSL para isso, utilize certificados gerados pelo próprio servidor da empresa (Self-signed certificates);
- ✓ Preste particular atenção nas conexões HTTPS saindo. Certifique-se que o seu firewall é capaz de controlar o nome nos certificados e a sua validade. Em seguida, bloqueie todos os acessos onde o host da conexão é um endereço IP, a não ser que seja um acesso conhecido;
- ✓ Quanto ao acesso à navegação, escolha a forma de controle de acordo com o perfil dos profissionais e o tipo de trabalho feito na empresa: para trabalhos simples que não exigem muita internet, crie uma lista com os sites permitidos; para trabalhos de criação, pesquisa ou desenvolvimento, opte por bloquear o que é nocivo, e não se esqueça de controlar periodicamente o que foi acessado para evitar eventuais abusos;
- ✓ Quando for necessário utilizar programas que não tem portas e endereços IP de acesso fixos, opte por fazer o controle baseado no nome do programa;
- ✓ Para manter o ambiente de rede mais controlado com relação ao firewall e seus acessos inbound e outbound, é recomendado que:
- ✓ Crie regras para permitir os serviços básicos de rede: NTP e DNS;
- ✓ Crie uma regra que permita a saída de todos os IPs dos servidores e computadores que precisam de acesso total;
- ✓ Crie as regras que se aplicam a programas específicos ou usuários específicos permitindo ou proibindo o acesso conforme o caso;
- ✓ Crie uma regra geral para permitir ou proibir o uso de todos os programas não listados. Para isso use o asterisco (\*) no nome do programa e selecione a ação desejada;

## 6.2 Autenticação

Procedimentos básicos de autenticação de usuários envolvem os seguintes requisitos:

- ✓ Deve ser criado um usuário para cada colaborador ativo da rede, desativando contas antigas;
- ✓ Uma única conta padrão de administração não deve ser utilizada por usuários diferentes: o acesso padrão deve ser utilizado somente para backup e emergências;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	6 de 11

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

- ✓ As senhas de acesso devem ser fortes, com políticas de segurança complexas;
- ✓ As senhas não devem ser armazenadas em texto puro: use uma função hash (PBKDF2, Bcrypt, Scrypt e Argon2);
- ✓ Utilização de senhas com verificação em duas etapas ou multi fator;

### 6.3 Autorização

Para a parte de autorização convém:

- ✓ Cada usuário deve ter permissão para acessar o equipamento de acordo com o seu trabalho. A senha de administrador não deve ser fornecida;
- ✓ Classificar o usuário em um grupo de privilégio, funcionalidade que é permitida em vários sistemas, como: apenas visualização de configurações, alteração de determinadas configurações e administrador com acesso pleno.

### 6.4 Auditoria

Como boas práticas de auditoria podemos destacar:

- ✓ Manter o registro de cada usuários com suas respectivas permissões;
- ✓ Registrar as ações dos usuários nos sistemas.
- ✓ Classificar os registros com nível de criticidade: Informativo, Aviso e Crítico;
- ✓ Classificar os registros em tipos: Documentos, Registros (Logs) e Backup de configuração;
- ✓ Os registros devem ter data e hora corretas;


### 6.5 Acesso

O acesso aos equipamentos da rede deve ser feito de forma segura seguindo os seguintes procedimentos básicos:

- ✓ Não utilize protocolos inseguros, como Telnet, FTP, HTTP, MAC-Telnet ou Winbox, desative-os se não estiverem operando. Se esse for o único meio de acesso à máquina, restrinja o alcance para somente ser acessada pela interface de gerência, uma rede separada e protegida;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	7 de 11



 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes


- ✓ Utilize preferencialmente protocolos com suporte a mensagens criptografadas: SSH, HTTPS, SFTP ou Winbox no secure mode, na última versão estável disponível. Para o SSH, utilize a versão 2 com strong crypto;
- ✓ Utilize uma mensagem de login como: "Roteador pertencente a empresa do **Grupo CPFL Energia**, acessos não autorizados serão monitorados, investigados e entregues às autoridades responsáveis";
- ✓ Mude a porta padrão do serviço. Essa medida é eficaz contra um ataque simples que faz varreduras por portas padrão;
- ✓ Armazene os registros sobre as ações realizadas na rede para finalidade de auditoria. Esses registros ajudam a identificar comandos indevidos na rede;
- ✓ Armazene o registro de tentativas de acesso. Essa medida ajuda a identificar ataques de força bruta, de negação de serviço e de tentativa de roubo de informações;
- ✓ Crie políticas de mitigação de ataques com filtros e rotas blackhole;
- ✓ Utilize a hora legal brasileira, sincronizando a rede com o **NTP.br**;
- ✓ Não permita acesso por todas as interfaces dos equipamentos;
- ✓ Escolha uma interface de loopback para os seus serviços e faça essa interface ser parte da sua rede de gerência. Essas interfaces são mais estáveis, não sofrem com variações no link e caso uma interface física fique indisponível, os protocolos de roteamento procuram um novo caminho;
- ✓ Force o logout depois de um tempo de inatividade. Isso evita que alguém use sua máquina em sua ausência e que um atacante monitore o tempo de inatividade para tomar controle da máquina;
- ✓ Force o logout depois de desconectar o cabo. Isso evita que alguém reconecte o cabo e use o seu login;

## 6.6 Ações avançadas

Port Knocking é um método para abrir portas externamente em um firewall, gerando tentativas de conexão em portas fechadas em uma sequência pré-estabelecida. Uma vez que a sequência correta é reconhecida, as regras do firewall são alteradas dinamicamente para permitir que a máquina que enviou as tentativas de conexão seja

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	8 de 11



 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

conectada à porta específica. Nenhuma porta aparecerá aberta aos ataques de scan, diminuindo a superfície de ataques, habilitar essa função trará mais segurança à rede.

## 6.7 Registros

Todos os registros (logs) obtidos da operação e configuração da rede devem seguir as seguintes recomendações:


- ✓ Configure os registros com diferentes níveis de criticidade;
- ✓ Evite gerenciar logs dentro dos roteadores, pois quanto mais funções o roteador tiver que executar, menos processamento será utilizado para rotear pacotes;
- ✓ Envie os logs de maneira segura para uma outra máquina. A segurança é importante, pois algum agente malicioso pode interceptá-los;
- ✓ Guarde os logs de maneira segura, eles são necessários para uma auditoria e podem ajudar em ações na Justiça;
- ✓ Data e horário dos registros devem estar sincronizados com o servidor **NTP.br**;

## 6.8 Sistema

Como requisitos de sistema, é recomendado:

- ✓ Desativar todas as interfaces não utilizadas, ou seja, interfaces que não possuem cabos conectados;
- ✓ Desativar todos os serviços não utilizados, inseguros e que podem ser utilizados para ataques de amplificação, como testadores de banda (quando não estiverem em uso), DNS recursivo e Servidor NTP;
- ✓ Remover ou desativar os pacotes de funções extras não utilizados, como por exemplo pacote wireless do dispositivo;
- ✓ Desabilitar os protocolos de descoberta de vizinhança, como CDP, MNDP e LLDP, que facilitam a descoberta do tipo do seu roteador e inunda a rede com mensagens desnecessárias. Cuidado com o IPv6, já que a descoberta de vizinhança é essencial nessa versão do protocolo IP: sem ela, nada funciona;
- ✓ Manter o sistema sempre atualizado na versão mais recente e estável;
- ✓ Configure os registros com diferentes níveis de criticidade;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	9 de 11

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

- ✓ Aplicar todos os patches de segurança, se não todos altos e críticos principalmente;
- ✓ Procurar testar as atualizações, antes de aplicá-las em produção, em um ambiente controlado;

## 6.9 Configurações

Por fim, para o requisito de configurações é recomendado que:

- ✓ Manter sempre um backup atualizado das configurações atuais;
- ✓ Enviar o backup para uma outra máquina de maneira segura, utilizando e-mail criptografado, SCP ou SFTP;
- ✓ Guardar o backup em local seguro, pois as informações operacionais da empresa estão neste Servidor e hashes de senhas podem ser decifrados;
- ✓ Manter um script de hardening de máquinas da rede, de forma que você saiba as políticas mínimas de segurança que precisam ser aplicadas ao comprar uma nova máquina;
- ✓ Manter o script de hardening atualizado: cada nova política precisa ser agregada ao script;


## 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 aplicável

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	10 de 11

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening em Redes

## 9. REGISTRO DE ALTERAÇÕES

### 9.1. Colaboradores

Empresa	Área	Nome
NAVA	Segurança da Informação	Mateus Rocha

### 9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não Aplicável	Não Aplicável	Documento em versão inicial

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18887	Instrução	1.0	Emerson Cardoso	17/08/2021	11 de 11