	Tipo de Documento: Procedimento
	Área de Aplicação: Segurança da Informação
	Título do Documento: Proteção de Servidor

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	9
8.	ANEXOS.....	9
9.	REGISTRO DE ALTERAÇÕES.....	9

1. OBJETIVO

Garantir a proteção dos servidores em redes e a proteção da infraestrutura do **Grupo CPFL Energia**.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas com participação direta do **Grupo CPFL Energia**

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.

CONTROLE: Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

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 a Segurança da Informação.

N.Documento: 18824	Categoria: Instrução	Versão: 1.0	Aprovado por: Emerson Cardoso	Data Publicação: 25/06/2021	Página: 1 de 9
-----------------------	-------------------------	----------------	----------------------------------	--------------------------------	-------------------

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

REDE CORPORATIVA: São computadores e outros dispositivos interligados que compartilham informações ou recursos do **Grupo CPFL Energia**.

RISCO: Combinação da probabilidade de um evento e suas possíveis consequências.

SERVIDOR: Computador responsável pelo compartilhamento de recursos com os demais computadores a ele conectados.

USUÁRIO: Qualquer pessoa (colaboradores, visitantes, estagiários, empregados, temporários, prestadores de serviços etc.) que possua ou não ligação com o **Grupo CPFL Energia** e que necessite de Credenciais de Acesso para acessar um sistema ou recurso computacional da organização.

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

• Responsabilidades dos usuários

- ✓ O usuário titular das credenciais de acesso terá total responsabilidade pelo seu uso.
- ✓ O usuário é o responsável pela sua senha sendo pessoal e intransferível.
- ✓ Utilizar suas credenciais somente para fins designados e para os quais estiver devidamente autorizado (de acordo com as suas funções e responsabilidades).
- ✓ Substituir a senha inicial gerada pelo sistema e alterá-la periodicamente.
- ✓ 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.
- ✓ Notificar 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.
- ✓ Ler e praticar as normas descritas neste documento.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	2 de 9

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

• Responsabilidade do departamento de Segurança da Informação

- ✓ 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 e o setor responsável pelo Tratamento de Incidentes de Segurança da Informação.
- ✓ 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.
- ✓ Instalar sistemas de proteção, prevenção e detecção, para garantir a segurança das informações e dos perímetros de acesso.

6. REGRAS BÁSICAS

Servidor nada mais é do que um computador potente que centraliza as informações de uma empresa em um único ponto. Ele é responsável por auxiliar o processamento dos demais dispositivos conectados à sua rede.

Ele é composto por programas e componentes de computadores comuns, no entanto mais robustos e capaz de atender coletivamente a todos os requisitos dos usuários. Além disso é mais tolerante a falhas e utiliza hardwares e softwares personalizados. Os servidores possuem um sistema operacional diferente do das outras máquinas dos usuários e seu software possui recursos específicos que possibilitam a execução de suas funções.


Por meio da centralização dos dados, ele fornece maior agilidade e desempenho para os usuários, que conseguem acessar os sistemas corporativos mais facilmente. Como você pôde perceber, o servidor tem um papel fundamental para o bom funcionamento dos processos corporativos e transmissão das informações entre os funcionários. Portanto, garantir sua segurança é crucial para a continuidade dos negócios.

Pensando nesse cenário, em proteger seus servidores, configurar a infraestrutura e garantir que todas as suas aplicações estão funcionando corretamente e de forma segura, onde o grupo não sofra com contratempo e tenha prejuízos com períodos de indisponibilidade, o **Grupo CPFL Energia** considera os seguintes pontos para proteger seus Servidores:

Rotina de backups

Os backups, ou cópias de segurança, ajudam a reforçar o controle de acesso e a disponibilidade dos dados. Afinal, as informações serão copiadas para locais específicos e protegidos, nos quais estarão imunes a interferências de criminosos. Com uma rotina preventiva, é possível se preparar melhor para situações que colocam em risco os servidores.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	3 de 9

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

Firewalls

Os firewalls também são essenciais para o planejamento de segurança. Eles filtram o acesso aos dados e possibilitam um controle mais inteligente de quem pode acessar os sistemas. Desse modo, evita-se o contato com criminosos e suas investidas.

Em termos de proteção do servidor, os firewalls podem ser essenciais para interromper a maioria dos ataques de hackers. Se uma conexão externa não puder acessar um sistema interno, ela não poderá roubar informações. Bloquear tudo por padrão e colocar na lista de permissões apenas as portas necessárias é um bom começo, mas os firewalls também podem criar logs de todas as tentativas de conexão a um sistema interno.

Além disso, muitos firewalls podem detectar o tráfego típico de determinados ataques ou identificar usuários internos ou aplicativos que estão enviando informações para um sistema externo.

VPNs e Redes Privadas

As VPNs cumprem um papel importante. Com elas, é viável ter um acesso seguro a servidores de forma remota. Ou seja, esse recurso permite que funcionários distantes consigam visualizar os dados e logar nos sistemas da empresa de uma forma protegida, como se estivessem em uma rede privada.

Criptografia

A proteção na hora de fazer login nos sistemas é crucial, por isso, reforçam-se as senhas com criptografia, a fim de garantir o máximo de controle e defesa. Esses códigos são praticamente inquebráveis e indecifráveis, e isso representa uma tranquilidade maior para a gestão.

Auditorias

Uma auditoria tem o poder de avaliar os processos e as políticas, sempre em busca de identificar falhas e proporcionar os melhores resultados. É uma forma de analisar o que está sendo feito e como a proteção dos sistemas está ocorrendo.


Assim, é possível chegar a insights que consolidam a decisão, como a escolha por atualização de servidores caso eles estejam obsoletos. Uma visão geral é fornecida para a gestão, o que se converte em proteção.

Atualizações de Segurança

No processo de proteção do servidor, muitos administradores relutam em instalar automaticamente os patches tanto para Windows quanto para Linux, já que as chances de um patch causar problemas no sistema operacional ou em um aplicativo são relativamente altas.

Há várias soluções para evitar a instalação manual de patches, sistemas que gerenciam a aplicação de correções de segurança e até de terceiros como Java, Adobe e outros.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	4 de 9

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

Alguns podem instalar patches em um ambiente de testes (sandbox), permitindo testá-los antes de aplicá-los aos sistemas de produção.

Portas e Protocolos de rede

No nível mais simples, um firewall mapeia UDP (User Datagram Protocol) e TCP (Transmission Control Protocol) de solicitações externas para portas específicas em servidores internos.

Bloquear todas as portas por padrão e, em seguida, habilitar (podendo até alterar o número padrão) somente as necessárias para fazer com que os aplicativos funcionem é uma etapa básica no fortalecimento do servidor. Isso é feito através de firewalls ou roteadores e em aplicativos de segurança.

Configurações de Usuário

No nível mais simples, essa etapa de proteção do servidor refere-se às opções de confirmação básicas, como exigir senhas complexas para todas as contas de usuário e administrativas, histórico de senhas, autenticação de dois fatores ou até biometria.

Existem ferramentas de proteção de servidor para auditar contas de usuário e aplicativos, a fim de garantir que as senhas sejam suficientemente complexas e sejam alteradas conforme necessárias.

Conceder excesso de direitos administrativos a contas de usuários do servidor pode resultar em infecções ou danos causados por falta de conhecimento, sabemos que pode ser realmente trabalhoso fazer com que alguns aplicativos funcionem com direitos limitados, mas é uma das melhores maneiras de bloquear ataques.

Recursos e Funções Administrativas de Usuários


Durante o processo de proteção do servidor, também é interessante criar ou remover funções, e adicionar ou subtrair recursos de segurança em contas de usuário, conforme necessário. Por exemplo, o suporte contratado do sistema interno utilizado pelo **Grupo CPFL Energia**, deve ter acesso administrativo ao servidor, mas apenas ao sistema de banco de dados e ao próprio software, mas não às pastas compartilhadas pelo servidor e o cadastro de usuários do AD (Active Directory).

Configuração NTP (Network Time Protocol)

O Network Time Protocol destina-se a garantir que todos os servidores do **Grupo CPFL Energia** sejam sincronizados com o mesmo padrão de tempo.

Servidores ou estações de trabalho fora de sincronia em apenas alguns minutos podem causar erros de configuração ou introduzir vulnerabilidades (ataques man-in-the-middle e outros spoofing contam com sistemas fora de padrão).

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	5 de 9

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

Monitoramento e Registro de Logs

O registro e o monitoramento de logs são configurados nos servidores do **Grupo CPFL Energia**, pois são um dos melhores amigos de quem administra a segurança. Há ataques que as vezes não são possíveis de serem bloqueados (como variantes de vírus que aparecem diariamente), mas com o registro de log é possível descobrir o problema e impedir que venha a se repetir.

Simplesmente registrar tudo não é prático pois normalmente geram-se centenas de milhares de linhas de texto por dia. A chave para o fortalecimento bem-sucedido dos servidores é registrar apenas os eventos do sistema que são úteis e, em seguida, localizar os eventos certos se houver um problema.

Por exemplo e um servidor de compartilhamento de arquivos, é interessante ativar a auditoria de arquivos, com ela é possível analisar o que ocorreu com determinado arquivo, quem abriu, editou ou deletou.

Restringir e Monitorar Acesso Remoto

O acesso remoto permite que um usuário com as credenciais adequadas se conecte a um servidor a partir de outro equipamento e acesse todo o seu conteúdo. É uma das melhores invenções para agilizar o suporte ou acesso externo, no entanto, também é uma ótima maneira de um usuário não autorizado obter acesso a vários recursos restritos.

O **Grupo CPFL Energia** além do básico de limitar o acesso remoto a funções específicas e limitar o acesso a endereços IP ou blocos de endereços específicos, ou ainda adicionar autenticação baseada em token adicional para garantir que o usuário realmente é autorizado. Além disso, coleta os registros de todos os acessos remotos e o endereço IP de origem para ajudá-lo a descobrir as ações dos usuários, caso ocorra uma violação.

Serviços do Servidor


Assim como na remoção ou limitação de funções e recursos de servidor, os serviços são aplicativos de nível mais baixo que permitem protocolos de rede específicos, acesso a hardware de servidor, funcionalidade de aplicativos etc.

Muitos serviços podem ser desligados ou configurados para serem executados sob demanda, em vez de serem constantemente ativados.

O mais importante é saber quais serviços são necessários para quais aplicativos, a desativação dos serviços corretos pode não apenas ajudar a proteger o servidor, desativando maneiras comuns de atacar o mesmo, como também pode aumentar o desempenho do mesmo liberando o uso CPU, disco ou memória.

Além de fazer todo o controle da parte lógica para garantir a proteção dos servidores, também é feita a parte física e assim proteger os servidores por completo.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	6 de 9

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

E assim para que esses equipamentos sejam acondicionados e protegidos corretamente é preciso que o ambiente tenha algumas especificações, tais como:

Racks

Os racks são móveis desenvolvidos especialmente para acomodar e organizar os servidores de maneira segura, ajudando na circulação de ar, e mantendo a refrigeração dos aparelhos. Eles também garantem que servidores e equipamentos fiquem dispostos de maneira ordenada, facilitando o acesso e manuseio dos equipamentos pelos profissionais de TI.

Sistema de resfriamento

Conservar o ambiente com a temperatura e a umidade correta é fundamental para a preservação dos servidores e demais equipamentos, já que o calor excessivo pode levar ao superaquecimento das máquinas, ocasionando mau funcionamento.

A temperatura de 21°C é a mais indicada para esses locais. Casos em que a empresa esteja instalada em regiões muito úmidas, a instalação de um desumidificador contribui para que as máquinas fiquem secas e livres de fungos.

Fornecimento constante de energia

Para o bom funcionamento dos servidores e a segurança dos dados que estão sendo armazenados, é importante que o fornecimento de energia seja constante. Para isso, é fundamental que o local disponha de nobreaks e geradores, ou ainda que seja abastecido por mais de uma subestação de energia.

A oscilação de abastecimento desse serviço pode fazer com que dados importantes sejam perdidos, sem ter como recuperá-los posteriormente.

Escolha da sala


O lugar para instalação do Data Center deve ter o tamanho adequado para receber todos os equipamentos, complementos, e claro, a equipe de TI, de modo que essa possa se movimentar dentro do ambiente de maneira segura tanto para eles quanto para os equipamentos.

Somado a isso é indicado que o pé direito tenha entre 3,5 e 5,5m de altura para uma melhor circulação de ar.

Cabos protegidos

É importante também manter a proteção e preservação dos cabos que alimentam os servidores. Por eles passam todas as informações e dados da empresa, assim, garantir

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	7 de 9

	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Proteção de Servidor

que esses componentes não estejam vulneráveis dentro e fora da sala do servidor é fundamental para evitar furto de dados ou perda de conexões.

Piso

O assoalho deve ser adaptado para receber os equipamentos. Dessa forma, o piso precisa ser elevado para que todo cabeamento passe sob ele. A indicação também é que o piso seja emborrachado, pois esse material evita energia estática que pode comprometer o funcionamento dos equipamentos.

Instalação elétrica

O lugar deve contar com instalação elétrica potente e que garanta uma tomada para cada equipamento, evitando compartilhamentos que podem gerar sobrecarga de energia.

Sistema anti-incêndio

Assim como demais setores da empresa, a sala do servidor também precisa contar com um sistema de detecção e combate a incêndios apropriado para o ambiente.

Pressão positiva


Para evitar entrada de poeira, fumaça ou partículas que podem comprometer o funcionamento dos equipamentos é importante que a sala do servidor seja mantida sob pressão positiva. Isso faz com que esses fragmentos sejam empurrados para fora da sala, e não sugadas.

Controle de acesso

A sala do servidor deve ser um ambiente frequentado apenas por pessoas autorizadas. Lá está o coração da empresa e tudo que envolve seu funcionamento. Por isso, restringir o acesso é fundamental para manter a segurança que o local exige.

Instalar alarmes, câmeras de segurança, e até abertura de portas via tranca biométrica são medidas indicadas para aumentar o controle de entrada e saída de pessoas.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18824	Instrução	1.0	Emerson Cardoso	25/06/2021	8 de 9

	Tipo de Documento: Procedimento
	Área de Aplicação: Segurança da Informação
	Título do Documento: Proteção de Servidor

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

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Ana Maria Leite Felix Pelepka

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: 18824	Categoria: Instrução	Versão: 1.0	Aprovado por: Emerson Cardoso	Data Publicação: 25/06/2021	Página: 9 de 9
-----------------------	-------------------------	----------------	----------------------------------	--------------------------------	-------------------