COOPANEST·PE

Rua Benfica, 326 - Madalena, Recife - PE, CEP: 50720-001 - Telefone: (81) 2126-2988

POLÍTICA DE SEGURANÇA DE TI

FOLHA DE CONTROLE

Título	Política de Segurança de TI
Nº da versão	2
Status	Aprovado
Autoria	TI/DPO
Aprovação	Conselho de Administração – CONAD
Data da aprovação	30/11/2020

Histórico de versionamento

Versão	Motivo	Data	Autoria
1	Versão inicial	11/09/2020	TI/DPO
1.1	Ajustes na Política de Acesso Remoto e Política de Mesa Limpa	27/02/2021	TI

FICHA TÉCNICA – CONSELHO DE ADMINISTRAÇÃO

Presidente – Dra. Simone Buonora Almeida
Vice-Presidente – Dr. Ruy Leite de Melo Lins Filho
1º Tesoureiro – Dr. Sergio José Gomes de Oliveira
2º Tesoureiro – Dra. Miriam Silva Passos
Secretário Geral – Dr. Gilberto Oliveira Reis Júnior

INTRODUÇÃO

A **Política de Segurança de TI** funciona como um conjunto de ações que asseguram a conservação da confidencialidade, integridade e disponibilidade da informação.

A primeira dessas características, a confidencialidade, tem como objetivo não fornecer a informação a pessoas, entidades ou sistemas que não estejam autorizadas.

A segunda, chamada de integridade, refere-se à preservação dos atributos originais da informação, isto é, impedir que ela seja corrompida. Fazendo assim, que apenas pessoas autorizadas acessem a informação.

Já a terceira, denominada disponibilidade, garante que a informação possa ser utilizada e acessada sempre que necessário por quem é autorizado.

A **Política de Segurança de TI** tem como intuito minimizar os impactos de incidentes de Segurança da Informação, bem como, elevar o nível de maturidade de sua área.

SUMÁRIO

AVISO DE MONITORAMENTO DE ARQUIVOS CONTENDO DADOS PESSOAIS EM ESTAÇÕES DOS FUNCIONÁRIOS

FUNDAMENTOS JURÍDICOS PARA O MONITORAMENTO DE ARQUIVOS COM DADOS PESSOAIS

Ao executar meditas técnicas e organizacionais visando atender à **Lei Nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)**, a Coopanest-PE, adiante designado **"controlador"**, terá o direito de processar e monitorar o uso de arquivos contendo dados pessoais, fornecido à empresa pelo funcionário ou outra parte titular do dado, permitindo que a empresa cumpra as suas obrigações legais e contratuais com qualidade e segurança, ao tomar medidas que gerem confidencialidade, disponibilidade e integridade às informações encontradas na Coopanest-PE, assim como expresso do **Art. 6 da Lei Geral de Proteção de Dados Pessoais.**

> *"**Art. 6º - VII** - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".*

FINALIDADE DO MONITORAMENTO DE ARQUIVOS COM DADOS PESSOAIS

A finalidade do monitoramento de arquivos com dados pessoais é evitar a perda ou o vazamento de dados pessoais no ambiente da Coopanest-PE, com base no **Art. 46 da Lei Nº 13.709/2018:**

> ***"Art. 46.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".*

RETENÇÃO

Os dados pessoais serão armazenados por um período não superior ao necessário, considerando as finalidades das atividades de processamento e as legislações atendidas pela Coopanest-PE.

DIREITOS DOS FUNCIONÁRIOS

O funcionário tem o direito de receber informações da empresa sobre o monitoramento dos arquivos contendo informações pessoais e que serão tratados pela empresa, como também, tem o direito de apresentar uma reclamação à sua gerência direta, ou também podem entrar em contato com o encarregado de proteção de dados em: **dpo@coopanestpe.com.br.**

POLÍTICA DE ACESSO REMOTO

INTRODUÇÃO

A Coopanest-PE opera uma abordagem controlada para acesso remoto (ou teletrabalho) e uso de dispositivos próprios, entendendo que devido à natureza do nosso negócio, trabalhar de fora do escritório e permitir o uso de dispositivos pessoais dentro da cooperativa é uma necessidade. No entanto, também apreciamos o risco adicional representado pelo acesso remoto, trabalhando fora da sede da cooperativa e o uso de dispositivos próprios e, como tal, temos procedimentos documentados e regras que devem ser seguidas.

Para efeitos desta política, o **"acesso remoto"** refere-se a qualquer trabalho que ocorra fora da sede da cooperativa e requer o uso de qualquer ativo de informações da Coopanest-PE. Isso inclui trabalhar em casa, usar notebooks da cooperativa, acessar a rede da cooperativa ou tirar informações pessoais da sede da cooperativa.

Uma vez que as visitas, viagens e possíveis impossibilidades de trabalho na sede da cooperativa são muitas vezes uma necessidade, poder acessar os sistemas de informação da Coopanest-PE é uma parte importante do nosso serviço, porém temos protocolos rígidos de segurança e restrição que se aplicam a todos os funcionários e gerentes.

Uso de Dispositivos Pessoais refere-se a funcionários, médicos ou terceiros (chamados coletivamente de "usuários"), usando seus dispositivos de propriedade pessoal para fins comerciais dentro do edifício da Coopanest-PE. Isso se refere especificamente ao uso de um dispositivo para uso comercial e não apenas ter tal dispositivo na pessoa. As restrições se aplicam a telefones pessoais, notebooks e tablets, que só são permitidos com autorização prévia da Coopanest-PE e de acordo com as medidas de segurança e regras desta política.

Muitas das medidas e controles em vigor para acesso remoto e o uso de dispositivos pessoais se sobrepõem e são cobertos genericamente nesta política, no entanto, quando protocolos específicos são fornecidos para um ou outro, eles são notados como tal. O **Uso de Dispositivos Pessoais** refere-se principalmente ao dispositivo pessoal próprio do usuário que é usado dentro do edifício da cooperativa, mas não externamente. O acesso remoto utiliza dispositivos fornecidos pela cooperativa para teletrabalho ou trabalho em casa. Isso permite que a cooperativa proteja, registre e monitore tais dispositivos.

DECLARAÇÃO DE POLÍTICA

É política da Coopanest-PE permitir acesso remoto e Uso de Dispositivos Pessoais quando houver uma necessidade genuína de negócios, mas apenas com permissão prévia e de acordo com as regras desta política. As medidas de segurança devem ser aplicadas, e todos os funcionários concordam com os termos deste documento ao trabalhar fora do local ou trazer dispositivos pessoais para a cooperativa. Independentemente de quem possui o dispositivo que está sendo usado ou de onde o acesso acontece, a Coopanest-PE permanece como controladora de dados em todas as instâncias e reconhece sua obrigação legal de cumprir as leis de proteção de dados. **Nós colocamos um alto valor nos ativos de informação dentro de nossa responsabilidade e visamos protegê-los em todos os momentos.** Espera-se que todos os usuários sigam as normas desta política e concordem em manter os dados e dispositivos, atualizados e seguros.

PROPÓSITO

Delinear a abordagem, os objetivos e as diretrizes da cooperativa para o acesso remoto e atividades de Uso de Dispositivos Pessoais. Documentar dispositivos aceitáveis, métodos de acesso e razões para o uso de dispositivos pessoais e/ou acesso remoto, bem como restrições a essas funções para garantir uma segurança eficaz para a Coopanest-PE, seus associados e nossos funcionários, além de proteger os dados pessoais que possuem.

ESCOPO

Esta política se aplica a todos os funcionários da cooperativa (ou seja, funcionários permanentes, fixos e temporários, quaisquer representantes ou subcontratados terceirizados, trabalhadores de agências, voluntários, estagiários e agentes envolvidos com a cooperativa em todo Brasil).

A adesão a esta política é obrigatória e o não cumprimento pode levar a ações disciplinares.

A Coopanest-PE autoriza o acesso remoto e o Uso de Dispositivos Pessoais, caso a caso e reserva-se o direito de recusar, impedir ou retirar o acesso aos usuários a qualquer momento.

OBJETIVOS

A Coopanest-PE permite o uso de acesso remoto e Uso de Dispositivos Pessoais para melhor atender nossos associados, parceiros e oferecer mais flexibilidade aos funcionários quando eles precisarem acessar os sistemas da cooperativa fora da nossa sede. Também valorizamos a flexibilidade que o uso de um dispositivo pessoal pode oferecer, especialmente com referência a notebook e smartphones para serviços externos ou provedores de serviços que possam precisar utilizar seus próprios dispositivos ou acessar as redes/conexões sem fio da cooperativa para realizar funções de negócios.

Devido a esses dispositivos e práticas precisarem de segurança adicional - correm o risco de perda de controle em torno de sua finalidade e uso. No entanto, a Coopanest-PE desenvolveu e cumpre esta política para fornecer orientação e requisitos para ambas as funções.

No que diz respeito ao Uso do Dispositivo Pessoal e ao acesso remoto, a cooperativa garante que:

- Possui uma política de acesso remoto e Uso do Dispositivos Pessoais robusta, mantida em conformidade e disseminada;
- Todos os usuários estão cientes desta política e entendem sua responsabilidade e compromisso com suas regras;
- Todos os dispositivos móveis que acessam as redes da cooperativa ou são trazidos para as instalações da cooperativa são registrados;
- A cooperativa se reserva o direito de verificar se todos os dispositivos móveis estão usando firewalls atualizados e eficazes para malware e software antivírus;
- Quando um dispositivo móvel for usado predominantemente para fins da cooperativa, é proibido instalar software não autorizado ou não aprovado pela cooperativa;
- Utilizamos criptografia forte e conexões de acesso seguras para todos os acessos remotos e dispositivos móveis;
- Quando um usuário de um local de acesso remoto ou conexão através de um dispositivo móvel usa credenciais não reconhecidas 3 vezes, seu dispositivo e acesso serão bloqueados até a liberação pelo departamento de TI da cooperativa;
- Todos os dispositivos móveis e conexões de acesso remoto são protegidos com senhas e devem seguir a política de senhas fortes da cooperativa;

- O departamento de TI restringirá o acesso instantaneamente e apagar conexões ativas de um dispositivo móvel em caso de ameaça;
- Qualquer informação ou ativo pertencente a um cliente ou associado, nunca é acessado ou usado através de acesso remoto ou dispositivos pessoais, a menos que a permissão expressa por escrito tenha sido obtida anteriormente;

DIRETRIZES E PROTOCOLOS DO USO DE DISPOSITIVOS PRÓPRIOS

A Coopanest-PE concede a seus funcionários e terceiros o privilégio de usar smartphones pessoais, notebooks e tablets para sua conveniência, mas reserva-se o direito de revogar esse privilégio a qualquer momento ou se os usuários não cumprirem os requisitos e diretrizes desta política.

Proteger as informações e ativos controlados e processados pela cooperativa é primordial para o nosso negócio e promove a confiança com nossos clientes e associados. O controle do uso de dispositivos pessoais nos permite manter uma infraestrutura segura e robusta e protege a integridade da cooperativa.

Todos os usuários devem concordar com os termos abaixo para poder usar e conectar seus dispositivos à rede da Coopanest-PE.

Todos os usuários são obrigados a:

- Considerar a exigência de usar seu dispositivo próprio e só o faça quando houver uma necessidade ou exigência específica da cooperativa;
- Habilitar e manter atualizados todos os recursos de segurança e software no dispositivo;
- Utilizar credenciais fortes para autenticação de login e aderir à nossa Política de Senha para quaisquer alterações;
- Ativar a função de tela de bloqueio sempre que o dispositivo não estiver em uso e certificar-se de que o desbloqueio requer um novo login;
- Manter o dispositivo atualizado com atualizações de sistema operacional e software;
- Usar apenas uma conexão de rede segura da cooperativa para acesso remoto e fazer isso através de um link seguro (VPN) e somente com autorização prévia;
- Ativar e usar serviços de criptografia e proteção antivírus em todos os dispositivos;
- Desligar qualquer câmera e/ou microfones sempre que possível;
- Abster-se de realizar qualquer atividade de negócios externos;
- Os usuários são obrigados a usar seus dispositivos de forma ética em todos os momentos e aderir aos termos de uso aceitáveis da cooperativa;
- Remover todas as informações da cooperativa armazenadas em seu dispositivo uma vez terminadas, incluindo cópias de e-mails, anexos, documentos baixados e arquivos temporários;

PROTOCOLOS DE ACESSO REMOTO

Será concedido aos funcionários e, ocasionalmente, os associados, que necessitem acessar os ativos e/ou redes da cooperativa enquanto estiverem fora da sede. Esse acesso remoto é fortemente regido e controlado para evitar riscos adicionais de segurança e para proteger o dispositivo que está sendo usado, a rede e a infraestrutura da cooperativa e as informações que estão sendo acessadas.

O acesso remoto só está disponível por meio de uma rede segura e com aprovação prévia. Geralmente utiliza dispositivos fornecidos pela Coopanest-PE (em oposição ao dispositivo do próprio usuário). A conexão é via autenticação e é configurada de forma restrita e limitada pelo departamento de TI.

Todos os usuários via acesso remoto são obrigados a:

- Utilizar apenas dispositivos fornecidos pela cooperativa para acesso remoto;
- Obter autorização por escrito da cooperativa para se conectar via acesso remoto;
- Tomar as medidas de segurança adequadas para proteger o dispositivo e as informações que estão sendo acessadas;
- Proteger seu dispositivo de ser acessado, usado ou copiado por indivíduos não autorizados;
- Acessar a rede através da rede autenticada usando conexões seguras;
- O departamento de TI tem responsabilidade geral por qualquer dispositivo externo utilizado pela conexão à rede da cooperativa por acesso remoto.

As pessoas [designadas como departamento de TI] devem:

- Proteger o dispositivo usado para acesso remoto com um *firewall, software antivírus* e *login* seguro por senha;
- Registrar cada dispositivo de acesso remoto e registrar para quem ele foi fornecido;
- Manter o controle do dispositivo e conexão de acesso em todos os momentos e ser capaz de retirar o acesso imediatamente;
- Proteger todos os dispositivos quando não estiverem em uso, através de cabos de segurança, gabinetes bloqueados ou em uma sala restrita de acesso seguro;
- Nunca deixar dispositivos de acesso remoto ou equipamentos sem vigilância;
- Quando um sistema requer um número *PIN* e um *"token de segurança"* de VPN, armazenar ambos separadamente e restringir o acesso a eles;
- Certificar-se de que uma rede privada virtual (VPN) seja usada para todas as conexões de acesso remoto;
- Certificar-se de que todos os dispositivos usados para acesso remoto requerem um nome de usuário e senha;
- Ativar e manter atualizado *software antivírus* eficaz, *malware* e um *firewall*;
- Eliminar dados dos dispositivos de acesso remoto uma vez que não estão mais em uso, seguindo os protocolos da **Política de Retenção de Dados**;

ACESSO FORA DO LOCAL DE TRABALHO

Não é apenas o uso do dispositivo pessoal e acesso remoto que pode representar um risco adicional de segurança para a Coopanest-PE e as informações retidas por nós. Quando os funcionários são autorizados a trabalhar em casa ou fora do local de trabalho (por exemplo, em visitas ou auditorias de prestadores de serviços), isso também pode exigir a retirada de ativos de informações para fora do local de trabalho, como papelada, relatórios, e-mails etc.

Nos casos em que os funcionários precisam levar as informações em papel para fora do local de trabalho, é necessário que estejam em um invólucro fechado durante o transporte, e em um armário trancado e seguro enquanto estiverem em casa. As informações em cópia impressa devem ser mantidas sempre em sigilo pessoal, não devem ser divulgadas a qualquer pessoa sem permissão prévia por escrito.
Se a papelada não for mais necessária, ela deve ser trazida de volta à cooperativa para arquivamento ou destruição. Espera-se que todos os funcionários cumpram essa política, suas regras e diretrizes.

USANDO E PROTEGENDO DISPOSITIVOS DE USO PESSOAL E ACESSO REMOTO

O uso de um dispositivo pessoal ou da Coopanest-PE para se conectar via acesso remoto, representam riscos adicionais de segurança e, como tal, são regidos pelos protocolos e diretrizes abaixo. O conteúdo a seguir refere-se a todas as formas de acesso remoto, trabalho externo e uso de dispositivos externos.

O acesso remoto seguro é sempre alcançado através de VPN configurado pelo departamento de TI e aprovado por um gerente ou diretor. A permissão por escrito para trabalhar fora do local de trabalho ou trazer/usar um dispositivo pessoal para local de trabalho é sempre necessária e é retida para fins de prova e auditoria.

Nos casos em que um dispositivo da cooperativa é usado para acesso remoto, isso é restrito apenas às informações essenciais para a finalidade do trabalho remoto e é configurado ao nível mínimo necessário para executar as atividades autorizadas.

Os usuários com seus próprios dispositivos ou usando uma conexão da Coopanest-PE não têm permissão para acessar, compartilhar, transmitir ou armazenar qualquer material restrito, confidencial ou inadequado.

Os dispositivos devem ser apresentados ao departamento de TI para a configuração adequada e ativação de medidas de segurança antes de serem usados no local ou antes que eles possam acessar a rede. Para evitar acesso não autorizado, os dispositivos devem ser protegidos por senha usando os recursos do dispositivo e uma senha forte é necessária para acessar a rede da cooperativa.

Qualquer dispositivo perdido ou roubado deve ser relatado ao departamento de TI dentro de 2 horas. Documentamos em diretrizes de acesso a telefones celulares para entrar em contato com o departamento de TI mesmo fora do horário de trabalho.

RESPONSABILIDADES

A Coopanest-PE garantirá que todos os funcionários tenham treinamento e suporte para aprender, entender e implementar a Política de Acesso Remoto e procedimentos subsequentes. Desta forma, **cada gestor de departamento é responsável por uma abordagem de cima para baixo, garantindo que toda a sua equipe esteja ciente de suas responsabilidades** provendo o suporte necessário para atender aos requisitos regulatórios solicitados em lei.

POLÍTICA DE USO DE E-MAIL CORPORATIVO

INTRODUÇÃO

Como empresa obrigada pelas leis de Proteção de Dados, bem como que possui responsabilidades legais e contratuais para a segurança da informação, a Coopanest-PE protege todas as formas de dados pessoais pertencentes a pessoas físicas e jurídicas.

Por utilizar e disponibilizar e-mails corporativos para nossos colaboradores no funcionamento de nossas atividades empresariais, mas reconhecendo os riscos à segurança e aos dados pessoais colocados por esse uso. Esta política descreve nosso uso aceitável de e-mail, restrições e regras para o uso de e-mail em toda a Coopanest-PE e serve como um documento de orientação no uso correto e comportamento de funcionários e terceiros ao acessar e usar e-mails.

Esta política deve ser lida em conjunto com nossas outras políticas de segurança da informação e protocolos de proteção de dados e com as medidas para uma abordagem completa para proteger e assegurar informações pessoais.

A POLÍTICA DE USO DE E-MAIL CORPORATIVO

A Coopanest-PE reconhece que o e-mail é uma forma necessária e padrão de comunicação nos negócios e compõe uma parte essencial da comunicação da cooperativa com outros funcionários, terceiros, médicos e nossos clientes.

Como todas as formas de tecnologia usadas pela Coopanest-PE, o e-mail pode representar riscos de segurança ou de negócios se usado ou configurado incorretamente ou inadequadamente. Esta política de e-mail define nossa abordagem e expectativas para o uso seguro de e-mail em toda a cooperativa e fornece diretrizes sobre um bom protocolo de e-mail para aqueles que usam e acessam suas mensagens no dia a dia.

PROPÓSITO

O objetivo desta política é fornecer a declaração de intenção da Empresa sobre como ela configura, segura, usa e monitora o uso de e-mail dentro do negócio. Ela fornece aos funcionários suas obrigações e expectativas ao usar o e-mail e ajuda a reduzir o risco associado ao uso de e-mails corporativos.

Uma parte das informações enviadas e recebidas por e-mail na empresa é constituída de informações pessoais e, como tal, esta política deve ser lida em conjunto com nossas outras políticas de segurança da informação e proteção de dados.

ESCOPO

Esta política se aplica a todos os funcionários da Coopanest-PE, ou seja, funcionários permanentes, fixos e temporários, e a quaisquer representantes de terceiros ou subcontratados, trabalhadores de agências, voluntários, estagiários e agentes envolvidos com a cooperativa, e diz respeito ao processamento de informações pessoais.

A política se aplica dentro das instalações da Coopanest-PE e fora, onde os funcionários estão usando ou acessando e-mails corporativos enquanto trabalham em casa ou viajam. Esta política é aplicável a qualquer dispositivo onde o e-mail é acessado, incluindo smartphones, tablets, outros dispositivos

móveis, notebooks e computadores desktop. A adesão a esta política é obrigatória e o não cumprimento pode levar a ações disciplinares.

USO E DIRETRIZES POR E-MAIL

A Empresa estabeleceu orientações para os funcionários sobre como usar o e-mail para as melhores práticas, uso aceitável e quaisquer ações consideradas inaceitáveis ao usar ou acessar o e-mail da Coopanest-PE.

USO ACEITÁVEL

A Empresa adotou o conjunto abaixo de diretrizes de uso aceitável para os funcionários seguirem ao usar o e-mail da Coopanest-PE:

- O e-mail deve ser usado de acordo com a legislação e regulamentos vigentes;
- Os funcionários devem aderir a esta política todo o tempo que façam uso do e-mail corporativo;
- O e-mail da Coopanest-PE só deve ser acessado fora das instalações comerciais ou do horário comercial, com a autorização explícita de um gerente ou do departamento de TI;
- Os funcionários só devem acessar seu próprio e-mail comercial e não devem compartilhar ou divulgar logins ou senhas;
- Os funcionários devem sinalizar mensagens de e-mail incomuns ao setor de tecnologia da informação imediatamente;
- O e-mail da Coopanest-PE só deve ser usado para uso legítimo de negócios;

USO PROIBIDO

Além do uso aceitável do sistema de e-mail da Coopanest-PE, as ações abaixo e formas de uso são inaceitáveis e devem ser evitadas por todos os funcionários.

O e-mail da Coopanest-PE não deve ser usado:

- Para enviar ou receber conteúdo ou anexo inadequado, incluindo distribuição, divulgação ou armazenamento de imagens, texto ou materiais que possam ser considerados indecentes, racistas, sexistas, abusivos, ofensivos, pornográficos, obscenos ou ilegais;
- Para uso pessoal, para disseminar opiniões ou opiniões pessoais ou para acessar e-mails pessoais (recebimento de e-mails pessoais dentro do e-mail corporativo);
- Para enviar mensagens confidenciais para qualquer pessoa ou local não autorizado;
- Para se inscrever em sites de internet pessoais, inapropriados ou não comerciais;
- Para enviar ou encaminhar "*correntes*" ou conteúdo de mídias sociais;
- Encaminhamento de mensagens confidenciais da empresa para locais externos;
- Enviar, receber ou acessar qualquer informação com direitos autorais de forma que viole seus direitos autorais;
- Enviar material corporativo, de marketing ou publicidade não solicitados;
- De forma a restringir o envio ou recebimento de arquivos por outros funcionários (ou seja, enviar arquivos grandes sem pré-autorização) ou para realizar atividades deliberadas que desperdicem quaisquer recursos em rede;
- De uma forma que poderia introduzir qualquer forma de vírus de computador ou *malware* na rede da Coopanest-PE;

MELHORES PRÁTICAS

Como o e-mail é usado com frequência para se comunicar com outras pessoas, a Coopanest-PE estabeleceu um protocolo de e-mail que deve ser seguida por todos os funcionários ou terceiros que usam o e-mail corporativamente. O uso adequado do sistema de e-mail e da estrutura de mensagens é essencial para a reputação da Coopanest-PE e para as melhores práticas ao entrar em contato com clientes ou outras entidades.

A Coopanest-PE sugere que, ao usar o e-mail corporativo, os funcionários devem:

- Certificar-se de que o campo '*Para*' esteja corretamente preenchido antes de enviar o e-mail;
- Certificar-se ao usar o "*Preenchimento automático de contato*" para que o sistema de e-mail não "*sugira*" de forma errada o nome da pessoa para quem você está enviando o e-mail;
- Não usar '*CCo*' para ocultar destinatários de e-mail como uma "*resposta a todos*" do destinatário pretendido continuará a copiar o '*CCo*' sem saber – em vez disso, envie uma cópia separada do e-mail para outros usuários;
- Não usar o sistema de e-mail para enviar conteúdo pessoal ou de funcionários, discussões ou opiniões como piadas, eventos de trabalho externo etc.;
- Certificar-se sempre de que a linha "*Assunto*" está significativa e apropriada;
- Mantenha o conteúdo de e-mail breve e direto ao ponto – não congestione o sistema de e-mail de outros funcionários com vários e-mails, se uma reunião ou telefonema servirem melhor;
- Usar apenas as opções '*bandeira*' ou '*urgente*' quando a mensagem é urgente ou precisa de uma resposta sensível ao tempo;
- Não digitar todos os '*CAPS*' para passar uma mensagem nas linhas de assunto ou nos termos de assunto, pois em termos de e-mail parece que é uma "*gritaria*" e não é educado;

SEGURANÇA POR E-MAIL

- O departamento de tecnologia da informação é responsável por garantir que a rede e o sistema de e-mail estejam adequadamente protegidos contra vírus e malware. No entanto, funcionários e usuários também podem ajudar a evitar problemas de segurança, cumprindo as responsabilidades abaixo.

Os usuários do sistema de e-mail não devem:

- Enviar ou abrir qualquer anexo que não seja reconhecido, autorizado ou tenha vindo de uma fonte desconhecida;
- Desativar ou alterar qualquer uma das configurações de segurança aplicadas por padrão ao sistema de e-mail e à rede da Coopanest-PE;
- Alterar qualquer uma das configurações de segurança no dispositivo que está sendo usado para acessar o sistema de e-mail;
- Enviar quaisquer dispositivos pessoais que estão sendo usados para acessar o sistema de e-mail da Coopanest-PE ao **Departamento de TI** para instalação e verificação de software de segurança;
- Divulgar seu login de e-mail ou senha ou tentar acessar o sistema de e-mail de outro usuário;
- Deixar os sistemas de e-mail abertos ou desbloqueados ao sair de uma mesa ou da sala;

ARQUIVAMENTO E RETENÇÃO DE E-MAILS

De acordo com o **Lei Geral de Proteção de Dados (LGPD)**, todos os dados pessoais, incluindo os armazenados como mensagem ou em um sistema de e-mail, estão sujeitos aos princípios de minimização de dados e limitação de armazenamento da LGPD, aos quais a Coopanest-PE adere estritamente.

Nossos períodos gerais de retenção e métodos de destruição e arquivamento estão detalhados em nossa **Política de Retenção e Eliminação**, à qual todas as mensagens de e-mail e arquivos estão sujeitas.
Para garantir que a Coopanest-PE esteja preparada para uma conformidade com a nova legislação de proteção de dados, nós:

- Analisamos dessa política de e-mail para garantir que a segurança e a confidencialidade sejam primordiais ao acessar, enviar e receber mensagens contendo informações pessoais;
- Avaliamos nosso banco de dados de mensagens e e-mails de arquivos existentes para todos os dispositivos, documentando quaisquer mensagens ou anexos relacionados a informações pessoais;
- Utilizamos nossa auditoria de informações para identificar a base legal para armazenar ou processar e-mails de informações pessoais e aplicar nossos processos de retenção e destruição a qualquer um que não seja mais necessário ou onde não temos uma obrigação legal de reter a mensagem;
- Criamos parâmetros para filtragem, categorização e destruição de e-mails que não somos obrigados a legalmente reter;

Os e-mails que temos uma obrigação ou base legal para reter são arquivados e se tornam responsabilidade do **Departamento de TI e do DPO** para revisão em períodos de retenção e definição de datas precisas de destruição.

Quando qualquer e-mail contém informações pessoais na forma de um anexo (*ou seja, notas fiscais médicas, cópias de passaportes, certidões de nascimento etc.*), esses anexos são armazenados de acordo com nossos protocolos de informações pessoais, conforme detalhado em nossas **políticas segurança da informação.**

MONITORAMENTO DE E-MAILS

O sistema de e-mail e o *software* são fornecidos aos funcionários e terceiros indicados para uso legítimo dos negócios e, como tal, estarão sujeitos a serem monitorados o tempo todo. O departamento de TI pode acessar e-mails corporativos, incluindo mensagens enviadas, recebidas e arquivadas e tem o direito de remover mensagens ou acesso a e-mails quando julgar apropriado.

Em conformidade com nossas obrigações comerciais legais, quaisquer e-mails enviados ou recebidos através do sistema de e-mail corporativo fazem parte de nossos registros de negócios, e, devem ser retidos de acordo com nosso cronograma de **Períodos de Retenção**.

RESPONSABILIDADES

Todos os usuários de e-mail dentro da Coopanest-PE são responsáveis por aderir a esta política e pelo uso correto e adequado do e-mail, assim como, por garantir a segurança das informações enviadas e recebidas. Qualquer funcionário que viole os padrões ou requisitos estabelecidos estará sujeito a ação disciplinar.

A penalidade disciplinar será proporcional ao nível de uso indevido de e-mail, mas pode variar de uma advertência verbal até a demissão, dependendo dos fatores envolvidos na violação da política. O uso consciente do e-mail de uma maneira que não cumpra com as obrigações legais ou esta política é um assunto sério e a Coopanest-PE monitorará e revisará todo o uso de e-mail para garantir que os procedimentos corretos estejam sendo seguidos e respeitados.

POLÍTICA DE MESA LIMPA

Como empresa obrigada pelas leis de Proteção de Dados, bem como que possui responsabilidades legais e contratuais para a segurança da informação, a Coopanest-PE protege todas as formas de dados pessoais pertencentes a pessoas físicas e jurídicas.
Essa é a política da Coopanest-PE que fala de uma abordagem de mesa limpa, no que diz respeito a materiais e papéis confidenciais. Os funcionários ficam cientes de que nunca devem deixar informações pessoais ou confidenciais em suas mesas, ou em qualquer área que possa ser vista ou acessada por uma pessoa não autorizada.

PROPÓSITO

O objetivo desta política é garantir que os funcionários estejam cientes das razões para operar em um ambiente de mesa limpa e proteger quaisquer informações pessoais mantidas ou processadas pela Coopanest-PE. A cooperativa ocasionalmente tem visitantes externos em sua sede, como fornecedores e auditores, além dos cooperados médicos anestesistas e, portanto, é importante evitar que informações pessoais ou confidenciais permaneçam sem vigilância.

Ter uma mesa limpa proporciona uma visão profissional e ajuda a manter um ambiente seguro para seus funcionários, reduzindo a desordem e prevenindo acidentes.

A Coopanest-PE está comprometida com a proteção de informações pessoais, sejam de médicos anestesistas, fornecedores, funcionários, pacientes e, para tal, utiliza sistemas eletrônicos para leitura e acesso a dados, sempre que possível. Devido à natureza do seu negócio, é necessário que a Coopanest-PE retenha algumas informações confidenciais e uma grande quantidade de informações pessoais relacionadas aos médicos anestesistas, fornecedores, funcionários e pacientes. Suas **políticas de proteção de dados e procedimentos** fornecem controles e medidas exatas para garantir esse tipo de informação.

ESCOPO

Esta política se aplica a todos os cooperados e funcionários da Coopanest-PE, ou seja, *funcionários permanentes, fixos e temporários, e a quaisquer representantes de terceiros ou subcontratados, trabalhadores de agências, voluntários, estagiários e agentes envolvidos com a cooperativa*, e diz respeito ao processamento de informações pessoais. A adesão a esta política é obrigatória e o não cumprimento pode levar a ações disciplinares.

OBJETIVOS

A Coopanest-PE tem o compromisso de garantir o cumprimento das regras, normas e regulamentos estabelecidos por seus órgãos auditores, governamentais e da própria cooperativa. Ter uma Política de Mesa Limpa permite manter a eficiência e um local de trabalho eficaz e garante a proteção das informações pessoais que devem ser mantidas, devido à natureza de seus negócios.

Os objetivos da Cooperativa em relação às mesas limpas são:

- Melhorar a segurança das informações e a proteção de dados pessoais;
- Cumprir os requisitos e princípios da **Lei 13.709/18 (Lei Geral de Proteção de Dados ou LGPD)**;
- Certificar-se de que informações pessoais e/ou confidenciais estão sendo protegidas, quando há um requisito para imprimi-la quando onde foram recebidas em formato de papel;
- Reduzir as informações em papel, tanto quanto possível, quando se tratar de informações pessoais que excedam nossos requisitos e necessidades;
- Demonstrar um local de trabalho eficaz e eficiente para visitantes, médicos anestesistas e auditores;
- Proteger as informações dos funcionários e os seus direitos;
- Evitar acidentes resultantes de desordem e um local de trabalho desordenado;
- Criar um ambiente sem estresse, limpo e arrumado para os funcionários;

MEDIDAS E CONTROLES

Os funcionários são continuamente lembrados de que as informações pessoais não devem ser impressas, a menos que seja necessário. No entanto, devido à natureza dos negócios e serviços prestados pela Coopanest-PE, informações confidenciais em formado de papel são recebidas ocasionalmente. Nesses casos, quando eles são obrigados a ficar em uma mesa por um tempo (*ou seja, para fins de administração ou entrada de dados nos sistemas eletrônicos*), deve-se oferecer formas seguras e bloqueios para proteger o papel armazenado, caso o usuário esteja longe de sua mesa. Os funcionários estão cientes de que as mesas limpas estão em funcionamento o tempo todo e, ao sair do escritório por qualquer período, as informações em papel devem ser protegidas ou destruídas.

No final do dia de trabalho, espera-se que todos os funcionários arrumem sua mesa e arrumem todos os papéis do escritório em gavetas trancadas e armários de arquivo. **O gerente do setor, também fará uma caminhada de escritório para garantir que os dados de papel foram bloqueados ou destruídos antes de sair do escritório.**

Não são apenas informações pessoais relativas a médicos ou funcionários ou pacientes que estão vinculados à abordagem da mesa limpa. Todos os formatos de papel, incluindo os usados para anotar informações, podem ser considerados informações privadas ou pessoais e estão sujeitos às mesmas regras de governança e proteção que é objetivo dessa política.

Tais documentos podem incluir, mas não se limitam a:

- Notas telefônicas;
- E-mails impressos;
- Avisos e atas de reuniões;
- Cartas disciplinares;
- Referências;
- Papelada contábil;
- Guias de planos de saúde e Glosas;

- Informações de Relatórios e Gerenciamento;
- Políticas e Procedimentos;
- Registros e Livros de acesso de Visitantes;

DIRETRIZES

Os funcionários recebem orientações para manter seu espaço de trabalho e escritório limpos, arrumados e livres de papel. Eles entendem suas obrigações de acordo com a lei de proteção de dados e não mantêm informações pessoais por mais tempo do que o necessário. A Coopanest-PE usa **lixeiras e um serviço seguro de descarte** quando as informações de papel não são mais necessárias, e isso é destruído diariamente. O papel que será triturado deve estar guardado em um armário trancado até a destruição.

Os funcionários limpam regularmente suas mesas da desordem desnecessária, como diários antigos, cadernos e documentos possíveis de arquivamento que não são mais necessários, oferecendo um ambiente seguro para informações pessoais em formatos de papel.

RESPONSABILIDADES

A Coopanest-PE garantirá, com o tempo, que todos os funcionários sejam treinados e suportados para aprender, entender e implementar a Política de Mesa Limpa e procedimentos subsequentes ou associados, para garantia da conformidade com a **Lei 13.709/18.** Desta forma, **cada gestor de departamento é responsável por uma abordagem de cima para baixo, garantindo que toda a sua equipe esteja ciente de suas responsabilidades** provendo o suporte necessário para atender aos requisitos regulatórios solicitados em lei.

POLÍTICA DE ANONIMIZAÇÃO

ESCOPO, FINALIDADE E USUÁRIOS

O objetivo deste documento é fornecer orientação para a Coopanest-PE estabelecer e manter a anonimização de dados pessoais.

Os usuários deste documento são responsáveis pela proteção dos dados. O gestor de TI e os representantes dos setores de negócios são responsáveis pelo processamento de dados pessoais.

DEFINIÇÕES

"**Anonimização**" significa utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

ANONIMIZAÇÃO DE DADOS PESSOAIS

O Setor de TI deve decidir se as técnicas de anonimização são apropriadas para atividades específicas de processamento de dados. O gestor de TI é responsável por escolher a tecnologia mais adequada para a implementação dessas técnicas.

Abaixo está uma lista não exaustiva de técnicas de anonimização.

ANONIMIZAÇÃO

A finalidade de anonimização de dados pessoais é tornar impossível identificar um indivíduo ligado a um conjunto de dados anonimizados, mesmo com o auxílio dos dados originais. Assim os dados anonimizados não são considerados dados pessoais. É importante notar que não existe uma norma prescritiva para a anonimização nos quadros jurídicos brasileiros, pelo que a escolha do uso de métodos de anonimização adequados cabe ao gestor de TI com a aprovação do encarregado da proteção de dados.

Os seguintes métodos serão utilizados pela empresa, considerando o grau de risco e o uso pretendido dos dados.

- ***Encriptação* (utilizando uma chave secreta)** – os dados são *encriptados* com a utilização de uma chave secreta. O titular da chave secreta pode facilmente pré-identificar os titulares de dados por *descriptografar* o conjunto de dados.
- ***Transport Layer Security* (TLS)** – é um protocolo de segurança projetado para fornecer segurança nas comunicações sobre uma rede de computadores. Usado na comunicação de dados pessoais para navegação na web, e-mail, mensagens instantâneas e compartilhamento de informações entre a TOTVS e a Coopanest-PE. Os sites podem usar o TLS para proteger todas as comunicações entre seus servidores e navegadores web. Por esse motivo a Coopanest-PE usa o protocolo HTTPS em seu site.
- ***Token*** – o processo de substituição de um elemento de dados confidenciais por um equivalente não-sensível, conhecido como um *token*. O *token* é uma referência (ou seja, identificador) que mapeia de volta para os dados confidenciais por meio de um sistema de *tokenização*. Usado como segundo fator de autenticação (comumente usados em acesso a sites bancários para envio de informação).

VALIDADE E GESTÃO DE DOCUMENTOS

O proprietário deste documento é o gestor de TI, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

FINALIDADE, ESCOPO E USUÁRIOS

O objetivo deste documento é garantir que as informações sejam protegidas a um nível adequado.
Este documento é aplicado a todo processo de negócio realizado pela Coopanest-PE, ou seja, a todos os tipos de informações (incluindo dados pessoais), independentemente de tratar-se de formulário, documentos em papel ou eletrônicos, aplicativos e bancos de dados, conhecimento das pessoas etc.
Os usuários deste documento são todos os funcionários da Coopanest-PE.

INFORMAÇÕES CLASSIFICADAS

PASSOS E RESPONSABILIDADES

As etapas e responsabilidades para o gerenciamento de informações são as seguintes:

	Nome da etapa	Responsabilidade
1	Inserir o ativo de informação no inventário de ativos	**Gestor de TI**
2	Classificação das informações	**Proprietário do documento**
3	Rotulagem das informações	**Proprietário do documento**
4	Manuseio de informações	**Pessoas com direitos de acesso de acordo com esta política**

Se a informação classificada for recebida de fora da organização, o **Gestor do departamento** é responsável por sua classificação de acordo com as regras prescritas nesta política, e esta pessoa torna-se o proprietário de tal ativo de informação.

CLASSIFICAÇÃO DA INFORMAÇÃO

CRITÉRIOS DE CLASSIFICAÇÃO

O nível de confidencialidade é determinado com base nos seguintes critérios:

- valor da informação – com base nos impactos avaliados durante a avaliação de risco
- sensibilidade e criticidade de informação – com base no maior risco calculado para cada item de informação durante a avaliação de risco
- obrigações legais e contratuais – com base no mapeamento de processos realizados com os gestores de cada departamento.

NÍVEIS DE CONFIDENCIALIDADE

Todas as informações devem ser classificadas em níveis de confidencialidade.

Nível de confidencialidade	Rotulagem	Critérios de classificação	Restrição de acesso
Público	Sem Rótulo	Tornar a informação pública não pode prejudicar a organização de qualquer forma	As informações estão disponíveis ao público
Uso interno	USO INTERNO	O acesso não autorizado à informação pode causar pequenos danos e/ou inconvenientes para a organização	Informações estão disponíveis para todos os funcionários e terceiros selecionados
Restrito	Restrito	O acesso não autorizado à informação pode prejudicar consideravelmente o negócio e/ou a reputação da organização	As informações estão disponíveis apenas para um grupo específico de funcionários e terceiros autorizados
Confidencial	Confidencial	O acesso não autorizado à informação pode causar danos catastróficos (irreparáveis) aos negócios e/ou à reputação da organização	As informações estão disponíveis apenas para indivíduos autorizados pela organização

A regra básica consiste em utilizar o nível de confidencialidade mais baixo, assegurando um nível de proteção adequado, a fim de evitar custos de proteção desnecessários.

LISTA DE PESSOAS AUTORIZADAS

As informações classificadas como "*restritas*" e "confidenciais" devem ser acompanhadas por uma lista de pessoas autorizadas em que o proprietário da informação especifica os nomes ou funções de trabalho de pessoas que têm o direito de acessar essas informações.

Essa mesma regra se aplica ao nível de confidencialidade "*uso interno*", no que se refere às pessoas fora da organização que terão acesso a tal informação.

RECLASSIFICAÇÃO

Os proprietários de ativos de informações devem revisar o nível de confidencialidade de seus ativos de informações anualmente e avaliar se o nível de confidencialidade deve ser alterado. Se possível, o nível de confidencialidade deve ser reduzido.

ROTULAGEM DAS INFORMAÇÕES

Os níveis de confidencialidade são rotulados da seguinte forma:

- **Documentos em papel** – o nível de confidencialidade deve ser indicado no canto superior direito de cada página do documento; ele também deve ser indicado na parte dianteira da capa ou envelope carregando um documento, bem como na pasta de arquivamento em que o documento é armazenado;
- **Documentos eletrônicos** – o nível de confidencialidade deve ser indicado no canto superior direito de cada página do documento;
- **Sistemas de informação** – o nível de confidencialidade em aplicações e bases de dados deve ser indicado através da restrição da visão e do acesso do usuário, ao entrar na aplicação ou base de dado, sendo responsabilidade do gestor de cada departamento informar o nível de acesso de cada funcionários ao setor de TI;
- **Correio eletrônico** – o nível de confidencialidade dever ser indicado no assunto, e na primeira linha da mensagem, com todas em letras em caixa alta (com a tecla *Caps Lock* habilitada);
- **Mídia de armazenamento eletrônico** (HD's, cartões de memória etc.) – o nível de confidencialidade deve ser indicado na superfície superior de tal meio;
- **Informações transmitidas por via oral** – o nível de confidencialidade das informações confidenciais ao transmitir em comunicação presencial, por telefone ou por algum outro meio de comunicação, deve ser comunicado antes da própria informação, definindo o seu nível de confidencialidade.

MANUSEIO DE INFORMAÇÕES CLASSIFICADAS

Todas as pessoas que acessam informações classificadas devem seguir as regras listadas na tabela a seguir. O **Conselho de Administração (CONAD)** deve iniciar a ação disciplinar sempre que as regras forem violadas ou se a informação for comunicada a pessoas não autorizadas. Cada incidente relacionado ao manuseio de informações classificadas deve ser relatado de acordo com o procedimento de resposta e notificação de violação de dados.

Os ativos de informação só podem ser retirados do local após a obtenção da autorização de acordo com a política de segurança de TI.

Tipo	Uso interno	Restrito	Confidenciais
Documentos em papel	❖ Apenas as pessoas autorizadas podem ter acesso. ❖ Se enviado fora da organização, o documento deve ser enviado por transporte registrado. ❖ Documentos só podem ser mantidos em salas sem acesso público. ❖ Documentos devem ser frequentemente removidos de impressoras ou máquinas copiadoras.	❖ O documento deve ser armazenado em um gabinete bloqueado. ❖ Os documentos podem ser transferidos dentro e fora da organização apenas em um envelope fechado. ❖ Se enviado para fora da organização, o documento deve ser enviado com um serviço de recebimento de devolução. ❖ Documentos devem ser imediatamente removidos de impressoras ou máquinas copiadoras. ❖ Somente o proprietário do documento pode copiar o documento. ❖ Somente o proprietário do documento pode destruir o documento.	❖ O documento deve ser armazenado em um cofre ou gabinete com chave e acesso restrito. ❖ O documento pode ser transferido dentro e fora da organização apenas por uma pessoa de confiança em um envelope fechado e selado. ❖ Não é permitido o documento ser enviado por fax ou meios similares. ❖ O documento só pode ser copiado se a pessoa autorizada estiver ao lado da impressora.
Documentos eletrônicos	❖ Apenas as pessoas autorizadas podem ter acesso. ❖ Quando os arquivos são trocados através de serviços como FTP, mensagens instantâneas etc., eles devem ser protegidos por senha. ❖ O acesso ao sistema de informação onde o documento é armazenado deve ser protegido por uma senha forte. ❖ A tela na qual o documento é exibido deve ser bloqueado automaticamente após	❖ Somente pessoas com autorização para este documento podem acessar a parte do sistema de informação onde este documento é armazenado. ❖ Quando os arquivos são trocados por meio de serviços como FTP, mensagens instantâneas etc., devem ser por meio de comunicação criptografadas. ❖ Somente o proprietário do documento pode apagar o documento.	❖ O documento deve ser armazenado de forma protegida de preferência criptografada. ❖ O documento pode ser armazenado apenas em servidores que são controlados pela organização. ❖ O documento não deve ser trocado através de serviços como FTP, mensagens instantâneas etc.

	10 minutos de inatividade.		
Sistemas de informação	❖ Apenas as pessoas autorizadas podem ter acesso. ❖ O acesso ao sistema de informação deve ser protegido por uma senha forte. ❖ A tela deve ser bloqueada automaticamente após 10 minutos de inatividade. ❖ O sistema de informação só pode ser localizado em salas com acesso físico controlado.	❖ Os usuários devem sair do sistema de informação se tiverem deixado temporariamente ou permanentemente o local de trabalho. ❖ Os dados devem ser apagados apenas de forma que assegure a eliminação segura.	❖ O acesso ao sistema de informação deve ser controlado através de um processo de autenticação usando a identificação do usuário que está acessando. ❖ O sistema de informação só pode ser instalado em servidores controlados pela organização. ❖ O sistema de informação só pode ser localizado em salas com acesso físico controlado e controle de identidade de pessoas que acessam o local.
Correio eletrônico	❖ Apenas as pessoas autorizadas podem ter acesso. ❖ O remetente deve verificar cuidadosamente o destinatário. ❖ Todas as regras indicadas em "sistemas de informação" devem ser aplicadas.	❖ O e-mail deve ser protegido se enviado fora da organização.	❖ Todos os e-mails devem ser protegidos, avaliando a necessidade do uso de senhas fortes.
Meios de armazenamento eletrônicos	❖ Apenas as pessoas autorizadas têm acesso. ❖ A mídia ou arquivos devem ser protegidos por senha. ❖ Se enviado para fora da organização, o meio deve ser enviado como transporte registado. ❖ O meio só pode ser mantido em salas com acesso físico controlado.	❖ A mídia e arquivos devem ser protegidos. ❖ A mídia deve ser armazenada em um gabinete de forma segura. ❖ Se enviado para fora da organização, o meio deve ser enviado com um serviço de recebimento de devolução.	❖ A mídia deve ser armazenada em um local seguro. ❖ A mídia pode ser transferida dentro e fora da organização apenas por uma pessoa de confiança em um envelope fechado e selado.
Informação transmitida por via oral	❖ Pessoas autorizadas podem ter acesso a informações.	❖ O local deve ser prova de som.	❖ Conversação conduzida através de vídeo conferencia ou meio

	❖ Pessoas não autorizadas não devem estar presentes na sala quando a informação é comunicada.	❖ A conversação não deve ser gravada.	similar dever ter a comunicação criptografada ❖ Nenhuma transcrição da conversa pode ser mantida.

**Os controles são implementados cumulativamente, desta forma os controles para qualquer nível de confidencialidade implicam na implementação de controles definidos para níveis de confidencialidade inferiores, ou seja, um controle de nível superior herdará os controles do nível inferior.*

VALIDADE E GESTÃO DE DOCUMENTOS

O proprietário deste documento é o Gestor de TI, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e adequação deste documento, devem ser considerados os seguintes critérios:

- número de incidentes relacionados com o acesso não autorizado à informação.
- número de ativos de informação classificados com um nível de confidencialidade inadequado.

POLÍTICA DE CONTROLE DE ACESSO E SENHAS

DECLARAÇÃO DE POLÍTICA

Como empresa obrigada pelas leis de Proteção de Dados, bem como que possui responsabilidades legais e contratuais para a segurança da informação, a Coopanest-PE protege todas as formas de dados pessoais pertencentes a pessoas físicas e jurídicas.

Entendemos que é vital proteger os sistemas e informações mantidos e usados por nós, do uso ou acesso não autorizados, e estamos plenamente cientes de como esse acesso pode afetar a segurança, as informações pessoais e os indivíduos.

Os tipos de medidas e controles utilizados pela Coopanest-PE são:

- Os **Controles de Acesso Físico** garantem que a disponibilidade de sistemas e informações seja restrita apenas a pessoas autorizadas, evitando que locais e informações sejam acessíveis a indivíduos não autorizados. Isso inclui medidas de segurança como: **cadeados, alarmes, biometria, sistemas de campainha etc., em portas e janelas**.
- Os **Controles de Acesso Lógico** utilizam ferramentas e protocolos para identificação, autenticação e autorização de nossos sistemas de informação de computador (*incluindo acesso remoto, notebooks e acesso por sistemas tecnológicos).* Os controles de acesso lógico da Empresa aplicam medidas de acesso aos nossos sistemas, programas, processos e informações, e incluem protocolos de senha, métodos de autenticação do usuário, *criptografia* e *firewall*.
- As **Medidas de Acesso Processual** incluem nossas políticas e procedimentos definidos, que são seguidos por todos os funcionários e terceiros, e fornecem as etapas para as rotinas de controle de acesso, segurança da informação, protocolos de senha e medidas de mesa limpa.

PROPÓSITO

O objetivo desta política é garantir que o acesso físico baseado no sistema a qualquer informação, localização e/ou sistema seja controlado, quando aplicável, restrito, usando controles e procedimentos que protejam os sistemas de informação e dados associados. A Coopanest-PE está comprometida com

a segurança das informações e ativos dentro de nossa responsabilidade, e deve aplicar e testar todas as medidas de acesso para garantir sua funcionalidade, eficácia e finalidade.

Sua política de Controle de Acesso e Senha visa restringir o acesso a informações controladas e/ou sistemas, apenas para aqueles funcionários ou terceiros que estejam autorizados ou tenham permissão por escrito de algum gestor da cooperativa. Quando for necessário acesso temporário e/ou parcial a informações ou sistemas, seguimos protocolos rigorosos para permitir apenas o acesso às informações e pela duração exigida pela atividade.

ESCOPO

Esta política se aplica a todos os funcionários da Coopanest-PE (*funcionários permanentes, fixos ou temporários, quaisquer representantes ou subcontratados de terceiros, médicos, funcionários de agências, voluntários, estagiários*). A adesão a esta política é obrigatória e o não cumprimento implica em ações disciplinares.

OBJETIVOS

A Coopanest-PE está comprometida em garantir o cumprimento das regras, normas e regulamentos estabelecidos por seus órgãos reguladores e governantes, e confirma que desenvolveu e implementou os procedimentos, sistemas, controles e medidas adequados para gerenciar e mitigar os riscos.

Para sistemas que contenham informações e dados pessoais restritos, deve-se registrar o acesso autorizado baseado na função exercida individualmente. Os procedimentos de autorização devem ser realizados de forma que os gestores autorizem todo o acesso (*incluindo acesso temporário e de curto prazo*) registrando a solicitação no sistema de chamados.

Como Coopanest-PE, temos plena compreensão das normas de conformidade que somos obrigados a cumprir e confirmamos que temos em vigor ferramentas e controles eficazes e eficientes para o cumprimento dessas obrigações no atual sistema regulatório.

Os objetivos da cooperativa em relação ao *compliance* são:

- Para ter acesso a sistemas e informações específicos, os funcionários seguem um processo formal de solicitação, que é enviado por sistema de chamado ao **Setor de TI**, após aprovação pelo gestor da área demandante.
- Os acessos (*login*) genéricos não são permitidos nos sistemas da cooperativa, no entanto, o uso de contas genéricas em circunstâncias 'controladas' pode ser permitido a critério do gestor de TI para serviços específicos.
- Para garantir que as normas de segurança contratual, regulatória e legislativa relevantes sejam atendidas e cumpridas, as verificações de triagem de funcionários e visitantes, se faz necessário.
- O nível adequado de acesso a sistemas e informações será determinado com base nos requisitos baseados no usuário, nas funções exercidas e pela determinação do gestor do setor pertencente ao usuário.
- Se a autorização para usar sistemas e informações for concedida, credenciais exclusivas de "*login*" e senha serão fornecidas ao funcionário, utilizando os fortes controles de senha detalhados nesta política.
- O acesso para usuários remotos estará sujeito à autorização dos gestores setoriais através do sistema de solicitação e chamados ao **Setor de TI**. Nenhum acesso é concedido sem uma solicitação feita pelo sistema preenchido e autorizado.

PROCEDIMENTOS, CONTROLES E MEDIDAS

É fundamental para nossas operações e prestação de serviços aos clientes, que a Coopanest-PE use computadores, sistemas informatizados, *software*, dispositivos de *hardware* e sistemas de armazenamento de dados. Devido à natureza do nosso negócio, esses sistemas são frequentemente usados para armazenar informações pessoais e confidenciais. Por isso, é essencial proteger tais informações, restringindo o acesso aos sistemas através de uma variedade de controles e medidas de acesso.

Adotamos uma abordagem multi-hierárquica ao proteger sistemas e restringir o acesso, detalhamos nesta política os procedimentos e métodos utilizados em toda a cooperativa. Essas informações são divulgadas a todos os funcionários, que fazem parte do nosso programa de segurança da informação.

CONTROLE DE ACESSO LÓGICO

O acesso aos sistemas dentro da Cooperativa-PE é regido por nossas medidas hierárquicas de controle de acesso lógico. O acesso a qualquer sistema é classificado e as restrições são implementadas no nível do usuário. Os níveis podem ser alterados a critério do **Gestor de TI** com aprovação do **Conselho de Administração**, por meio da conclusão de uma solicitação de alteração de acesso feita em nosso sistema de solicitações.

Considerações para a concessão de acesso são avaliadas com base em:

- A necessidade de acesso de um funcionário ou usuário para completar seu trabalho e/ou tarefa;
- Duração do acesso;
- Nível de acesso;
- Tipos de informações localizados no sistema;
- Medidas de segurança em vigor se o acesso for concedido;
- Capacidade de remover acesso em um momento pré-determinado;
- O acesso é decidido e alocado caso a caso, só podendo ser atribuído ao usuário pelo gestor do setor ou departamento.

SENHAS

As senhas são uma parte fundamental da estratégia de proteção da Coopanest-PE e são usadas em toda a empresa para proteger informações e restringir o acesso a sistemas. Usamos uma abordagem multi-hierárquica que inclui senhas nos níveis de usuário, gerenciamento dos dispositivos, dos sistemas e da rede, para garantir uma abordagem completa e abrangente.

As senhas oferecem um alto nível de proteção aos recursos e dados, são requisitos obrigatórios para todos os funcionários e/ou terceiros que são responsáveis por uma ou mais conta, sistema ou têm acesso a qualquer recurso que exija uma senha.

REVISÃO E ALTERAÇÃO DA SENHA

Somente aqueles autorizados a acessar dispositivos, informações e sistemas específicos são fornecidos com as senhas relevantes, e tais disposições são revisadas semestralmente para garantir que o acesso ainda seja válido e necessário. Os **funcionários nunca poderão compartilhar suas senhas** com outra pessoa da cooperativa, incluindo colegas de trabalho, gerentes ou funcionários de TI. Senhas exclusivas devem ser usadas para todos os funcionários ao acessar sistemas e dispositivos.

Os funcionários são informados que as senhas devem ser consideradas "fortes", pois são necessárias para todos os sistemas e acesso feito pelo usuário, em um protocolo rigoroso de não divulgação das senhas. Quando aplicável ao sistema ou dispositivo que está sendo utilizado, a Coopanest-PE utiliza *software* para impor o uso de senhas fortes. Os **funcionários "não" podem compartilhar ou divulgar qualquer senha.**

Senhas fortes são aplicadas em sistemas e usuários e devem ser:

- Mais de 8 caracteres.
- Inclua letras, números e pelo menos 1 caracteres especiais.
- Não ser facilmente reconhecível (*ou seja, sem nomes, datas de nascimento, lugares etc.*).
- Deve incluir letras maiúsculas e minúsculas.

Todas as senhas são alteradas a cada 3 meses, e os usuários não podem reutilizar a mesma senha dentro de um período de 1 ano. Isso é forçado a usar *software* em todos os sistemas e uma mudança de senha é automaticamente promovida no início de cada ciclo. Esta alteração é aplicada dentro de 5 dias após o lembrete de alteração ser mostrado.

Se uma senha for esquecida, apenas o **Setor de TI** poderá redefinir as senhas por meio da abertura de chamado pelo gestor do departamento demandante. As senhas que foram esquecidas são alteradas por padrão e não podem ser redefinidas para usar a mesma senha. Uma mudança de senha forçada deve ser feita se o usuário suspeitar que a senha foi comprometida.

SENHAS PADRÃO

Ocasionalmente é necessário configurar a senha padrão. Isso geralmente é apenas quando um novo sistema ou usuário está sendo configurado e uma mudança de senha será promovida a partir do primeiro uso do usuário. As senhas padrão são trocadas o mais rápido possível e, quando aplicável, o acesso às informações é restrito até que uma senha forte seja criada.

Quando novos sistemas, dispositivos ou *software* são comprados, as senhas padrão são imediatamente alteradas e redefinidas para usar as variáveis fortes indicadas acima.

PROTEGENDO FUNCIONÁRIOS

A Coopanest-PE está ciente de que vírus, *software* e golpes de *phishing* podem tentar obter senhas em nível de usuário. Embora os *Firewalls* sejam usados para proteger sistemas e softwares, são fornecidos aos funcionários treinamento e orientação sobre *phishing* e são instruídos a não divulgar suas senhas em um ambiente físico ou *on-line*. Isso inclui não divulgar senhas para terceiros, clientes ou representantes que possam ter uma necessidade legítima de acessar um sistema.

Os campos de senha são sempre exibidos em um formato *hash* ou estrela (*ou seja, ### ou ****) de modo que o texto claro não esteja presente quando uma senha é digitada. Isso ajuda a evitar o acesso não autorizado ou a divulgação de senhas por meio de métodos de cópia e cola ou impressão eletrônica.

Escrever ou armazenar senhas em qualquer formato escrito ou digital é proibido para todos os funcionários. A divulgação ou perda não intencional de uma senha que tenha sido escrita em qualquer formato resultará em ações disciplinares.

Quando o *login* falhar, operamos uma abordagem de três tentativas e o sistema ficará indisponível por 15 minutos antes uma nova tentativa de *login* seja feita. Isso protege contra os ataques externos de '*bot*' (robôs) e força bruta.

CRACHÁS DO USUÁRIO

A Coopanest-PE adotou crachás de identificação para todos os funcionários, visitantes e terceiros que estão em nosso prédio de escritórios. Esses crachás são específicos daqueles a quem são atribuídos e os crachás não utilizados, são armazenados em uma área segura e bloqueada.

Os funcionários devem usar seu crachá de identificação o tempo todo enquanto estiverem no prédio, ou enquanto visitam escritórios de terceiros, e não podem compartilhar ou copiar seu crachá.

Os visitantes recebem '***Crachás de Identificação de Visitantes*** ' que declara seu nome, empresa, posição e pessoa responsável na recepção da Coopanest-PE. Os visitantes são acompanhados no local o tempo todo e são obrigados a entrar e sair do prédio, assinar acordos de confidencialidade, e a receber um funcionário da cooperativa que é responsável por eles durante sua visita.

CONTAS PRIVILEGIADAS

A Coopanest-PE entende a extrema importância de garantir restrição ao acesso a contas privilegiadas. Essas contas permitem acesso direto à nossa rede, servidores, *firewall*, roteadores, servidores de banco de dados, sistemas e *software* e, como tal, são tratadas com a máxima segurança e proteção. Funcionários e terceiros nunca têm acesso a contas privilegiadas, a menos que tenham sido atribuídas responsabilidade por uma função direta. Se for o caso, o acesso só é dado ao sistema específico ou infraestrutura necessário para completar sua ação ou atividade.

Auditamos o acesso a contas privilegiadas semanalmente e revisamos o acesso mensalmente para garantir que ela ainda seja necessária ou seja de uso. Os registros de acesso a contas privilegiadas são revisados por consistência com registros de acesso.

ACESSO AUTORIZADO

A Coopanest-PE mantém um Registro de Acesso e detalha quais funcionários ou terceiros têm acesso a quais sistemas e informações. O cadastro também observa quando o acesso foi dado, quando será restrito (se acesso *temporário*), o tipo de dados ou sistema a ser acessado e o motivo do acesso.

CONTROLES DE LOGIN

Os sistemas só podem ser acessados por autenticação segura da validação do usuário, que consiste em um nome de usuário e senha no nível de usuário. Todos os computadores possuem um cliente de antivírus ativo e por padrão uma tela de bloqueio com autenticação do usuário necessária, após 10 minutos de inatividade a tela é bloqueada novamente. Todos os funcionários estão cientes de que se saírem de sua estação de trabalho, seu monitor deve ser desligado e seu sistema bloqueado.

CREDENCIAIS E FUNÇÕES

O acesso a qualquer sistema dentro da Coopanest-PE (incluindo o *envio de e-mails*), utiliza a autenticação com base nas credenciais válidas que estão sendo utilizadas. Cada usuário recebe credenciais exclusivas e não tem permissão para compartilhá-las ou divulgá-las a qualquer outro funcionário ou terceiro. É necessário que as credenciais sejam armazenadas para que, quando forem usadas para acessar um sistema, banco de dados ou enviar um e-mail, o processo de autenticação

funcione. Todas as credenciais de autenticação são criptografadas quando armazenadas e transmitidas e o acesso é restrito ao **Departamento de Tecnologia**.

CONTROLES DE ACESSO FÍSICO

O acesso ao prédio da Coopanest-PE, seções de escritórios e salas seguras são protegidos por **medidas de segurança** (**ou seja, cadeados, CFTV, alarmes, biometria etc.**). Isso aumenta a segurança do edifício, informações e funcionários, e garante que nenhum acesso não autorizado seja possível.

Todas as janelas estão alarmadas e são mantidas trancadas quando o prédio é desocupado. Os visitantes são escoltados o tempo todo durante uma visita e recebem um crachá de identificação. Quando um visitante é obrigado a levar qualquer bolsa com eles (incluindo *notebooks*), reservamo-nos o direito de revistá-los ao entrar e sair do prédio.

HORÁRIO DE FUNCIONAMENTO EXTERNO

Quando o prédio é desocupado no final do horário de trabalho, o sistema de alarme é ativado e protege todas as janelas e portas. Ao final de expediente qualquer gatilho de alarme notificará imediatamente os **Serviços de Segurança**, que têm uma árvore de contato para o **diretor e o responsável pela segurança patrimonial**.

ACESSO DIRETO

O uso de chaves para quaisquer edifícios, salas, armários seguros, cofres etc. são sempre controlados e registrados e as chaves são fornecidas apenas aos funcionários que as necessitam por razões funcionais. Os locais das chaves são conhecidos o tempo todo e se houver alguma suspeita de que uma chave foi perdida ou comprometida, os pontos de bloqueio e de acesso são alterados imediatamente e monitorados até que a alteração seja afetada.

RESPONSABILIDADES

Os gestores de cada departamento são responsáveis por garantir que todos os funcionários estejam cientes das **políticas de segurança**, incluindo controle de acesso e senhas seguras e a Coopanest-PE opera uma abordagem de cima para baixo. Os gestores precisam estar cientes de que têm a responsabilidade de garantir que os funcionários tenham conhecimentos suficientes e relevantes sobre a segurança das informações.

COOPANEST · PE

Cooperativa dos médicos anestesiologistas de Pernambuco.

Rua Benfica, 326 - Madalena,
Recife - PE, CEP: 50720-001

CONTATOS:

e-mail: anestpe@coopanestpe.com.br

Telefone: (81) 2126-2988