DIRETORIA EXECUTIVA
COORDENADORIA DE INFORMÁTICA - COINF

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas

PSI 001 REV 002

Recife – PE, Maio de 2024.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Elaboração	Rubrica	Data
Rodrigo Gonçalves Muniz Área: Informática		/ /

Revisão	Rubrica	Data
Sweet Gallegher Caetano Costa Área: Informática		/ /

Aprovação	Rubrica	Data
Erick Renan Pereira de Acioli Chefe da Divisão de Informática		/ /
Sérgio Noronha Diretor Administrativo Financeiro		/ /

Efetivação	Rubrica	Data
Tereza Raquel F. Almeida Coordenadora da Garantia da Qualidade		/ /

Elaborado por:_____

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

1.1 O objetivo é estabelecer diretrizes, princípios e responsabilidades que permitam aos colaboradores do LAFEPE seguirem padrões de comportamento relacionados à segurança da informação, relacionados ao tratamento das informações e uso adequado às necessidades de negócio e da proteção legal da instituição, especialmente voltados ao cumprimento do quanto previsto nas leis nº 12.965/2014 (“Marco Civil da Internet”) e 13.709/2018 (“Lei Geral da Proteção de Dados Pessoais” ou “LGPD”), preservando as informações no tocante a:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais. É o nível de confiança sobre a veracidade das informações;
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos Ativos correspondentes sempre que necessário.

1.2 Dessa forma, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar da melhor forma, as ferramentas de TI e, ao mesmo tempo, reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

2. ÂMBITO DA POLÍTICA

2.1 As diretrizes aqui estabelecidas deverão ser seguidas por todos os servidores, empregados, estagiários, jovens aprendizes, terceirizados e prestadores de serviços que exerçam atividades no âmbito do LAFEPE, partes interessadas nas atividades executadas pelo LAFEPE, ou ainda quem quer que venha a ter acesso a dados ou informações e em qualquer meio ou suporte;

2.2 Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, mediante prévia e expressa informação nesse sentido, conforme previsto nas leis brasileiras;

2.3 É também obrigação de cada colaborador manter-se atualizado em relação a esta PSIe aos procedimentos e normas relacionadas, buscando orientação do seu gestor, do departamento jurídico ou da área de tecnologia da informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações;

2.4 À exceção de dados pessoais de titulares (pessoas naturais), colaboradores do LAFEPE, terceiros, clientes e/ou parceiros, toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional desenvolvida para o LAFEPE pertence à referida instituição. Demais exceções devem ser explícitas e formalizadas em contrato entre as partes interessadas;

2.5 Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados unicamente para a realização das atividades profissionais e de acordo com a função exercida pelo colaborador.

3. DIRETRIZES GERAIS

3.1 Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio;

3.2 Ameaças e riscos devem ser reavaliados periodicamente – de natureza preventiva, sem exclusão das avaliações de natureza corretiva - para garantir que a organização esteja efetivamente protegida, evitando, ainda, a interrupção das atividades do LAFEPE;

3.3 A Avaliação de conformidade do Sistema de Segurança da Informação deve ser contínua e aplicada visando contribuir com a Gestão de Segurança da Informação;

3.4 As não-conformidades relativas ao descumprimento da legislação, normas e procedimentos serão considerados riscos de Segurança da Informação e deverão ser tratados;

3.5 A Política de Segurança da Informação e seus documentos acessórios aplicam-se, indistintamente, a todos os recursos humanos da instituição, próprios ou terceirizados, permanentes ou temporários, a qualquer título;

3.6 Os gestores da informação classificarão as informações e estabelecerão os níveis de requisitos das mesmas;

3.7 O acesso a informações sigilosas, produzidas ou recebidas pelo LAFEPE, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos;

3.8 Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir esta PSI e seus documentos acessórios, sem prejuízo da observância da legislação em vigor;

3.9 Todos os colaboradores são responsáveis pela proteção pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os com os quais tenham contato, assim como dos ambientes (físicos ou digitais) a que tenham acesso, independentemente das medidas de segurança já implementadas;

3.10 O LAFEPE irá auditar, periodicamente, acesso e a utilização de seus ativos tecnológicos, de forma que ações indesejáveis ou não autorizadas sejam detectadas, para garantir a conformidade das ações de seus colaboradores em relação ao ora estabelecido, e em obediência à legislação aplicável;

3.11 Esta política de Segurança da Informação pode ser revisada periodicamente e eventualmente revista sempre que eventos ou fatos relevantes ocorram.

4. CONCEITOS E DEFINIÇÕES

4.1 Para os fins dessa Política, considera-se:

- **Acesso Não Autorizado -** Acesso indevido ou não previsto obtido, por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nosmecanismos de controle de acesso. Contrasta com acesso autorizado;
- **Acesso Lógico –** acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
- **Acesso Remoto –** ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
- **AES –** ***Advanced Encription Standard*** **-** sistema de criptografia bastante complexo e capaz de prover confidencialidade e integridade dos dados. Atualmente, é o algoritmo de criptografia internacionalmente aceito e adotado como padrão para sistemas de segurança;
- **Ameaça –** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Análise/avaliação de riscos –** processo completo de análise e avaliação de riscos;
- **Ativo -** qualquer bem, tangível ou intangível, que tenha valor para a organização;
- **Ativo da Informação –** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **Auditoria –** verificação e avaliação dos sistemas e procedimentos internos como objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;
- **Autenticação –** é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;
- **Autenticidade –** propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

- **Banco de Dados (ou Base de Dados) –** é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;
- **Bloqueio de acesso –** processo que tem por finalidade suspender temporariamente o acesso;
- **Classificação da informação** - atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
- **Colaborador –** servidores, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito do LAFEPE;
- **Confidencialidade –** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- **Contingência -** descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;
- **Controle de Acesso -** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Cópia de Segurança (*Backup*) –** copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;
- **Correio Eletrônico -** é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
- **Credenciais ou contas de acesso -** permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;
- **Criptografia –** é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");
- **Criptografia WPA2 – *Wi-Fi Protected Access 2* -** recurso de criptografia para redes do tipo *Wi-Fi*, compatível com o padrão IEEE 802.11 (ver 1.7.1.1), que devido aos aspectos de segurança tratados tornou-se mais indicado que sua versão anterior (WPA) e que o protocolo de segurança WEP – *Wired Equivalent Privacy* – prescrito pelo padrão 802.11;
- **Dado –** representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;
- **DHCP – *Dynamic Host Configuration Protocol*** protocolo que oferece configuração

dinâmica de terminais com concessão de endereços IP (*Internet Protocol*) de *Host* e outros parâmetros de configuração para clientes de rede;

- **Disponibilidade -** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- ***Download* -** Baixar/copiar arquivos de um servidor (*Site*) na internet para um computador pessoal;
- ***Firewall* -** mecanismo que atua como uma barreira de proteção entre duas ou mais redes, de modo a regular, por meio de regras e a filtragem de dados, o tráfego de dados entre essas redes e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra;
- ***Firmware* -** *software* proprietário que controla diretamente o *Hardware* do equipamento. Esse *software* é armazenado diretamente no *chip* de memória tais como ROM (*Read Only Memory*), *EPROM* (*Erasable and Programable ROM*) e memória *flash*. Alguns fabricantes de equipamentos fornecem atualizações desse tipo de *software*;
- **Gestão de Continuidade de Negócios -** Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;
- **Gestão de Risco –** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Gestão de Segurança da Informação e Comunicações -** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Gestor da Informação -** pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;
- **Gestor de Segurança da Informação e das Comunicações –** é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APE;
- ***Hardware* –** É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;
- ***Host* -** ou cliente, é qualquer máquina ou computador conectado a uma rede que se beneficia de um serviço oferecido por esta;
- **IEEE –** ***Institute of Electrical and Electronics Engineers* -** criado em 1884, nos E.U.A., a

IEEE é uma sociedade técnico-profissional internacional, dedicada aoavanço da teoria e prática da engenharia nos campos da eletricidade, eletrônica e computação;

- **Incidente de Segurança -** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- **Informação -** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **Informação sigilosa -** informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais desigilo;
- **Integridade –** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Internet –** rede mundial de computadores;
- **Intranet –** rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;
- ***Log* -** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;
- ***Logon* -** Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
- **Norma -** Documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSI, no todo ou em parte da instituição. As normas mapeiam a PSI na organização técnico- administrativa da instituição, estabelecendo regras para a sua implementação;
- ***Online* –** (Estar disponível ao vivo) no contexto da Internet significa estar disponível para acesso imediato, em tempo real;
- ***Peer-to-peer* (P2P) –** (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;
- **Perfil de acesso -** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
- **Política de Segurança da Informação (PSI) –** documento aprovado pela autoridade

responsável pelo órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação na instituição;

- **Ponto de Acesso -** do inglês *Access Point* ou simplesmente AP. É um equipamento que realiza a interconexão entre todos os dispositivos que fazem parte de uma rede sem fio. Em geral se conecta a uma rede cabeada servindo de ponto de acesso para uma outra rede, como por exemplo, a Internet;
- **Protocolo -** convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;
- ***Proxy* -** é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede *proxy* serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;
- **Recursos Computacionais -** recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, *notebooks*, servidores de rede, equipamentos de conectividade e infraestrutura;
- **Rede Corporativa -** conjunto de todas as redes locais sob a gestão da instituição;
- **Rede Pública –** rede de acesso a todos;
- **Responsabilidade -** Obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos Ativos de informação de qualquer natureza;
- **Senha ou Credencial de Acesso-** Credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado Ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes;
- **Servidor de Rede -** recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
- ***Software* -** São todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
- ***Site* -** Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;
- **SSID – *Service Set Identifier* -** identificador de uma rede sem fio. Normalmente usado no momento da conexão, no qual o cliente localiza as redes sem fio disponíveis e escolhe a que ele quer realizar a conexão por meio do SSID;

- ***Streaming*** **-** transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;
- **Termo de Responsabilidade -** termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações as quais tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;
- **Termo de Responsabilidade:** Computador Compartilhado – termo assinado pela chefia do setor que se responsabiliza pela integridade de computadores que, pelas funções as quais administra, não são passíveis de uso de único colaborador, como computadores ligados à equipamentos analíticos;
- **Tratamento de Incidentes de Segurança em Redes Computacionais -** serviço que consiste em receber, filtrar, classificar e responder às solicitações ealertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- **Usuário -** servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APE, formalizada por meio da assinatura do Termo de Responsabilidade;
- **VLAN (*Virtual Local Area Network* ou *Virtual LAN*) –** (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;
- **VPN (*Virtual Private Network*) –** (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;
- **Vulnerabilidade -** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;
- ***Wireless*** **(rede sem fio) -** rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

5. COMPETÊNCIAS E RESPONSABILIDADES

5.1 **Diretor Administrativo e Financeiro:**

- Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização;
- Apoiar a Política e manter compromisso com sua continuidade e resultados.

5.2 **Coordenador de Informática:**

- Promover cultura de segurança da informação e comunicações, através de ações de interesse do LAFEPE, bem como treinamentos regulares, programas educacionais e de conscientização do corpo de colaboradores;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Propor recursos necessários às ações de segurança da informação e comunicações;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
- Propor normas Complementares e Procedimentos de Segurança da Informação e das Comunicações;
- Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;
- Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;
- Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;
- Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;
- Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso.

5.3 **Colaboradores do LAFEPE:**

- - Firmar Termo de Responsabilidade presente nos anexos e de Ciência da Política de Segurança da Informação;
- - Conhecer e Cumprir com todas as orientações, diretrizes e normas estabelecidas por esta Política e seus anexos;
- - Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes do LAFEPE;
- - Utilizar, modificar ou reproduzir dados e informações do LAFEPE exclusivamente para o

desempenho de suas funções, da mesma forma que a utilização dos recursos de TIC em nome do LAFEPE;

- - Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não tenham nível de autorização suficiente;
- - Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle do LAFEPE sem autorização formal;
- - Proteger Ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizados;
- - Informar às situações que comprometam a segurança das informações nas unidades organizacionais do LAFEPE, diretamente ao seu Gestor, ou ao setor de TIC do LAFEPE;
- - Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias, tais como cartões de identificação, *login*s e senhas, crachás, dentre outros.

5.4 **Divisão de Pessoal do LAFEPE:**

- Informar ao setor de tecnologia da informação todos os desligamentos, alteração de função/cargo, afastamentos, retornos e modificações no quadro funcional doLAFEPE.

5.5 **Superintendência Jurídica:**

- Prestar assessoramento de natureza jurídica, supervisionar e coordenar as atividades de natureza jurídica, inclusive àquelas relacionadas com a elaboração de atos normativos.

5.6 **Comissão de Apuração e Aplicação de Penalidades**

- Prestar apoio de natureza jurídica, na análise do não cumprimento pelo colaborador das normas estabelecidas para a utilização da rede LAFEPE;

6. NORMAS COMPLEMENTARES

6.1 O detalhamento da Política de Segurança da Informação está segmentado nas seguintes Normas Complementares:

6.1.1 NC 01 - Política de Controle de Acesso;

6.1.2 NC 02 - Política de Acesso a Internet;

6.1.3 NC 03 - Política de uso de Equipamentos de Informática;

6.1.4 NC 04 - Política de boas práticas no uso do e-mail corporativo;

6.1.5 NC 05 - Política para uso de rede sem fio.

7. PENALIDADES

7.1 O não cumprimento das determinações da Política de Segurança da Informação é considerada falta grave e sujeitará o infrator às penalidades previstas na legislação aplicável ao tema e nos regulamentos internos do LAFEPE;

7.2 O descumprimento das disposições constantes nessa Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil, inclusive, sem limitação, eventual ajuizamento de ações de regresso e/oude perdas e danos;

7.3 Todas as disposições legais, documentos institucionais e demais normas do LAFEPE, como o seu Código de Conduta e Integridade, e Estatuto Social devem ser rigorosamente observadas.

8. CONSIDERAÇÕES FINAIS

8.1 Os casos omissos e dúvidas serão submetidos à Coordenadoria de Informática, em conjunto com o Departamento Jurídico, sempre que aplicável.

9. REFERÊNCIAS

9.1 Esse documento teve como base fundamental o Plano de Segurança da Informação da Secretaria de Administração do Estado de Pernambuco de 2015 - (PSI-SAD_2015 http://www.sad.pe.gov.br/web/sad/politica-de-seguranca) e a documentação da Agência de Tecnologia do Estado de Pernambuco - ATI-PE disponível em http://www2.ati.pe.gov.br/web/*Site*-ati/seguranca-de-ti#nogo .

10. ANEXOS

ANEXO I
NORMAS COMPLEMENTARES:

NC 01 – POLÍTICA DE CONTROLE DE ACESSO

1. Objetivo

1.1. Estabelecer critérios para a disponibilização e administração do acesso aos serviços detecnologia de informação do LAFEPE, bem como estabelecer critérios relativos a *login*se senhas das respectivas contas.

2. Diretrizes Gerais

2.1. A conta de acesso é o instrumento para identificação do usuário na rede do LAFEPE e caracteriza-se por ser de uso pessoal, individual e intransferível e sua divulgação é vedada sob qualquer hipótese;

2.2. Todo cadastramento de conta que permita acesso à rede de dados, sistemas, contas de e-mail ou outro tipo de acesso gerido pela COINF deve ser efetuado mediante solicitação da chefia imediata via sistema de chamados ou e-mail de suporte da área de tecnologia contendo identificação do colaborador a acessar o sistema e detalhamento de suas atividades, concessões e restrições;

2.3. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas;

2.4. Todas as senhas, para autenticação na rede do LAFEPE, devem seguir os seguintes critérios mínimos:

- Toda senha deve ser constituída de, no mínimo, 8 caracteres utilizando obrigatoriamente, letras maiúsculas e minúsculas, números e, preferencialmente, caracteres especiais como: !,@,#, etc;
- A senha não pode conter parte do nome do usuário e outros caracteres facilmente descobertos, como data de aniversário, por exemplo;
- A tempo de expiração da senha é de no máximo 90 (noventa) dias, caso não seja alterada, esta será bloqueada;
- Após o vencimento da senha, a mesma não poderá ser reutlizada nas próximas 04 alterações,

onde somente será aceito o uso de uma senha antiga após 04 modificações;

- A conta de usuário que tiver sua senha digitada de forma incorreta por 3 vezes, será bloqueada de forma automática pelo nosso Servidor, sendo desbloqueada automaticamente após o intervalo de 15 minutos;
- Será obrigatória a troca de senha ao efetuar o primeiro *Logon*.

2.5. A base de dados de senhas será armazenada com criptografia e restrita aos administradores do setor de tecnologia;

2.6. O acesso aos serviços de tecnologia de informação do LAFEPE deve ser disponibilizado aos colaboradores que oficialmente executem Atividade vinculada à atuação institucional do LAFEPE;

2.7. O setor de Recursos Humanos do LAFEPE deve comunicar à Coordenadoria de Informática todos os desligamentos, afastamentos e aposentadorias e as movimentações de funcionários, via planilha de controle de pessoal, que impliquem mudança de lotação e/ou de permissões;

2.8. Contas sem acesso por mais de 90 (noventa) dias serão bloqueadas automaticamente à exceção daquelas comunicadas previamente pelo setor de Recursos Humanos, e que estejam relacionadas a algum regime especial, como, por exemplo, licença maternidade, licença por prazo indeterminado, afastamento de trabalho por acidente, dentre outros;

2.9. O processo de aprovação dos acessos deve ser iniciado pelo superior imediato do usuário e os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe o Órgão Público. Se um desses dois eventos ocorrer, a chefia imediata tem que notificar imediatamente a unidade responsável;

2.10. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada à Coordenadoria de Informática;

2.11. As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede;

2.12. Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

3. Acesso Remoto

3.1. O acesso remoto aos serviços corporativos somente devem ser disponibilizados aos

servidores e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do LAFEPE e que necessitam temporariamente deste serviço para execução de suas atividades institucionais, desde que autorizados pela chefia responsável pela informação;

3.2. A liberação de acesso remoto só será efetivada após avaliação e aprovação pela Coordenadoria de Informática, para que se evitem ameaças à integridade e sigilo das informações contidas na rede LAFEPE;

3.3. As conexões remotas à rede do LAFEPE devem ocorrer da seguinte maneira:

I. Utilização de autenticação;

II. As senhas e as informações que trafegam entre a estação remota e a rede do LAFEPE devem estar criptografadas;

III. É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.

3.4. O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

I. Finalização do período solicitado ou termino do Contrato;

II. Perda da necessidade de utilização do serviço;

III. Transferência do usuário para outras unidades;

IV. Identificação de vulnerabilidade, risco ou uso indevido.

4. Controle de Acesso Físico

4.1. Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e suprimentos da COINF e à proteção dos recursos computacionais, permitido apenas às pessoas autorizadas;

4.2. O acesso ao *datacenter* somente poderá ser feito por pessoas autorizadas;

4.3. O acesso de visitantes ou terceiros ao *datacenter* somente poderá ser realizado com acompanhamento de um colaborador autorizado;

4.4. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da Divisão de Serviços Gerais;

4.5. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;

4.6. A entrada ou retirada de quaisquer equipamentos somente se dará com a solicitação formal

pelo do colaborador solicitante ou autorização formal pelo responsável do Datacenter.

NC 02 - POLÍTICA DE ACESSO À INTERNET

1. Objetivo

1.1 Estabelecer critérios para administração e utilização de acesso aos serviços de Internet no âmbito do LAFEPE.

2. Diretrizes Gerais

2.1. O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

2.2. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

2.3. A Coordenadoria de Informática (COINF) deverá prover o serviço de conexão à Internet implementando mecanismos de segurança adequados, bem como níveis de acesso adequados;

2.4. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, Site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação;

2.5. Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela COINF, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede do LAFEPE;

2.6. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:

a. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;

b. Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede do LAFEPE;

c. Uso recreativo da internet em horário de expediente;

d. Uso de *proxy* anônimo;

e. Acesso a salas de bate-papo (chats), exceto aqueles definidos como ferramenta de trabalho homologada pela Coordenadoria de Informática;

f. Acesso à rádio e TV em tempo real, exceto os canais corporativos em horário de expediente;

g. Acesso a jogos;

h. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;

i. Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensagens ou bate-papo, *blogs*, *microblogs*, ou ferramentas semelhantes;

j. Envio a destino externo de qualquer *software* licenciado à LAFEPE ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;

k. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do LAFEPE;

l. Utilização de *softwares* de compartilhamento de conteúdos na modalidade peer- to-peer (P2P) ou similares;

m. Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação do LAFEPE, na forma definida pela COINF.

2.7. Caso o órgão julgue necessário, haverá bloqueios de acesso a arquivos e s*ite*s não autorizados que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do colaborador, bem como, que exponham a rede ariscos de segurança;

2.8. O usuário poderá solicitar liberação de determinada página, com a devida justificativa, mediante solicitação formal da Chefia imediata à Coordenadoria de Informática;

2.9. Somente serão liberadas as páginas analisadas e autorizadas pela COINF em consonância com essa PSI;

2.10. É proibido utilizar os recursos do LAFEPE para fazer o *download* ou distribuição de *software* ou dados não legalizados, ou ainda, que não guardem relação com a natureza da função executada pelo colaborador;

2.11. Haverá geração de relatórios dos *sites* acessados por usuário para verificação da adequação à política vigente;

2.12. Comprovada a utilização irregular, o usuário envolvido poderá ter o seu acesso à Internet bloqueado, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

NC 03 – POLÍTICA DE USO DE EQUIPAMENTOS DE INFORMÁTICA

1. Objetivo

1.1 Estabelecer critérios na utilização dos equipamentos de informática no LAFEPE.

2. Diretrizes Gerais

2.1. Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse do LAFEPE;

2.2. Cada estação de trabalho possui controle de IP (*Protocol Internet*), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que ausentar do ambiente de trabalho tenha certeza que efetuou o logoff ou bloqueou a estação de trabalho;

2.3. Não é permitido a nenhum usuário utilizar *software/hardware* sem autorização da COINF;

2.4. Não é permitido gravar nas estações de trabalho e na Rede do LAFEPE arquivos de áudio em formato MP3 ou similares, filmes, fotos e *software* com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;

2.5. Todos os dados relativos às atividades do laboratório devem ser mantidos no servidor de rede, onde existe sistema de *backup* diário e confiável;

2.6. Os arquivos gravados em diretórios temporários (pastas públicas) podem ser acessados por todos os usuários que utilizarem a rede local, portanto não garante sua integridade, podendo ser alterados ou excluídos sem prévio aviso e por qualquer usuário;

2.7. Não será feito cópia de segurança dos arquivos criados no computador local dos colaboradores. O próprio usuário deve fazer cópia de segurança dos arquivos e verificar o que pode ser eliminado, evitando acumulo de dados desnecessários, podendo ser monitorados pela equipe de SUPORTE da COINF, caso haja irregularidades no armazenamento destes arquivos;

2.8. É proibida a abertura de computadores para qualquer tipo de reparo, seja isto feito em departamentos ou laboratórios de informática, caso seja necessário o reparo deverá ocorrer pela Coordenadoria de Informática – COINF;

2.9. Quanto à utilização de equipamentos de informática particulares (celulares, *notebooks*, *tablets* e/ou quaisquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada) o colaborador deverá comunicar a chefia imediata, que solicitará sua liberação de acesso;

2.10. Nos casos de eventos no ambiente do laboratório, tais como, seminários, licitações, etc, deverá ser solicitado à Coordenadoria de Informática - COINF a senha de acesso à rede sem fio para visitantes, que será analisado e caso autorizado, liberado pela COINF;

2.11. Em caso de dano, inutilização ou extravio do equipamento o colaborador deverá comunicar imediatamente à COORDENADORIA DE INFORMÁTICA - COINF que deverá adotar as providências legais cabíveis;

2.12. Em caso de furto ou roubo, providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo na COINF, que deverá adotar as providências legais cabíveis;

2.13. É obrigatória a vinculação dos componentes (gabinete, monitor, teclado e mouse), conforme nºs de tombamentos ou números de série, impedindo a sua utilização para outro usuário que não assina o Termo de Responsabilidade. A exceção de impedimento se aplica aos computadores ditos compartilhados, onde o Termo de Responsabilidade é assinado pela chefia do setor;

2.14. É proibida a colocação de adesivos, imãs e adereços autocolantes, exceto o adesivo da empresa que executa o serviço de *SERVICEDESK*;

2.15. É dever, do colaborador, zelar pela integridade do equipamento estritamente como instrumento de trabalho, juntamente com os acessórios que foram utilizados;

2.16. É proibida a instalação ou remoção de s*oftwares* que não forem devidamente acompanhadas pela Coordenadoria de Informática - COINF;

2.17. É de inteira responsabilidade do usuário ao receber o Termo de Responsabilidade, verificar as informações nele contidas como Tombamento, série, além dos seus dados pessoais, matrícula e unidade de trabalho;

2.18. Não é permitido alterar as configurações de rede e da *BIOS* das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro;

2.19. Não é permitido retirar ou transportar qualquer equipamento do LAFEPE sem autorização prévia da COINF;

2.20. Fica proibida, sem odevido consentimento, a utilização de equipamentos de informática por pessoas sem vínculo com o LAFEPE;

2.21. É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática;

2.22. Não é permitido conectar e/ou configurar equipamento à rede, sem a prévia liberação da Coordenadoria de Informática - COINF;

2.23. Todas as estações de trabalho deverão possuir o programa de antivírus compatível com seu sistema operacional.

2.24. O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;

2.25. O usuário deve, nos dispositivos com acesso a esse tipo de mídia, obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho.

3. Política de *Backup* e Restauração de Arquivos

3.1. Todos os *Backup*s devem ser realizados por sistemas configurados como citado nos POP COINF 003 e POP COINF 009 de acordo com particularidade de uso e os dados voltados para *Backup*;

3.2. *Backups* Incrementais Arquivos (Incremental diários) serão realizados todos os dias preferencialmente a partir das 23:00, com 16 (dezesseis) dias de retenção;

3.3. Os *Backups* completos de arquivos (completo semanais) serão realizados a partir das 23:00, sempre quando houver inclusão de pastas na rede, com 16 dias de retenção;

3.4. Os *Backups* completos das Máquinas Virtuais,que porventura sejam configuradas, devem ser realizados na primeira sexta-feira do mês, realizados a partir das 23:00h, com um mês de retenção;

3.5. A restauração de Arquivos só será possível em arquivos nos quais foram feitos *Backup* no dia anterior;

3.6. Devido ao *Backup* ser feito apenas às 23h00 de cada dia não é possível restaurar um arquivo criado e editado no mesmo dia que foi perdido;

3.7. Restauração da versão de arquivo terá um prazo máximo de 16 (dezesseis) dias, não sendo possível recuperar versões desses arquivos mais antigos que esse período;

3.8. Não e possível recuperar um arquivo criado e editado e perdido no mesmo dia, já que o mesmo não foi feito pelo *Backup* das 23h00;

3.9. Os colaboradores responsáveis pela gestão dos sistemas de *Backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida quando o *software* não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

4. Política de uso de impressoras e documentos físicos

4.1. Todas as impressões deverão ser executas nas suas respectivas áreas, exceto quando uma impressora está disponibilizada de forma previamente planejada para diversas áreas ou quando a impressão for destinada a outra área, evitando locomoção dos funcionários, também previamente

planejado;

4.2. Não é permitido imprimir documentos que não estejam dentro das atividades de trabalho;

4.3. Não é permitido deixar impressões erradas na mesa das impressoras, sendo certo que, tais impressões, quando possuam dados pessoais de titulares – colaboradores ou não – do LAFEPE deverão ser imediatamente destruídas. Caso não possuam dados de natureza pessoal, poderão servir como rascunho, pelo que o colaborador deve acondicionar tais papéis no local designado para este fim;

4.4. Os colaboradores devem utilizar seu *login* e senha de rede para permitir a impressão, escaneamento e demais funcionalidades da impressora;

4.5. Os documentos deverão preferencialmente ser impressos frente e verso, para economia de papel;

4.6. Os colaboradores poderão utilizar a digitalização nas impressoras multifuncionais, facilitando a economia de impressão, sem custo para o LAFEPE;

4.7. Nenhum documento impresso deverá ficar sem qualquer tipo de tratamento, seja encaminhado para o setor/colaborador responsável, seja digitalizado e arquivado, ou mesmo destruído e descartável;

4.8. Documentos impressos ou manualmente escritos que possuam dados pessoais de qualquer natureza, tais como, sem limitação, fichas, relatórios, notas fiscais, contratos, formulários, requerimentos, dentre outros, jamais deverão estar disponíveis para o acesso de outros (terceiros ou colaboradores) que não os colaboradores especificamente designados para o seu tratamento. É proibido o acondicionamento de tais documentos em bancadas, mesas, ao lado de impressoras ou escaninhos que não sejam designados para o seu acondicionamento. O proprietário do documento é inteiramente responsável pela sua posse e guarda, e deverá garantir que pessoas não autorizadas não tenham acesso ao conteúdo de tais documentos.

NC 04 – POLÍTICA DE BOAS PRÁTICAS NO USO DE E-MAIL CORPORATIVO

1. Objetivo

1.1 Estabelecer critérios para disponibilização do serviço de correio eletrônico corporativo do LAFEPE aos usuários.

2. Diretrizes Gerais

2.1. O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do LAFEPE;

2.2. São usuários do serviço de correio eletrônico corporativo os colaboradores que executem atividade vinculada à atuação institucional do LAFEPE;

2.3. A concessão de contas de correio eletrônico depende de pedido da chefia imediata;

2.4. Poderá ser solicitada a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação;

2.5. É vedado o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

2.6. Para fins legais de auditoria, o LAFEPE se reserva ao direito de realizar investigações nas caixas postais do e-mail corporativo;

2.7. O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

2.8. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I. Praticar crimes e infrações de qualquer natureza;

II. Executar ações nocivas contra outros recursos computacionais do LAFEPE ou de redes externas;

III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede do LAFEPE;

V. Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

VI. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções

institucionais desempenhadas pelo LAFEPE;

VII. Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

VIII. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

2.9. É de responsabilidade do usuário do correio eletrônico:

I. Manter em sigilo sua senha de acesso ao correio eletrônico;

II. Fechar o aplicativo de correio (cliente) toda vez que se ausentar, evitando o acesso indevido;

III. Comunicar imediatamente a COINF do recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;

IV. Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo;

V. Envio de mensagens indesejáveis recebidas, que não foram bloqueadas pelo servidor de e-mail, para a COINF, juntamente com o endereço do remetente, para comunicação a ATI inclusão na lista de mensagens filtradas.

2.10. É de responsabilidade da Coordenadoria de Informática:

I. Criar e manter cadastro dos usuários, das caixas postais e das listas dedistribuição;

II. Cancelar os acessos ao serviço de correio eletrônico dos usuários que se desvincularem do Laboratório;

III. Propor a divulgação de orientação sobre o uso correto do correio eletrônico;

IV. Fiscalizar a utilização do serviço de correio eletrônico, observados os critérios estabelecidos nesta norma;

V. Desenvolver demais ações que garantam a operacionalização desta norma.

NC 05 – POLÍTICA DE USO DE REDE SEM FIO

1. Objetivo

1.1 Estabelecer critérios para a utilização das redes sem fio disponibilizadas pelo LAFEPE.

2. Diretrizes Gerais

2.1 O acesso à Internet e/ou corporativo por meio de rede sem fio no LAFEPE, implica na devida subordinação às demais normas que compõem a política de segurança do LAFEPE, pelo usuário. A utilização de redes sem fio permite mobilidade e independência de infraestrutura cabeada, sobretudo para os pontos isolados e com equipamentos de rede sobrecarregados. Entretanto, faz-se necessário o uso de recursos de segurança de forma a garantir não apenas a restrição de acesso à infraestrutura, mas também, que os demais requisitos de segurança da informação: confidencialidade, autenticidade, integridade e disponibilidade, especialmente quando se trata de acesso aos recursos corporativos sejam cumpridos.

3. Ambientes de uso da rede sem fio

3.1 Ambiente corporativo

A implementação de uma rede sem fio corporativa no ambiente da organização deverá atender aos seguintes requisitos de segurança:

a) A solução de rede sem fio corporativa deverá seguir os padrões de mercado recomendados e estar de acordo com as normas estabelecidas neste documento, devendo para tanto, existir um projeto elaborado por uma equipe técnica especializada, que deverá estudar também as peculiaridades do ambiente, o raio de cobertura do sinal de rádio, a velocidade da conexão, a especificação dos equipamentos e seus recursos de segurança e demais itens necessários à implantação da solução;

b) Os pontos de acesso deverão ser conectados aos ativos de rede da rede local atendendo ao raio de cobertura da solução, porém, sob uma VLAN específica para este fim, com faixa de endereços IP's inválidos e distintos aos da rede local corporativa, de forma a evitar que os recursos corporativos estejam sob risco de segurança;

c) Os pontos de acesso deverão estar dispostos em locais físicos que não permitam ou, ao menos, intimidem ou desestimulem a manipulação feita por terceiros não autorizados. Para uma melhor proteção do equipamento, recipientes poderão ser utilizados ou adaptados para esses dispositivos, de forma que não comprometam a eficiência da transmissão de dados por ondas de rádio;

d) Cada ponto de acesso deverá ter seu *firmware* sempre atualizado, de maneira a evitar invasões por brechas no seu sistema de configuração;

e) Os pontos de acesso deverão ser configurados com criptografia forte de acordo com o

padrão AES mais seguro e atual do mercado, que implementa a autenticação 802.11;

f) Para fazer uso dos recursos da rede sem fio corporativa, os usuários deverão configurar seus respectivos dispositivos sem fio para usar a criptografia padrão AES, conforme a alínea e) desta seção;

g) O controle de acesso à Internet e/ou corporativo por meio da rede sem fio da organização deverá ser subordinado a um *firewall*. Este, por sua vez, interligará a rede sem fio à rede local e ao servidor *proxy*, se houver;

h) Deverá estar habilitado, de forma integrada ao serviço de diretório ou a algum sistema de autenticação de usuário, um serviço de autenticação remota, que permitirá o acesso à base única de usuários por qualquer etapa de autenticação, seja do ponto de acesso, de uma VPN ou do domínio, sendo este último opcional;

i) Os usuários ao se conectarem à rede sem fio, conforme a alínea f) desta seção, a princípio, apenas terão acesso à internet por meio de autenticação no Firewall, permanecendo, dessa forma, isolados da rede corporativa e dos recursos disponibilizados por esta. A autenticação será realizada a partir de uma base única de usuários, conforme explícito na alínea h) desta seção;

j) O acesso aos recursos corporativos da organização exigirá aos usuários, além da autenticação na rede sem fio, uma nova autenticação, dessa vez no serviço de VPN, de acordo com seu enquadramento na política de acesso aos recursos da rede corporativa da organização, se houver;

k) O identificador da rede sem fio (SSID) deverá ser diverso ao padrão de fábrica, portanto, deve ser substituído por outro a ser definido pela equipe técnica responsável. O recurso de publicação do SSID deverá estar habilitado para que a rede sem fio possa ser automaticamente detectada;

l) O serviço de DHCP da rede sem fio deverá estar habilitado e configurado com uma faixa de endereços IP's inválidos e distintos da rede corporativa da organização, conforme já definido na alínea b);

m) A senha de administração dos pontos de acesso integrantes da rede sem fio deverá ser diversa ao padrão de fábrica e, portanto, deverá ser substituída por outra a ser definida pela equipe técnica responsável, conforme as recomendações de uso e formação de senhas. Esta senha deve ser a mesma para todos os pontos de acesso integrantes da solução, de forma a facilitar sua administração pela equipe técnica responsável;

n) O sistema de *log* dos pontos de acesso integrantes da rede sem fio deverá ser ativado e configurado pela equipe técnica responsável a fim de viabilizar auditorias e detecção de problemas;

o) O acesso à rede sem fio deverá estar subordinado ao cadastramento prévio do usuário no serviço de diretório da rede ou outra solução que dê provimento a uma base única de usuários (ver alínea h).

ANEXO II

TERMO DE RESPONSABILIDADE

Pelo presente termo de responsabilidade, eu _____, matrícula_____, pertencente ao setor _____, responsabilizo-me pelo computador_____ de tombo/serial_____, lacre_____e seus componentes: monitor (tombo/serial_____), teclado(tombo/serial_____) e mouse(tombo/serial_____), pertencentes ao LAFEPE, à título de empréstimo, comprometendo-me pelo zelo e utilização de acordo com o determinadono Plano de Segurança da Informação do LAFEPE enquanto desenvolver minhas atividades.

Por ser a expressão da verdade, firmo o presente termo de responsabilidade.

Recife,_____de_____de_____.

_____

Assinatura e matrícula ou carimbo

DEVOLUÇÃO

Atestamos que o bem descrito acima foi devolvido em __/__/____ , nas seguintes condições:

(_) Em perfeito estado(_) Apresentando defeito(_) Faltando peças/ acessórios.

_____ _____

(Data / assinatura / nome do responsável pelo recebimento)

Elaborado por:_____

TERMO DE RESPONSABILIDADE – COMPUTADOR COMPARTILHADO

Pelo presente termo de responsabilidade, eu _____, matrícula_____, responsável pelo setor _____, responsabilizo-me pelo computador_____ de tombo/serial_____, lacre_____e seus componentes: monitor (tombo/serial_____), teclado(tombo/serial_____) e mouse(tombo/serial_____), pertencentes ao LAFEPE, à título de empréstimo, comprometendo-me pelo zelo e utilização de acordo com o determinadono Plano de Segurança da Informação do LAFEPE enquanto for responsável pelas atividades desenvolvidas pelos colaboradores do setor.

Por ser a expressão da verdade, firmo o presente termo de responsabilidade.

Recife,_____de_____de_____.

_____

Assinatura e matrícula ou carimbo

DEVOLUÇÃO

Atestamos que o bem descrito acima foi devolvido em __/__/____ , nas seguintes condições:

(_) Em perfeito estado(_) Apresentando defeito(_) Faltando peças/ acessórios.

_____ _____

(Data / assinatura / nome do responsável pelo recebimento)

11. HISTÓRICO

Revisão	Data	Descrição da alteração A: Alterações I: Inclusões E: Exclusões
002	20/05/2024	A: Nome do Diretor Administrativo e Financeiro; Alteração no nome do Termo de Responsabilidade; Alteração das páginas dos capítulos; Alteração do item 2.13 sobre Termo de Responsabilidade; Alteração do texto de do Termo de Responsabilidade. I: Inclusão do Termo de Responsabilidade e Devolução pela Guarda e Uso de Equipamento Compartilhado; Inclusão da Descrição do Termo de Responsabilidade Computador Compartilhado; Registro da Devolução.
001	29/08/2022	Emissão

Elaborado por:_____