Política de Segurança da Informação

MELHORES PRÁTICAS AO AMBIENTE DE TRABALHO

PBPREV
PARAÍBA PREVIDÊNCIA

AVENIDA RIO GRANDE DO SUL, S/N | JOÃO PESSOA - PARAÍBA

SUMÁRIO

INFORMAÇÕES E CONTATO 4
João Pessoa 4
Cajazeiras 4
Itaporanga 4
Campina Grande 4
Patos 5
Guarabira 5
Horário de Funcionamento 5
ESTRUTURA ORGANIZACIONAL 6
Presidente 6
Diretor Administrativo-Financeiro 6
Procurador 6
Gerente Previdenciário 6
Gerente Contábil-Financeiro 6
Gerente de Informática 6
Gerente de Folha de Pagamento 6
Coordenador de Concessão de Benefícios 6
Coordenador de Manutenção de Benefício e Cadastro 6
Coordenador de Compensação Previdenciária 7
Coordenador de Programas 7
Coordenador Jurídico Administrativo 7
Coordenador Jurídico Previdenciário 7
Coordenador de Orçamento e Execução Financeira 7
Coordenador de Investimentos 7
Coordenador de Perícia 7
Coordenador de Controle Interno 7
Coordenador de Arquivo 7
Coordenador de Atendimento e Protocolo 7
Coordenador de Aposentadorias 7
Coordenador de Pensão 8
Coordenador de Gestão de Pessoas 8
Coordenador de Digitalização 8
Ouvidor 8

Representantes PARAÍBA PREVIDÊNCIA (Presidente) 9
Representantes Secretaria de Estado da Administração 9
Representantes Poder Legislativo 9
Representantes Poder Judiciário 9
Representantes Ministério Público 9
Representantes Tribunal de Contas 10
Representantes Servidores Militares 10
Representantes Servidores Civis 10
Representantes Inativos e Pensionistas 10
Representantes Procuradoria-Geral 10
Representantes Civis Ativos (Presidente) 11
Representantes Civis Inativos 11
Representantes Militares Ativos 11
Representantes Militares Inativos 11
Representantes Conselho Administrativo 12
Representantes Procuradoria-Geral 12
Representantes Procuradoria-Geral 12
Representantes Controladoria Geral 12
1. INTRODUÇÃO 13
2. OBJETIVO 14
3. ABRANGÊNCIA 15
3.1 Divulgação e acesso à estrutura normativa 15
4. DEFINIÇÕES 15
4.1 Classificação da informação 16
5. REGRAS 17
5.1 Política de uso da internet 17
5.2 Uso da rede Sem Fio 18
5.3 Uso da Rede Cabeada 18
5.4 Política de Acesso aos Arquivos da Rede 19
5.5 Política de proteção da informação 19
5.6 Política de privacidade da informação 20
5.7 Política de Uso do E-mail 21
5.8 Política de uso dos computadores 21
5.9 Política de instalação de novos sistemas, aplicativos e/ou equipamentos 22
5.10 Política de senha e acesso 23
6. POLÍTICAS DE AUDITORIA E REGISTRO DE LOGS DE ACESSO 23

6.1. Credenciais de acesso 23
6.2. Arquivos pessoais 23
6.3. Política de descarte de dados e informações 24
6.4. Políticas de uso de dispositivos pessoais (celulares, tablets, notebook) 24
6.5. Política de uso de impressoras 24
7. POLÍTICA DE BACKUP E CONTINGÊNCIA 24
7.1. Procedimentos de backup dos arquivos e bancos de dados 24
7.2. Armazenamento dos backups 25
7.3. Teste de recuperação 25
7.4. Procedimentos de Contingência 25
8. POLÍTICA DE CONTROLE DE ACESSO À INFRAESTRUTURA 25
8.1. Regras de acesso ao datacenter 25
8.2. Bloqueio de acesso a funcionários desligados 26
8.3. Registro de chamados 26
9. RESPONSABILIDADES 26
9.1. Servidores, segurados, estagiários, colaboradores e prestadores de serviços 26
9.2. Gestor da informação 27
9.3. Gerências 28
9.4. Diretoria Jurídica 29
9.5. Coordenação de Gestão de Pessoas 29
9.6. Diretoria Administrativa-Financeira 29
10. CUMPRIMENTO 30
10.1. Sanções 30
10.2. Legislação aplicável 30

INFORMAÇÕES E CONTATO

João Pessoa

Paraíba Previdência – Paraíba Previdência

Avenida Rio Grande do Sul - Bairro dos Estados

CEP: 58.030-020 - João Pessoa – PB

(83) 2107-1100

Cajazeiras

Av. Cmte. Vital Rolim Shopping

CASA DA CIDADANIA – Centro

58.900-000

(83) 3531-3458

Itaporanga

Estr. do Caravelas, 187,

CASA DA CIDADANIA

58.780-000

(83) 3451-2819

Campina Grande

Rua Dr. Severino Cruz,

Agenor Vasconcelos, 283

CASA DA CIDADANIA – Centro

58.400-258

(83) 3337-5189

Patos

Rua Doutor Pedro Firmino, 265,

Centro, Patos – PB

58.700-070

(83) 3421-1196

Guarabira

Rua Padre Inácio de Almeida, S/N

CASA DA CIDADANIA – Centro

58.200-000

(83) 3271-4245

Horário de Funcionamento

Segunda à Sexta: 8h às 13h

Telefone: (83) 2107 - 1100

Whatsapp: (83) 98130 - 8505.

E-mail do Atendimento: atendimento@pbprev.pb.gov.br

1ª Edição

João Pessoa, 2022

ESTRUTURA ORGANIZACIONAL

Presidente

José Antônio Coêlho Cavalcanti

Diretor Administrativo-Financeiro

Frederico Augusto Cavalcanti Bernardo

Procurador

Paulo Wanderley Câmara

Gerente Previdenciário

Michel Costa Carvalho

Gerente Contábil-Financeiro

Luiz Carlos Júnior

Gerente de Informática

Rivaldo da Silva Júnior

Gerente de Folha de Pagamento

Adriana de Moraes Cordeiro

Coordenador de Concessão de Benefícios

Juliene Jeronimo Vieira Torres

Coordenador de Manutenção de Benefício e Cadastro

Emanuella Maria de Almeida Medeiros

Coordenador de Compensação Previdenciária

Thiago Jesus Marinho Luiz

Coordenador de Programas

Sabrina Rayza Margarete Fernandes Topel

Coordenador Jurídico Administrativo

Clarissa Pereira Leite

Coordenador Jurídico Previdenciário

Camilla Ribeiro Dantas

Coordenador de Orçamento e Execução Financeira

Roberto Brasil Siqueira

Coordenador de Investimentos

Regina Karla Batista Alves

Coordenador de Perícia

Juliana Aquino Teixeira Zorrilla

Coordenador de Controle Interno

Roberto Alves de Melo Filho

Coordenador de Arquivo

Andreza de Morais Batista

Coordenador de Atendimento e Protocolo

Maxmiliano Leite Cavalcanti

Coordenador de Aposentadorias

Mary Stela Pereira da Silva

Coordenador de Pensão

Paulo Ferreira dos Santos Júnior

Coordenador de Gestão de Pessoas

Marilene Felix da Silva

Coordenador de Digitalização

Francisco Rafael Melo Patrício

Ouvidor

Zailton Frederico Beuttenmuller

CONSELHO DE ADMINISTRAÇÃO

Biênio (2020 - 2022)

Representantes PARAÍBA PREVIDÊNCIA (Presidente)

Titular: José Antonio Coêlho Cavalcanti

Suplente: Frederico Augusto Cavalcanti Bernardo

Mandato: Permanente

Representantes Secretaria de Estado da Administração

Titular: Jacqueline Fernandes de Gusmão

Mandato: Permanente

Suplente: Maria das Graças Aquino Teixeira da Rocha

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Poder Legislativo

Titular: Evandro José da Silva

Suplente: Marcélia dos Santos Ferreira

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Poder Judiciário

Titular: Eduardo Faustino Diniz

Suplente: Einstein Roosevelt Leite

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Ministério Público

Titular: Reynaldo Di Lorenzo Serpa Filho

Suplente: Francisco Seraphico Ferraz da Nóbrega Filho

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Tribunal de Contas

Titular: Maria Zaira Chagas Guerra Pontes

Suplente: Ludmilla Costa de Carvalho Frade

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Servidores Militares

Titular: Walter Dias de Araújo Júnior

Suplente: Rômulo Nobre Formiga

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Servidores Civis

Titular: Ruy Ramalho de Freitas

Suplente: Isabella Gondim do Nascimento Aires

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Inativos e Pensionistas

Titular: Uyramir Veloso Castelo Branco

Suplente: Sezenando Ventura Filho

Início Mandato: 19/12/2020 – Fim Mandato: 19/12/2022

Representantes Procuradoria-Geral

Titular: Fábio Andrade Medreiros

Suplente: Lúcio Landim Batista da Costa

Início Mandato: 07/12/2021 – Fim Mandato: 19/12/2022

CONSELHO FISCAL

Biênio (2020 - 2022)

Representantes Civis Ativos (Presidente)

Titular: John Kennedy Ferreira

Suplente: Gleydson Farias Bronzeado

Início Mandato: 19/12/2020

Fim Mandato: 19/12/2022

Representantes Civis Inativos

Titular: Hélida Cavalcanti de Brito

Suplente: Yara Sílvia Mariz Maia Pessoa

Início Mandato: 19/12/2020

Fim Mandato: 19/12/2022

Representantes Militares Ativos

Titular: Hamilton Torres Holmes

Suplente: José Jorge Lopes Xavier Júnior

Início Mandato: 19/12/2020

Fim Mandato: 19/12/2022

Representantes Militares Inativos

Titular: Iremar Clementino Neves

Suplente: Antônio Félix Barbosa

Início Mandato: 19/12/2020

Fim Mandato: 19/12/2022

Representantes Conselho Administrativo

Titular: Maria Zaira Chagas Guerra Pontes

Suplente: Maria das Graças Aquino Teixeira da Rocha

Início Mandato: 19/12/2020

Fim Mandato: 19/12/2022

Representantes Procuradoria-Geral

Titular: Paulo Márcio Soares Madruga

Suplente: Felipe de Brito Lira Souto

Início Mandato: 19/12/2020

Fim Mandato: 19/12/2022

Representantes Procuradoria-Geral

Titular: Paulo Márcio Soares Madruga

Suplente: Felipe de Brito Lira Souto

Início Mandato: 07/12/2021

Fim Mandato: 19/12/2022

Representantes Controladoria Geral

Titular: Aurea Bustorff Feodrippe Quintão

Suplente: Rodolfo Emanuel Lima Serrano

Início Mandato: 07/12/2021

Fim Mandato: 19/12/2022

1. INTRODUÇÃO

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. ”

De acordo com a mesma norma, “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. ”

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

- **Integridade:** somente alterações, supressões e adições que forem autorizadas pela instituição devem ser realizadas nas informações;
- **Confidencialidade:** somente pessoas devidamente autorizadas pela instituição devem ter acesso à informação;
- **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

A violação desta política de segurança é qualquer ato que:

- Exponha a Instituição a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Ainda de acordo com a norma ABNT NBR ISO/IEC 27002:2005, "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio. "

Mediante tal embasamento e considerando o disposto em seu Planejamento Estratégico, a Paraíba Previdência resolve implantar um Sistema de Segurança da Informação (S.S.I.), cuja estrutura e diretrizes são expressas neste documento.

2. OBJETIVO

O presente documento constitui uma declaração formal da Paraíba Previdência acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser observado por todos os seus servidores, segurados, estagiários e prestadores de serviços.

Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação na Instituição, estabelecendo as diretrizes a serem seguidas para implantação e manutenção de um S.S.I., guiando-se, principalmente, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

É dever de todos dentro do Paraíba Previdência:

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a instituição e deve sempre ser tratada profissionalmente.

3. ABRANGÊNCIA

Os documentos que compõem a estrutura normativa são divididos em três categorias:

i. Política (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o Paraíba Previdência decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados;

ii. Normas (nível tático): especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política;

iii. Procedimentos (nível operacional): instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da Paraíba Previdência.

3.1 Divulgação e acesso à estrutura normativa

Os documentos integrantes da estrutura devem ser divulgados a todos os servidores, segurados, estagiários e prestadores de serviços do Paraíba Previdência quando de sua admissão, bem como, através dos meios oficiais de divulgação interna do Paraíba Previdência e, também, publicadas no site da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento.

4. DEFINIÇÕES

Definição dos termos relacionados à segurança da informação:

- **Credencial de acesso:** É o conjunto de usuário e senha, que permite acesso a determinado sistema ou ambiente.
- **Ativo:** Todos os itens da organização onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas.

- **Proxy:** Software de controle de acesso à rede, que pode produzir relatórios sobre os acessos.
- **Backup:** É a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais.
- **Firewall:** É um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- **Spam:** É o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.
- **Log:** Os logs são registros de atividades gerados por programas de computador. No caso de logs relativos aos incidentes de segurança, eles normalmente são gerados por firewalls ou por sistemas de detecção de intrusão.

4.1 Classificação da informação

Define-se como necessária a classificação de toda a informação de propriedade do Paraíba Previdência, de maneira proporcional ao seu valor para a instituição, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

a) **Pública:** É uma informação do Paraíba Previdência ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

b) **Interna:** É uma informação do Paraíba Previdência o qual não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos ao Paraíba Previdência deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da instituição, porém, não com a mesma magnitude de uma informação confidencial ou restrita. Pode ser acessada sem restrições por todos os segurados e prestadores de serviços do Paraíba Previdência.

c) **Confidencial:** É uma informação crítica para os servidores do Paraíba Previdência ou de seus segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, segurados e/ou fornecedores.

d) **Informação Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos à organização e/ou comprometer a estratégia da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

5. REGRAS

5.1 Política de uso da internet

O acesso à internet deverá ser feito seguindo as diretrizes compostas nesta política de segurança, levando em conta os princípios da segurança da informação: Confidencialidade, Integridade, Disponibilidade e Autenticidade. São elas:

i. O acesso à internet será monitorado através de software de monitoramento (Proxy) que registrará as informações de acesso, como sites visitados, horários de visita, quantidade de visitas, arquivos baixados, usuário que acessou, etc.

ii. O usuário não deverá compartilhar sua credencial de acesso ao computador e à internet para terceiros acessarem a internet de sua máquina, caso contrário se responsabilizará pelo acesso indevido.

iii. É vedado o acesso a sites que estejam fora do interesse do instituto, como sites de bate papo, redes sociais, sites com conteúdo ofensivo, racista ou pornográfico e comércio eletrônico.

iv. É vedado o acesso a sites de estrutura duvidosa que ofereçam risco à segurança da informação ou que possuam ferramentas que visem burlar os mecanismos de segurança do Instituto ou ocultar as credenciais de acesso à internet, como navegadores anônimos e proxy anônimo.

v. A critério da administração, sites com conteúdo não pertinente ao trabalho, terão o acesso bloqueado.

vi. O funcionário que fizer mau uso da internet, terá o acesso bloqueado.

5.2 Uso da rede Sem Fio

A utilização da rede sem fio de internet (Wi-Fi) deve ser feita somente por dispositivos autorizados e configurados pela equipe de suporte, do mesmo modo os roteadores sem fio, a utilização das redes sem fio deve ser realizada seguindo as regras dispostas nesta política de segurança da informação.

Em caso de descumprimento desta política ou má utilização do recurso, a equipe de suporte poderá tomar providências, como a suspensão do recurso ou bloqueio da máquina ou usuário na rede sem fio.

5.3 Uso da Rede Cabeada

A utilização da rede cabeada de internet deve ser feita somente por dispositivos autorizados e configurados pela equipe de suporte, estes dispositivos receberão um endereço IP automático e serão configurados para que funcionem de acordo com a política de segurança da Informação.

5.4 Política de Acesso aos Arquivos da Rede

Todos os arquivos deverão ser salvos na rede, nas pastas dos respectivos setores, onde serão realizados Backups periódicos, os arquivos salvos no disco do computador pessoal de trabalho, não terão garantia de recuperação, em caso de pane.

5.5 Política de proteção da informação

Define-se como necessária a proteção das informações da instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, segurado, estagiário ou prestador de serviços do Paraíba Previdência, sendo que:

i. Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do Paraíba Previdência e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade do Paraíba Previdência;
ii. As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;
iii. Assuntos confidenciais não devem ser expostos publicamente;
iv. Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
v. Somente softwares homologados podem ser utilizados no ambiente computacional do Paraíba Previdência;
vi. Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
vii. Todo usuário, para poder acessar dados das redes de computadores do Paraíba Previdência, deverá possuir um código de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;

viii. Não é permitido o compartilhamento de pastas nos computadores de servidores da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

ix. Todos os dados considerados como imprescindíveis aos objetivos do Paraíba Previdência devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos à testes periódicos de recuperação;

5.6 Política de privacidade da informação

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos meios às quais o Paraíba Previdência detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do Paraíba Previdência e reafirmam o seu compromisso com a melhoria contínua desse processo:

i. As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;

ii. As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

iii. As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;

iv. As informações somente são fornecidas a terceiros, mediante autorização prévia da diretoria executiva ou para o atendimento de exigência legal ou regulamentar;

v. As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

5.7 Política de Uso do E-mail

i. O e-mail deverá ser utilizado apenas para os interesses do instituto, não devendo ser utilizado para fins particulares, envio de spams, propaganda, conteúdo impróprio, difamatório, calunioso ou que prejudique a imagem do instituto e seus colaboradores.

ii. O usuário deverá utilizar senha com a complexidade descrita nesta política de segurança e não fornecer sua senha para terceiros sob nenhuma hipótese.

iii. O acesso ao e-mail deverá ser realizado somente através da página de webmail do instituto: http://webmail.pb.gov.br, não devendo ser acessado por outros meios.

iv. A senha será alterada a cada 180 dias de acordo com a definição do controlador de domínio.

v. O usuário não deverá abrir e-mails de origem duvidosa, ou que julgar não pertinentes ao trabalho do instituto, incluindo anexos. Diante de qualquer dúvida deverá entrar em contato com o setor de suporte e mover a mensagem suspeita para a caixa de spam.

5.8 Política de uso dos computadores

i. O acesso aos computadores, sistemas e arquivos da rede do instituto será fornecido através de credenciais de acesso de uso pessoal, a credencial de acesso será composta por login e senha.

ii. A senha deverá ser composta de no mínimo 8 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais.

iii. A senha de acesso aos computadores será alterada a cada 180 dias, de acordo com a definição do controlador de domínio.

iv. Todo computador deverá possuir sistema antivírus instalado, ativo e atualizado que será fornecido, instalado e monitorado pela equipe de suporte.

v. Não deverão ser instalados softwares não homologados pelo setor de TI, softwares piratas, softwares de acesso remoto, softwares para fins que não são do interesse do instituto ou não relacionados com a função do usuário.

vi. Somente a equipe de suporte está autorizada à instalação de softwares de qualquer tipo, devendo ser solicitada para instalação.

vii. Não deverão ser baixados e/ou executados arquivos desconhecidos ou fora do interesse do instituto, que possuam as extensões: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, ou qualquer outra extensão que represente um risco à segurança.

viii. Os computadores poderão ser monitorados e auditados pela equipe de suporte a qualquer tempo, para fim de verificação de conformidade com a política de segurança da informação.

ix. Os computadores terão padronizados: o papel de parede, impressoras, ícones e unidades de rede mapeadas, de acordo com cada setor. Essas configurações serão definidas através do controlador de domínio.

x. O computador deverá ser bloqueado quando o usuário se ausentar do seu setor, mesmo que por breve período de tempo, se o usuário tiver que se ausentar por tempo indeterminado deverá desligar o computador.

xi. Não será fornecida credencial de acesso do tipo Administrador.

5.9 Política de instalação de novos sistemas, aplicativos e/ou equipamentos

O setor de Informática é responsável pela aplicação da Política do Paraíba Previdência em relação à definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas ("softwares") ou de novos

equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

5.10 Política de senha e acesso

A senha de acesso de um novo usuário de qualquer sistema deverá ser requisitada pelo superior imediato do setor, através de e-mail, ou memorando, descrevendo o nome do usuário, os sistemas que serão utilizados e o tipo de acesso a ser fornecido ao usuário.

A senha de acesso aos sistemas e computadores é de uso pessoal e não deve ser compartilhada.

A senha de acesso deve ser composta por no mínimo 8 dígitos, compostos de letras e números.

Após 3 tentativas seguidas de acesso com senha inválida, a senha será bloqueada e o usuário deverá entrar em contato com a equipe de suporte para desbloqueio da senha.

As senhas terão validade de 180 dias, após esse período deverão ser alteradas para uma nova senha.

6. POLÍTICAS DE AUDITORIA E REGISTRO DE LOGS DE ACESSO

6.1. Credenciais de acesso

Serão registrados em logs automáticos, todos os acessos dos usuários aos recursos do instituto, incluindo acesso aos sistemas, criação, exclusão e alteração de arquivos, horário de logon na máquina, utilização de impressora e outros sistemas.

6.2. Arquivos pessoais

Não será permitido a guarda de arquivos pessoais na rede do Instituto, que incluem: Músicas, Imagens, Vídeos e outros arquivos em geral.

6.3. Política de descarte de dados e informações

Os dados e informações do instituto que estejam armazenados em mídias como cd, dvd, disquete, disco rígido, fita de dados ou outro meio digital e os dados registrados em papel, formulários, deverão ser descartados de maneira a preservar a confidencialidade das informações

6.4. Políticas de uso de dispositivos pessoais (celulares, tablets, notebook)

Será permitido o uso de dispositivos pessoais, como notebook, desde que estejam de acordo com as políticas de segurança da Informação do Instituto, após serem avaliados pelo setor de suporte.

Não é permitido trazer equipamento pessoal para que o setor de suporte faça manutenção, instalação de programas ou qualquer outro serviço de caráter pessoal.

6.5. Política de uso de impressoras

A quantidade de impressões, será registrada em Log, e poderá ser auditada quanto ao usuário que imprimiu, quantidade de páginas, nome do arquivo impresso. O uso das impressoras deve ser feito para os interesses do instituto e utilizadas com consciência ecológica.

7. POLÍTICA DE BACKUP E CONTINGÊNCIA

7.1. Procedimentos de backup dos arquivos e bancos de dados

O backup é realizado diariamente, sendo este incremental e realizado de maneira automatizada por script.

O backup dos Bancos de Dados é realizado diariamente e semanalmente, sendo este completo e automatizado.

O backup do sistema gerenciador de documentos (GED) é realizado diariamente, sendo este incremental e automatizado e dividido em 2 tarefas: arquivos e banco de dados.

7.2. Armazenamento dos backups

Os backups são realizados diariamente e armazenados em nuvem diariamente. Os Dados são replicados em duas nuvens distintas.

7.3. Teste de recuperação

Serão realizados testes de recuperação de backup a cada 30 dias.

7.4. Procedimentos de Contingência

Em caso de indisponibilidade dos sistemas ou internet, o instituto, conforme o procedimento de contingência, definido pelo setor de tecnologia da informação, serão utilizados um servidor de contingência, bem como nobreak, switch e internet redundante.

Os procedimentos de contingência serão utilizados somente para os setores e sistemas considerados críticos para o instituto, ou seja, cuja indisponibilidade cause impacto à reputação ou saúde financeira.

8. POLÍTICA DE CONTROLE DE ACESSO À INFRAESTRUTURA

8.1. Regras de acesso ao datacenter

O acesso ao datacenter é restrito aos funcionários do setor de TI, o acesso por terceiros, como prestadores de serviço, deverá sempre ser acompanhado de um funcionário do setor. O mesmo se aplica a funcionários de outros setores do instituto.

O datacenter será monitorado por câmera de segurança.

A porta de acesso ao datacenter deve permanecer fechada, mesmo quando houver funcionários autorizados em suas dependências.

8.2. Bloqueio de acesso a funcionários desligados

O setor de Recursos Humanos deverá informar ao setor de suporte ou à divisão de tecnologia da informação, quando houver o desligamento de funcionários, para que as credenciais de acesso aos sistemas, computadores, e-mail e ambiente de rede, sejam bloqueadas.

8.3. Registro de chamados

Diante de qualquer incidente ou pedido de suporte, deverá ser registrado o pedido ou demanda por ligação para o setor de suporte no ramal 1118 ou 1128.

9. RESPONSABILIDADES

9.1. Servidores, segurados, estagiários, colaboradores e prestadores de serviços

Todo arquivo em mídia proveniente de entidade externa ao Paraíba Previdência deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Cabe aos servidores, estagiários e prestadores de serviços do Paraíba Previdência cumprir com as seguintes obrigações:

a) Zelar continuamente pela proteção das informações da instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada;
b) Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;
c) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
d) Comunicar imediatamente ao setor de Informática qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

9.2. Gestor da informação

O Gestor da Informação é um servidor de TI sugerido pelo gerente de TI e designado pela Diretoria como responsável por um determinado ativo de informação.

Este gestor deve dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade, seja este de propriedade do Paraíba Previdência.

O Gestor da Informação pode delegar sua autoridade sobre o ativo de informação, porém, continua sendo dele a responsabilidade final pela sua proteção.

Compete ao Gestor da Informação:

a) Classificar a informação sob sua responsabilidade, inclusive aquela gerada por servidores, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;
b) Inventariar todos os ativos de informação sob sua responsabilidade;
c) Enviar ao Gerente de TI, quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade. Os modelos de relatórios serão definidos pelo Gerente de TI e aprovados pela Diretoria;

d) Sugerir procedimentos ao Gerente de TI para proteger os ativos de informação, conforme a classificação realizada, além da estabelecida pela Política de Segurança da Informação e pelas Normas de Segurança da Informação;
e) Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;
f) Reavaliar, periodicamente, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;
g) Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

9.3. Gerências

Cabe às Gerências:

a) Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;
b) Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;
c) Sugerir ao Gestor, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
d) Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo Gestor;
e) Comunicar imediatamente ao Gestor eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

9.4. Diretoria Jurídica

Cabe, adicionalmente, à diretoria Jurídica:

a) Manter as áreas do Paraíba Previdência informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;
b) Incluir na análise e elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do Paraíba Previdência;
c) Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

9.5. Coordenação de Gestão de Pessoas

Cabe, adicionalmente, à Gerência de Recursos Humanos:

a) Assegurar-se de que os servidores e estagiários, comprovem, por escrito, estarem cientes da estrutura normativa de segurança e dos documentos que as compõem;
b) Criar mecanismos para informar, antecipadamente aos fatos, alterações no quadro de servidores do Paraíba Previdência.

9.6. Diretoria Administrativa-Financeira

Cabe à Diretoria Executiva:

a) Aprovar a política e as normas de segurança da informação e suas revisões;
b) Nomear os gestores da informação, conforme as indicações do Gerente de TI;
c) Receber, por intermédio do setor de informática, relatórios de violações da Política e das normas de segurança da informação, quando aplicáveis;

d) Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas do setor de informática.

10. CUMPRIMENTO

Diante do descumprimento desta política em geral, o usuário poderá, a qualquer tempo, ser auditado, através da equipe de TI e poderá receber em consequência, a aplicação de ações disciplinares cabíveis que se fizerem necessárias.

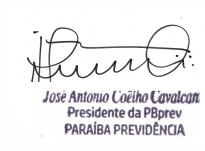
10.1. Sanções

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação do Paraíba Previdência são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

10.2. Legislação aplicável

a) Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);
b) Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);
c) Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);
d) Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);
e) Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
f) Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
g) Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias).

João Pessoa, 27 de março de 2023.



Assinado de forma digital por JOSE ANTONIO COELHO CAVALCANTI:10515097420
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR COPIAR DIGITAL, ou=Presencial, ou=17072702000183, cn=JOSE ANTONIO COELHO CAVALCANTI:10515097420
Dados: 2023.04.03 08:28:22 -03'00'

JOSÉ ANTONIO COÊLHO CAVALCANTI

Presidente da Paraíba Previdência

Assinado de forma digital por RIVALDO DA SILVA JUNIOR:56235267215
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=VALID, ou=AR COPIAR DIGITAL, ou=Presencial, ou=17072702000183, cn=RIVALDO DA SILVA JUNIOR:56235267215
Dados: 2023.04.03 09:30:38 -03'00'

RIVALDO DA SILVA JÚNIOR

Gerente de Tecnologia da Informação da Paraíba Previdência