IPREVI

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE ITATIAIA

MANUAL DE CONTROLE DE ACESSO FÍSICO E LÓGICO

PREFEITURA MUNICIPAL DE ITATIAIA
ESTADO DO RIO DE JANEIRO

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DE ITATIAIA

DIRETORIA EXECUTIVA

DIRETORA PRESIDENTE
ALESSANDRA ARANTES MARQUES

DIRETORA ADMINISTRAÇÃO E FINANÇAS
ISALTINA CÁSSIA DA SILVA ALVIM DIAS

DIRETORA DE BENEFÍCIOS
FLAVIA GONÇALVES CAVALCANTE

IDENTIFICAÇÃO

RAZÃO SOCIAL	INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE ITATIAIA – IPREVI CNPJ: 03.716.646/0001-68
ENDEREÇO	AVENIDA DOS EXPEDICIONÁRIOS, Nº 301, CENTRO - ITATIAIA/RJ CEP: 27580-000
TELEFONE/WHATSAPP	(24) 3352-4043
INSTAGRAM	@IPREVIITATIAIA
FACEBOOK	@IPREVIITATIAIA
SITE OFICIAL	HTTP://WWW.IPREVI.RJ.GOV.BR/
E-MAIL	IPREVI@IPREVI.RJ.GOV.BR

HISTÓRICO DE VERSÕES

TÍTULO	**CONTROLE DE ACESSO FÍSICO E LÓGICO**
VOLUME	I
EDIÇÃO	2ª
APROVADO POR:	DIRETORIA EXECUTIVA
APROVAÇÃO EM:	20/10/2023
INSTRUMENTO DE HOMOLOGAÇÃO	PORTARIA Nº 118/2023
AUTORIA:	MÁRIO LUIZ VERDEIRO FERREIRA
REVISADO POR:	MÁRIO LUIZ VERDEIRO FERREIRA

SUMÁRIO

INTRODUÇÃO

COM O AVANÇO TECNOLÓGICO E SUAS CONSEQUENTES IMPLICAÇÕES, CADA VEZ MAIS AS ROTINAS ADMINISTRATIVAS SE VEEM ATRELADAS AOS INSTRUMENTOS DE TECNOLOGIA DA INFORMAÇÃO, SEJAM ELES NO SENTINDO FÍSICO, NAQUILO QUE SE REFERE A EQUIPAMENTOS E MAQUINÁRIOS, BEM COMO AO AMBIENTE VIRTUAL ONDE AS ATIVIDADES SÃO DESENVOLVIDAS. PORTANTO, TAIS FATORES ASSUMIRAM UMA IMPORTÂNCIA FULCRAL NO DIA-A-DIA DAS ATIVIDADES FUNCIONAIS, SENDO ASSIM SUA PRESERVAÇÃO, MATÉRIA DE REGULAÇÃO POR PARTE DAS INSTITUIÇÕES. DESSA MANEIRA, O PRESENTE MANUAL FOI DESENVOLVIDO NO INTUITO DE ESTABELECER REGRAS QUE NORTEIAM AS ATIVIDADES DE CONTROLE DE ACESSO LÓGICO E SEGURANÇA FÍSICA NO INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE ITATIAIA (IPREVI), DE FORMA A SEREM EFETIVAMENTE CONTROLADOS E EXECUTADOS PELO SETOR DE INFORMÁTICA.

MÁRIO LUIZ VERDEIRO FERREIRA

REDATOR DO MANUAL

CONCEITOS

- **ACESSO**

ATO DE INGRESSAR, TRANSITAR, CONHECER OU CONSULTAR A INFORMAÇÃO, SEJA LOCAL, OU REMOTAMENTE, BEM COMO A POSSIBILIDADE DE USAR OS ATIVOS DE INFORMAÇÃO DE UM ÓRGÃO OU ENTIDADE.

- **ÁREA SEGURA**

SÃO SALAS TRANCADAS OU UM CONJUNTO DE SALAS DENTRO DE UM PERÍMETRO FÍSICO DE SEGURANÇA, QUE PODEM SER TRANCADAS E QUE DISPONHAM DE ARQUIVOS DE AÇO TRANCÁVEIS OU COFRES. A LOCALIZAÇÃO DE UMA ÁREA SEGURA DEVE LEVAR EM CONTA OS RISCOS E VULNERABILIDADES E DEVEM CONTEMPLAR OS REGULAMENTOS E NORMAS RELEVANTES DE SAÚDE E SEGURANÇA E CONSIDERAR EVENTUAIS AMEAÇAS À SEGURANÇA CAUSADAS POR INSTALAÇÕES VIZINHAS, COMO INFILTRAÇÕES, VAZAMENTO DE ÁGUA PROVENIENTE DE OUTRA ÁREA ETC.

- **ATIVOS DE INFORMAÇÃO**

OS MEIOS DE ARMAZENAMENTO, TRANSMISSÃO E PROCESSAMENTO DA INFORMAÇÃO; OS EQUIPAMENTOS NECESSÁRIOS A ISSO; OS SISTEMAS UTILIZADOS PARA TAL; OS LOCAIS ONDE SE ENCONTRAM ESSES MEIOS, E TAMBÉM OS RECURSOS HUMANOS QUE A ELES TÊM ACESSO.

- **BLOQUEIO DE ACESSO**

PROCESSO QUE TEM POR FINALIDADE SUSPENDER TEMPORARIAMENTE O ACESSO.

- **CONTAS DE SERVIÇO**

CONTAS DE ACESSO À REDE CORPORATIVA DE COMPUTADORES NECESSÁRIA A UM

PROCEDIMENTO AUTOMÁTICO (APLICAÇÃO, SCRIPT, ETC.) SEM QUALQUER INTERVENÇÃO HUMANA NO SEU USO.

- **CREDENCIAMENTO DE ACESSO**

PROCESSO PELO QUAL O USUÁRIO RECEBE CREDENCIAIS QUE CONCEDERÃO O ACESSO, INCLUINDO A IDENTIFICAÇÃO, A AUTENTICAÇÃO, O CADASTRAMENTO DE CÓDIGO DE IDENTIFICAÇÃO E DEFINIÇÃO DE PERFIL DE ACESSO EM FUNÇÃO DE AUTORIZAÇÃO PRÉVIA.

- **CREDENCIAIS OU CONTAS DE ACESSO**

IDENTIFICAÇÕES CONCEDIDAS POR AUTORIDADE COMPETENTE APÓS O PROCESSO DE CREDENCIAMENTO DE ACESSO, QUE PERMITAM HABILITAR DETERMINADA PESSOA, SISTEMA OU ORGANIZAÇÃO AO ACESSO. A CREDENCIAL PODE SER FÍSICA, COMO CRACHÁ, CARTÃO, CREDENCIAL BIOMÉTRICA OU LÓGICA COMO IDENTIFICAÇÃO DE USUÁRIO E SENHA.

- **CONTÊINERES DOS ATIVOS DE INFORMAÇÃO**

O CONTÊINER É O LOCAL ONDE "VIVE" O ATIVO DE INFORMAÇÃO, ONDE ESTÁ ARMAZENADO, COMO É TRANSPORTADO OU PROCESSADO.

- **CUSTODIANTE DO ATIVO DE INFORMAÇÃO**

É O RESPONSÁVEL PELOS CONTÊINERES DOS ATIVOS DE INFORMAÇÃO E PELA APLICAÇÃO DOS NÍVEIS DE CONTROLES DE SEGURANÇA EM CONFORMIDADE COM AS EXIGÊNCIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, COMUNICADAS PELOS PROPRIETÁRIOS DOS ATIVOS DE INFORMAÇÃO.

- **EQUIPAMENTOS**

INSTRUMENTOS NECESSÁRIOS PARA DETERMINADA FUNÇÃO.

- **EXCLUSÃO DE D I REITO DE ACESSO**

PROCESSO QUE TEM POR FINALIDADE SUSPENDER DEFINITIVAMENTE O ACESSO.

- **EXCLUSÃO DE CONTA DE ACESSO**

PROCESSO QUE TEM POR FINALIDADE O CANCELAMENTO DO CÓDIGO DE IDENTIFICAÇÃO E DO PERFIL DE ACESSO.

- **GESTÃO DE RISCOS 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 DO ATIVO DE INFORMAÇÃO**

INDIVÍDUO LEGALMENTE INSTITUÍDO POR SUA POSIÇÃO E/OU CARGO, O QUAL É RESPONSÁVEL PRIMÁRIO PELA VIABILIDADE E SOBREVIVÊNCIA DOS ATIVOS DE INFORMAÇÃO.

- **IDENTIFICAÇÃO DO USUÁRIO OU NOME DO USUÁRIO**

FORMA PELA QUAL O USUÁRIO É CONHECIDO NO AMBIENTE DE INFORMÁTICA DO IPREVI. O USUÁRIO RECEBE AS PERMISSÕES DE UTILIZAÇÃO DOS RECURSOS COMPUTACIONAIS EM FUNÇÃO DE SUA IDENTIFICAÇÃO, QUE DEVE SER VALIDADA COM O USO DE UMA SENHA.

- **MENU**

LISTA DE OPÇÕES OU ENTRADAS POSTAS À DISPOSIÇÃO DO USUÁRIO, QUE APARECE NO VÍDEO DE UM TERMINAL DE COMPUTADOR COM AS FUNÇÕES QUE ESTE PODERÁ

REALIZAR POR MEIO DE UM PROGRAMA OU DE UM SOFTWARE.

- **NECESSIDADE DE CONHECER**

CONDIÇÃO PESSOAL, INERENTE AO EFETIVO EXERCÍCIO DE CARGO, FUNÇÃO, EMPREGO OU ATIVIDADE, INDISPENSÁVEL PARA O USUÁRIO TER ACESSO À INFORMAÇÃO, ESPECIALMENTE SE FOR SIGILOSA, BEM COMO O ACESSO AOS ATIVOS DE INFORMAÇÃO.

- **PERFIL DE ACESSO**

CONJUNTO DE ATRIBUTOS DE CADA USUÁRIO, DEFINIDOS PREVIAMENTE COMO NECESSÁRIOS PARA CREDENCIAL DE ACESSO.

- **PERÍMETRO DE SEGURANÇA**

ÁREAS QUE PODEM SER COMPOSTAS POR DIFERENTES DIMENSÕES, EQUIPAMENTOS E TIPOS DE CONTROLE DE ACESSO FÍSICO PARA AS INSTALAÇÕES OU ÁREAS CRÍTICAS. PODEM SER DELIMITADAS POR PAREDES, PORTAS DE ENTRADA CONTROLADAS POR CARTÃO OU BALCÃO DE RECEPÇÃO COM RECEPCIONISTA, ETC.

- **QUEBRA DE SEGURANÇA**

AÇÃO OU OMISSÃO, INTENCIONAL OU ACIDENTAL, QUE RESULTA NO COMPROMETIMENTO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

- **TRATAMENTO DA INFORMAÇÃO**

RECEPÇÃO, PRODUÇÃO, REPRODUÇÃO, UTILIZAÇÃO, ACESSO, TRANSPORTE, TRANSMISSÃO, DISTRIBUIÇÃO, ARMAZENAMENTO, ELIMINAÇÃO E CONTROLE DA INFORMAÇÃO, INCLUSIVE AS SIGILOSAS.

- **USUÁRIO**

QUALQUER SERVIDOR OCUPANTE DE CARGO EFETIVO, CARGO EM COMISSÃO, CEDIDO, PRESTADOR DE SERVIÇO TERCEIRIZADO, ESTAGIÁRIO OU QUALQUER OUTRO INDIVÍDUO QUE TENHA ACESSO, DE FORMA AUTORIZADA, AOS RECURSOS COMPUTACIONAIS DO IPREVI.

SIGLAS UTILIZADAS:

CFTV -CIRCUITO FECHADO DE TELEVISÃO;

CPD -CENTRO DE PROCESSAMENTO DE DADOS;

IPREVI -INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE ITATIAIA;

SIC -SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES;

TIC -TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÕES.

NORMATIVA APLICADA

- GSI IN1 NC7/2014: ESTABELECE DIRETRIZES PARA IMPLEMENTAÇÃO DE CONTROLES DE ACESSO RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NOS ÓRGÃOS E ENTIDADES DE TODA A ADMINISTRAÇÃO PÚBLICA FEDERAL;
- ABNT NBR ISO/IEC 27002:2013: FORNECE DIRETRIZES PARA PRÁTICAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E NORMAS DE SEGURANÇA DA INFORMAÇÃO PARA AS ORGANIZAÇÕES, INCLUINDO A SELEÇÃO, A IMPLEMENTAÇÃO E O GERENCIAMENTO DE CONTROLES, LEVANDO EM CONSIDERAÇÃO OS AMBIENTES DE RISCO DA SEGURANÇA DA INFORMAÇÃO DA ORGANIZAÇÃO;
- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: ESTABELECE ORIENTAÇÕES ESTRATÉGICAS SOBRE AS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES ADOTADAS PARA O CUMPRIMENTO DA MISSÃO E O ALCANCE DA VISÃO DO INSTITUTO.

CONTROLE DE ACESSO LÓGICO- RESPOSABILIDADES GERAIS

O CONTROLE DE ACESSO LÓGICO SE CARACTERIZA PELO CONJUNTO DE PROCEDIMENTOS, RECURSOS E MEIOS UTILIZADOS PELO INSTITUTO COM A FINALIDADE DE CONCEDER OU BLOQUEAR O ACESSO AOS ATIVOS DE INFORMAÇÃO A USUÁRIOS AUTORIZADOS OU NÃO. DESSA MANEIRA, ENVOLVE DIFERENTES ATORES QUE POSSUEM DISTINTOS PAPÉIS E RESPONSABILIDADES DENTRO DESSE CONJUNTO DE FORMA QUE GARANTAM SUA EFETIVIDADE, ESTANDO ESSES ÚLTIMOS DESCRITOS A SEGUIR.

SETOR DE TECNOLOGIA DA INFORMAÇÃO:

- DEFINIR, IMPLEMENTAR E GERENCIAR UM SISTEMA DE CONTROLE DE ACESSO PARA TODOS OS ATIVOS DE INFORMAÇÃO DO IPREVI, NÃO IMPORTANDO SUA LOCALIZAÇÃO FÍSICA;
- PROVER O CONTROLE E A AUTENTICAÇÃO DAS CONEXÕES EXTERNAS DOS USUÁRIOS E VIABILIZAR A SEGURANÇA DA INFORMAÇÃO QUANDO FOR NECESSÁRIA A UTILIZAÇÃO DE COMPUTAÇÃO MÓVEL E DEMAIS RECURSOS DE TRABALHO REMOTO;
- ESTABELECER PROCEDIMENTOS QUE GARANTAM A SEGURANÇA DA INFORMAÇÃO PARA O ACESSO AOS SISTEMAS (LOGON);
- PROVER A SEGURANÇA DA INFORMAÇÃO QUANDO DA UTILIZAÇÃO DE PROGRAMAS UTILITÁRIOS QUE SEJAM CAPAZES DE SOBREPOR OS CONTROLES DOS SISTEMAS E APLICAÇÕES;
- ASSEGURAR QUE O ACESSO À INFORMAÇÃO E ÀS FUNÇÕES DOS SISTEMAS DE APLICAÇÃO, POR PARTE DOS USUÁRIOS, SEJA BASEADO NOS REQUISITOS DE RESTRIÇÃO DE ACESSO DO NEGÓCIO;
- CRIAR CONTAS DE SERVIÇO OBSERVANDO-SE A PREMISSA DO MENOR PRIVILÉGIO POSSÍVEL, OS REQUISITOS DO NEGÓCIO, E O RESULTADO DA ANÁLISE DE RISCO;
- MONITORAR O ACESSO E O USO DOS SISTEMAS PARA OS FINS DESTA NORMA.

GESTOR DO ATIVO DE INFORMAÇÃO:

- DESCREVER O ATIVO DE INFORMAÇÃO;
- DEFINIR AS EXIGÊNCIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO ATIVO DE INFORMAÇÃO;
- DEFINIR PROCEDIMENTOS E CRITÉRIOS DE ACESSO DAS INFORMAÇÕES, OBSERVADOS OS DISPOSITIVOS LEGAIS E REGIMENTAIS RELATIVOS AO SIGILO E A OUTROS REQUISITOS DE CLASSIFICAÇÃO PERTINENTES;
- PROPOR REGRAS ESPECÍFICAS AO USO DAS INFORMAÇÕES;
- INDICAR OS RISCOS QUE PODEM AFETAR OS ATIVOS DE INFORMAÇÃO;
- COMUNICAR AS EXIGÊNCIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO ATIVO DE INFORMAÇÃO A TODOS OS CUSTODIANTES E USUÁRIOS;
- BUSCAR ASSEGURAR-SE DE QUE AS EXIGÊNCIAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES ESTEJAM CUMPRIDAS POR MEIO DE MONITORAMENTO;
- REALIZAR UMA ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO DOS USUÁRIOS, AUTORIZANDO OU NÃO O ACESSO;
- AUTORIZAR O ACESSO ÀS INFORMAÇÕES SOB SUA GESTÃO SOMENTE PARA O PESSOAL BASEADO ESTRITAMENTE NAS NECESSIDADES DE CONHECIMENTO.

CUSTODIANTE DO ATIVO DE INFORMAÇÃO

- MANTER A DISPONIBILIDADE, A INTEGRIDADE, A CONFIDENCIALIDADE E A AUTENTICIDADE DA INFORMAÇÃO, DE ACORDO COM OS REQUISITOS DE SEGURANÇA E OS DIREITOS DE ACESSO DEFINIDO PELO GESTOR DA INFORMAÇÃO.

USUÁRIOS:

- ZELAR PELA INTEGRIDADE E CONFIDENCIALIDADE DE SUAS CREDENCIAIS DE ACESSO AOS RECURSOS COMPUTACIONAIS DO IPREVI (IDENTIFICAÇÃO DE USUÁRIO E SENHA);
- ZELAR E CONTRIBUIR PARA UM EFETIVO CONTROLE DE ACESSO AOS RECURSOS COMPUTACIONAIS DO IPREVI, DE FORMA A PREVENIR O ACESSO NÃO AUTORIZADO AOS ATIVOS INFORMACIONAIS E EVITAR O COMPROMETIMENTO OU FURTO DA INFORMAÇÃO E DOS RECURSOS DE PROCESSAMENTO DA INFORMAÇÃO;
- ZELAR PELA SEGURANÇA DA INFORMAÇÃO AO UTILIZAR COMPUTAÇÃO MÓVEL E DEMAIS RECURSOS DE TRABALHO REMOTO.

CONTROLE DE ACESSO LÓGICO-ETAPAS E PROCEDIMENTOS

O PROCESSO DE CONCESSÃO DE CREDENCIAIS DE ACESSO AOS ATIVOS DE INFORMAÇÃO DO IPREVI DEVE LEVAR EM CONTA OS RESULTADOS DA ANÁLISE DE RISCO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES E O PROCESSO DE CONCESSÃO DE ACESSO À INFORMAÇÃO DEVE LEVAR EM CONTA A AUTENTICIDADE DESSAS CREDENCIAIS DE ACESSO.

ASSIM, O PROCESSO DE CONCESSÃO E CONTROLE DO ACESSO LÓGICO, NÃO IMPORTANDO SUA LOCALIZAÇÃO FÍSICA, SERÁ ORIENTADO PELOS SEGUINTES REQUISITOS A SEREM CUMPRIDOS DURANTE TODA SUA EXECUÇÃO PELO SETOR DE TECNOLOGIA DA INFORMAÇÃO:

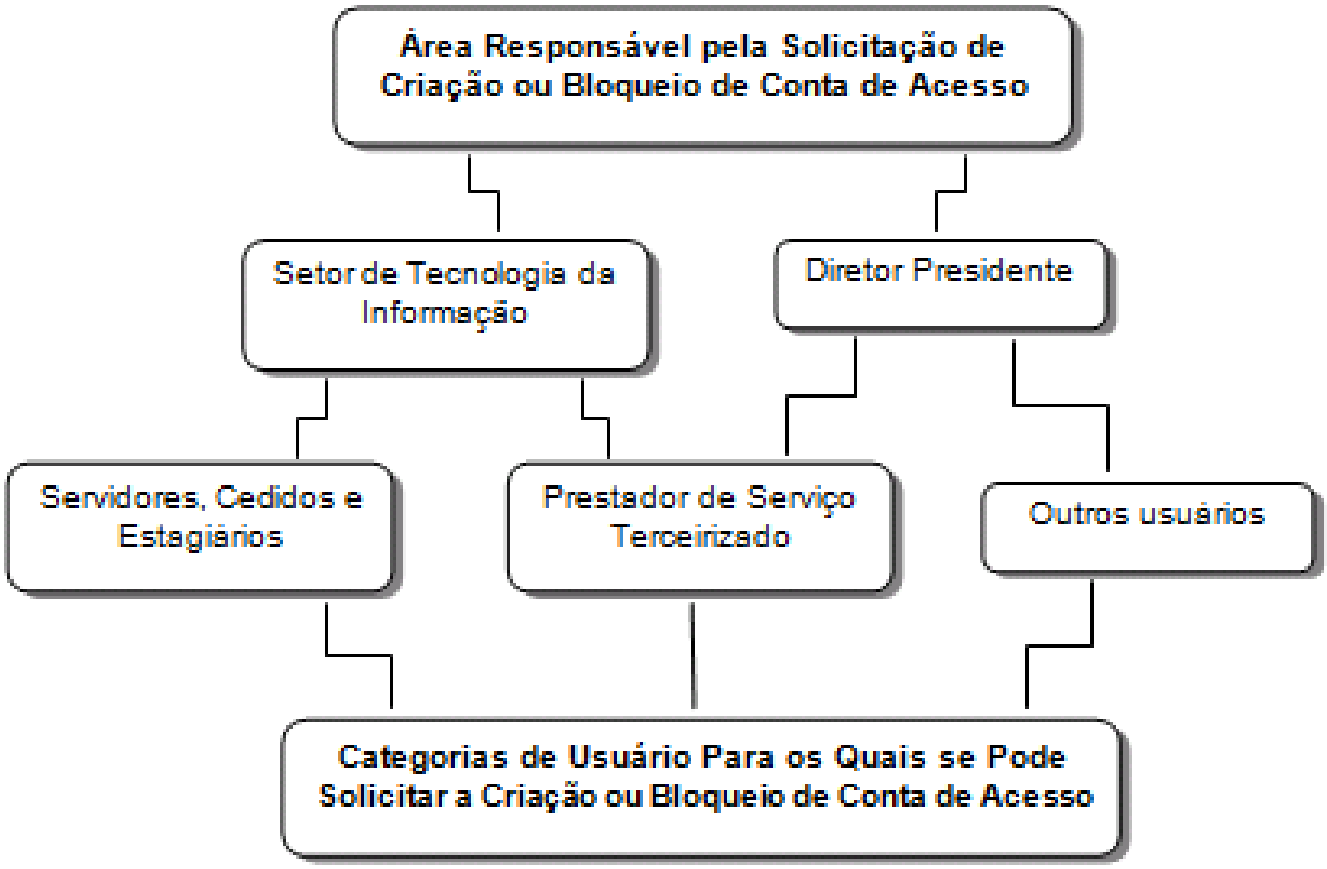
- POSSIBILITAR O GERENCIAMENTO DO DIREITO DE ACESSO AOS DIVERSOS ATIVOS DE INFORMAÇÃO;
- CONCEDER OS DIREITOS DE USO EXCLUSIVAMENTE CONFORME A NECESSIDADE;
- ESTABELECER E MANTER UM PROCESSO DE AUTORIZAÇÃO E REGISTRO DE TODOS OS DIREITOS DE ACESSO CONCEDIDOS;
- CONTEMPLAR O TREINAMENTO DOS USUÁRIOS QUANTO ÀS BOAS PRÁTICAS DE SEGURANÇA NA SELEÇÃO E USO DE SENHAS;
- GARANTIR QUE AS SENHAS DOS USUÁRIOS DOS RECURSOS COMPUTACIONAIS DO IPREVI, QUANDO DIGITADAS, NÃO SEJAM MOSTRADAS NA TELA DE SEUS RESPECTIVOS COMPUTADORES; GARANTIR QUE AS
- SENHAS SEJAM ARMAZENADAS DE FORMA SEGURA, POR MEIO DE CRIPTOGRAFIA, NÃO PERMITINDO A LEITURA DAS MESMAS;
- ALTERAR AS SENHAS PADRÕES DEFINIDAS PELOS FABRICANTES DE EQUIPAMENTOS PROGRAMÁVEIS OU CONFIGURÁVEIS, TÃO LOGO O EQUIPAMENTO TENHA SIDO ENERGIZADO;
- PERMITIR O ACESSO SOMENTE COM OS PROCEDIMENTOS DE AUTORIZAÇÃO CONCLUÍDOS;

- ATUALIZAR O DIREITO DE ACESSO DE USUÁRIOS QUE TENHAM MUDADO DE FUNÇÃO OU BLOQUEAR O DIREITO DE ACESSO DE USUÁRIOS QUE TENHAM CESSADO O VÍNCULO COM O IPREVI;
- ESTABELECER PROCEDIMENTOS PARA A PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO CONTRA SOFTWARE MALICIOSO;
- PREVER A REALIZAÇÃO DE AUDITORIA E MONITORAÇÃO DA SEGURANÇA;

1º PROCEDIMENTO: CONCESSÃO DE ACESSO LÓGICO NO LOCAL

- **1ª ETAPA: SOLICITAÇÃO PELO REQUERENTE**

A SOLICITAÇÃO PARA CRIAÇÃO OU BLOQUEIO DE CONTAS DE ACESSOS DE USUÁRIOS, QUANDO DO INÍCIO OU TÉRMINO DA PRESTAÇÃO DE SERVIÇO, PODE SER REALIZADA PELAS ÁREAS DO QUADRO ABAIXO.



- **2ª ETAPA: CRIAÇÃO OU BLOQUEIO DE CONTA DE ACESSO**

A CRIAÇÃO DE CONTAS DE ACESSO AOS ATIVOS DE INFORMAÇÃO REQUER PROCEDIMENTOS PRÉVIOS DE CREDENCIAMENTO DE ACESSO PARA QUALQUER USUÁRIO. PORTANTO, ANALISADA A DEMANDA, O SERVIDOR RESPONSÁVEL IRÁ PROCEDER A CRIAÇÃO OU O BLOQUEIO DO ACESSO.

- **3ª ETAPA: MANUTENÇÃO PELO USUÁRIO – INTEGRIDADE E CONFIDENCIALIDADE DAS CREDENCIAIS DE ACESSO**

UMA VEZ COM O ACESSO CONCEDIDO, A FIM DE ZELAR PELA INTEGRIDADE E CONFIDENCIALIDADE DE SUAS CREDENCIAIS DE ACESSO E EFETIVAMENTE CONTRIBUIR PARA A EFETIVA GESTÃO DO CONTROLE DE ACESSO AOS RECURSOS COMPUTACIONAIS E INFORMACIONAIS DO IPREVI, O USUÁRIO DEVE SEGUIR AS SEGUINTES REGRAS:

- MANTER A CONFIDENCIALIDADE DE SUA SENHA PESSOAL;
- TROCAR DE SENHA NA PRIMEIRA VEZ QUE UTILIZAR A CONTA DE ACESSO AOS SISTEMAS; SOLICITAR UMA NOVA SENHA, QUANDO DO ESQUECIMENTO;
- EVITAR O REGISTRO DAS SENHAS EM QUALQUER MEIO;
- ALTERAR A SENHA SEMPRE QUE EXISTIR QUALQUER INDICAÇÃO DE POSSÍVEL COMPROMETIMENTO DE SUA CONFIDENCIALIDADE;
- CRIAR SENHAS QUE SEJAM FÁCEIS DE LEMBRAR, MAS QUE NÃO SEJAM BASEADAS EM ELEMENTOS QUE OUTRAS PESSOAS OU POSSÍVEIS INVASORES POSSAM FACILMENTE ADIVINHAR, OU DEDUZIR, A PARTIR DE INFORMAÇÕES PESSOAIS, COMO, POR EXEMPLO:
    - NOME DO USUÁRIO;
    - IDENTIFICADOR DO USUÁRIO (ID), MESMO QUE SEUS CARACTERES ESTEJAM EMBARALHADOS;

- NOME DE MEMBROS DE SUA FAMÍLIA OU DE AMIGOS ÍNTIMOS;
  NOME DE PESSOAS OU LUGARES EM GERAL;
- NOME DO SISTEMA OPERACIONAL OU DA MÁQUINA QUE ESTÁ SENDO UTILIZADA;
- DATAS SIGNIFICATIVAS, COMO A DO NASCIMENTO PRÓPRIO, DE UM FILHO, ESPOSA, ETC.;
- NÚMEROS DE TELEFONE, DE CARTÃO DE CRÉDITO, DE CARTEIRA DE IDENTIDADE OU DE OUTROS DOCUMENTOS PESSOAIS;
- PLACAS OU MARCAS DE VEÍCULOS;
- PALAVRAS QUE CONSTAM DE DICIONÁRIOS EM QUALQUER IDIOMA;
- LETRAS OU NÚMEROS REPETIDOS.

- ALTERAR A SENHA EM I NTERVALOS REGULARES E EVITAR A REUTILIZAÇÃO DE SENHAS ANTIGAS;
- ESCOLHER SUAS PRÓPRIAS SENHAS;
- SELECIONAR SENHAS DE BOA QUALIDADE, EVITANDO O USO DE SENHAS MUITO CURTAS OU MUITO LONGAS, QUE O OBRIGUE A REGISTRÁ- LA EM QUALQUER OUTRO MEIO PARA NÃO SEREM ESQUECIDAS;
- ENCERRAR AS SESSÕES ATIVAS OU UTILIZAR- SE DO MECANISMO DE BLOQUEIO DE ACESSO (TELA DE PROTEÇÃO COM SENHA) QUANDO PRECISAR SE AFASTAR DOS EQUIPAMENTOS.

É VEDADO A TODO USUÁRIO:

- INCLUIR SENHAS EM PROCESSOS AUTOMÁTICOS DE ACESSO A SISTEMAS, POR EXEMPLO, ARMAZENADAS EM MACROS OU NOS NAVEGADORES DA WEB;
- REVELAR CREDENCIAIS DE ACESSO OU PERMITIR O ACESSO A ATIVOS DE INFORMAÇÃO POR TERCEIROS NÃO AUTORIZADOS POR MEIO DESSAS CREDENCIAIS.

4ª ETAPA: ANÁLISE CRÍTICA DO DIREITO DE ACESSO

CONFORME ESPECIFICADO EM PROCEDIMENTO PRÓPRIO, O SERVIDOR RESPONSÁVEL IRÁ REALIZAR A CADA 6 (SEIS) MESES UMA ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO DO USUÁRIO AOS ATIVOS DE INFORMAÇÃO SOB SUA GESTÃO. NOS CASOS DE ATIVOS DE INFORMAÇÕES SIGILOSAS, ESTA ANÁLISE DEVE SER FEITA A CADA 3 (TRÊS) MESES.

2º TIPO DE PROCEDIMENTO: CONCESSÃO DE ACESSO LÓGICO REMOTO

PARA ALÉM DOS REQUISITOS JÁ ESTABELECIDOS, A FIM DE PROVER O CONTROLE E A AUTENTICAÇÃO DO ACESSO REMOTO PELO USUÁRIO, E VIABILIZAR A SEGURANÇA DA INFORMAÇÃO, QUANDO FOR NECESSÁRIA A UTILIZAÇÃO DE COMPUTAÇÃO MÓVEL E DEMAIS RECURSOS DE TRABALHO REMOTO, É NECESSÁRIO AO SETOR DE TECNOLOGIA DA INFORMAÇÃO:

- DETERMINAR O NÍVEL DE PROTEÇÃO E O MÉTODO DE AUTENTICAÇÃO REQUERIDO SOMENTE APÓS UMA AVALIAÇÃO DE RISCO;
- PROVER RECURSOS DE CRIPTOGRAFIA PARA O ACESSO REMOTO DO USUÁRIO;
- ESTABELECER PROTEÇÕES PARA EVITAR O ACESSO NÃO AUTORIZADO OU A DIVULGAÇÃO DE INFORMAÇÕES ARMAZENADAS E PROCESSADAS NOS RECURSOS MÓVEIS;
- CRIAR E MANTER PROTEÇÃO ADEQUADA CONTRA PERDA, FURTO OU ROUBO DE INFORMAÇÕES; CASO UMA DESSAS SITUAÇÕES OCORRA, DEVE SER POSSÍVEL EXECUTAR A RECUPERAÇÃO RÁPIDA E FÁCIL DAS INFORMAÇÕES;
- EFETUAR TREINAMENTO ESPECIALMENTE DIRECIONADO À SEGURANÇA E UTILIZAÇÃO DE EQUIPAMENTOS MÓVEIS, AOS RESPECTIVOS USUÁRIOS;

- PERMITIR O ACESSO REMOTO AOS RECURSOS COMPUTACIONAIS DA REDE DO IPREVI SOMENTE APÓS AUTORIZAÇÃO DO RESPONSÁVEL PELO USUÁRIO SOLICITANTE;
- PROVISIONAR EQUIPAMENTO DE COMUNICAÇÃO APROPRIADO QUE INCLUA MÉTODOS SEGUROS DE ACESSO REMOTO;
- REVOGAR OS DIREITOS DE ACESSO REMOTO QUANDO CESSAREM AS ATIVIDADES DE TRABALHO REMOTO;
- PROTEGER COMPUTADORES E SISTEMAS DE COMUNICAÇÃO QUE ESTEJAM INSTALADOS COM RECURSOS QUE PERMITEM O DIAGNÓSTICO REMOTO PARA MANUTENÇÃO;
- VERIFICAR A REAL NECESSIDADE DE INTERLIGAÇÃO OU COMPARTILHAMENTO DE RECURSOS DE REDE E DE PROCESSAMENTO DE INFORMAÇÕES ENTRE PARCEIROS DE NEGÓCIOS;
- IMPLEMENTAR UM SISTEMA DE AUTENTICAÇÃO DOS EQUIPAMENTOS QUE PODEM TER ACESSO ÀS FACILIDADES DE COMUNICAÇÃO DE REDE.

1 ª ETAPA: SOLICITAÇÃO PELO REQUERENTE

2 ª ETAPA: CRIAÇÃO OU BLOQUEIO DE CONTA DE ACESSO

3 ª ETAPA: MANUTENÇÃO PELO USUÁRIO - ACESSO E UTILIZAÇÃO DE COMPUTAÇÃO MÓVEL

UMA VEZ CONCEDIDO O ACESSO, PARA V I ABILIZAR A SEGURANÇA DA INFORMAÇÃO AO ACESSAR E UTILIZAR COMPUTAÇÃO MÓVEL E DEMAIS RECURSOS DE TRABALHO REMOTO, O USUÁRIODEVE:

- EFETUAR O ACESSO REMOTO ÀS INFORMAÇÕES DO NEGÓCIO, PELA INTERNET, UTILIZANDO- SE DOS RECURSOS DE COMPUTAÇÃO MÓVEL DA INSTITUIÇÃO, APÓS O PROCESSO DE I DENTIFICAÇÃO E AUTENTICAÇÃO BEM- SUCEDIDO E COM OS MECANISMOS DE CONTROLE DE ACESSO APROPRIADOS;
- EVITAR AO MÁXIMO O ACESSO À REDE DE COMUNICAÇÃO DO IPREVI A PARTIR DE EQUIPAMENTO DE TERCEIROS;

- LEVAR EM CONTA A AMEAÇA DE ACESSO NÃO AUTORIZADO À INFORMAÇÃO, OU AOS RECURSOS INFORMACIONAIS SOB SUA RESPONSABILIDADE, POR OUTRAS PESSOAS NA RESIDÊNCIA OU LOCAL DE TRABALHO REMOTO;
- EFETUAR O PROCESSO CORRETO DE DESCONEXÃO QUANDO CONECTADO A PARTIR DE UM COMPUTADOR REMOTO.

4 ª ETAPA: ANÁLISE CRÍTICA DO DIREITO DE ACESSO

CONFORME ESPECIFICADO EM PROCEDIMENTO PRÓPRIO, O SERVIDOR RESPONSÁVEL IRÁ REALIZARA CADA 6 (SEIS) MESES UMA ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO DO USUÁRIO AOS ATIVOS DE INFORMAÇÃO SOB SUA GESTÃO. NOS CASOS DE ATIVOS DE INFORMAÇÕES SIGILOSAS, ESTA ANÁLISE DEVE SER FEITA A CADA 3 (TRÊS) MESES.

3º TIPO DE PROCEDIMENTO: UTILIZAÇÃO DE PROGRAMAS UTILITÁRIOS

COM O OBJETIVO DE PROVER A SEGURANÇA DA INFORMAÇÃO, QUANDO DA UTILIZAÇÃO DE PROGRAMAS UTILITÁRIOS QUE SEJAM CAPAZES DE SOBREPOR OS CONTROLES DOS SISTEMAS E APLICAÇÕES, DEVE-SE:

- UTILIZAR PROCEDIMENTOS DE AUTENTICAÇÃO PARA UTILITÁRIOS DE SISTEMA;
- LIMITAR A UTILIZAÇÃO DOS UTILITÁRIOS DE SISTEMAS A UM NÚMERO MÍNIMO DE USUÁRIOSCONFIÁVEIS E AUTORIZADOS;
- EFETUAR O REGISTRO DE CADA USO DOS UTILITÁRIOS DE SISTEMA;
- DEFINIR E DOCUMENTAR TODOS OS NÍVEIS DE AUTORIZAÇÃO NECESSÁRIOS PARA OS UTILITÁRIOS DE SISTEMA;
- REMOVER TODOS OS SOFTWARES UTILITÁRIOS E DEMAIS SISTEMAS DESNECESSÁRIOS.

4º TIPO DE PROCEDIMENTO: EXCLUSÃO DE CONTA DE ACESSO

A EXCLUSÃO DE CONTA DE ACESSO DE UM USUÁRIO SOMENTE PODERÁ SER EXECUTADA CASO SUA IDENTIFICAÇÃO NÃO TENHA SIDO CRIADA CORRETAMENTE E NÃO EXISTAM REGISTROS DE LOGS GERADOS PELOS ACESSOS AOS ATIVOS DE INFORMAÇÃO DA ORGANIZAÇÃO. CASO TENHA OCORRIDO PELO MENOS UM REGISTRO DE ACESSO AOS ATIVOS DE INFORMAÇÃO, A CONTA DE ACESSO DEVE SER BLOQUEADA INDEFINIDAMENTE.

5º TIPO DE PROCEDIMENTO: ANÁLISE CRÍTICA DO DIREITO DE ACESSO

CABE AO GESTOR DA INFORMAÇÃO REALIZAR A CADA 6 (SEIS) MESES UMA ANÁLISE CRÍTICA DOS DIREITOS DE ACESSO DO USUÁRIO AOS ATIVOS DE INFORMAÇÃO SOB SUA GESTÃO. NOS CASOS DE ATIVOS DE INFORMAÇÕES SIGILOSOS, ESTA ANÁLISE DEVE SER FEITA A CADA 3 (TRÊS) MESES.

6º TIPO DE PROCEDIMENTO: RESTRIÇÃO DE ACESSO DO NEGÓCIO

A FIM DE ASSEGURAR QUE O ACESSO À INFORMAÇÃO E ÀS FUNÇÕES DOS SISTEMAS DE APLICAÇÃO, POR PARTE DOS USUÁRIOS, SEJA BASEADO NOS REQUISITOS DE RESTRIÇÃO DE ACESSO DO NEGÓCIO E DOS RESPECTIVOS SISTEMAS E SERVIÇOS, OS SISTEMAS APLICATIVOS DEVEM CONTEMPLAR AS SEGUINTES REGRAS:

- FORNECER MENUS PARA CONTROLAR O ACESSO ÀS FUNÇÕES DOS SISTEMAS DE APLICAÇÃO;
- RESTRINGIR O CONHECIMENTO DE INFORMAÇÕES OU FUNÇÕES DA APLICAÇÃO AS QUAIS O USUÁRIO NÃO TEM AUTORIZAÇÃO DE ACESSO, POR MEIO DA ELABORAÇÃO DE MANUAIS DE UTILIZAÇÃO DE SISTEMAS DE APLICAÇÃO DIRECIONADOS ÀS NECESSIDADES DO USUÁRIO;
- CONTROLAR OS DIREITOS DOS USUÁRIOS DE LEITURA, ESCRITA, DELEÇÃO E EXECUÇÃO;
- ASSEGURAR QUE AS SAÍDAS DOS SISTEMAS DE APLICAÇÃO QUE TRATAM INFORMAÇÕES

SENSÍVEIS CONTENHAM SOMENTE INFORMAÇÕES RELEVANTES A ESSAS SAÍDAS E SEJAM ENVIADAS PARA TERMINAIS E LOCAIS AUTORIZADOS.

SEGURANÇA FÍSICA-RESPONSABILIDADES GERAIS

A SEGURANÇA FÍSICA DISPÕE SOBRE A IMPORTÂNCIA DA PREVENÇÃO CONTRA O ACESSO FÍSICO NÃO AUTORIZADO QUE PODE CAUSAR DANOS E INTERFERÊNCIAS COM AS INSTALAÇÕES EINFORMAÇÕES DO INSTITUTO. DESSA MANEIRA, ENVOLVE DIFERENTES ATORES QUE POSSUEM DISTINTOS PAPÉIS E RESPONSABILIDADES DENTRO DESSE CONJUNTO DE FORMA QUE GARANTAM SUA EFETIVIDADE, ESTANDO ESSES ÚLTIMOS DESCRITOS A SEGUIR.

TODOS OS SETORES DO INSTITUTO

- PREVENIR O ACESSO NÃO AUTORIZADO, DANO OU INTERFERÊNCIA ÀS INSTALAÇÕES FÍSICAS DO IPREVI;
- PROTEGER AS ÁREAS E PERÍMETROS DE SEGURANÇA INTERNOS POR CONTROLES DE ENTRADA APROPRIADOS;
- ZELAR PELA SEGURANÇA PATRIMONIAL DO INSTITUTO, PARTICULARMENTE QUANDO DA PRESENÇA DE TERCEIROS NAS DEPENDÊNCIAS DO INSTITUTO.

SETOR DE TECNOLOGIA DA INFORMAÇÃO - STI

- PROVER O SUPORTE DE TIC NA IMPLEMENTAÇÃO DAS REGRAS DE SEGURANÇA FÍSICA.

GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - GSIC

- ESTABELECER OS REQUISITOS DE SEGURANÇA FÍSICA NECESSÁRIOS A GARANTIR A SIC;
- MONITORAR CONTINUAMENTE A EFICIÊNCIA E EFETIVIDADE DAS MEDIDAS DE SEGURANÇAFÍSICA QUE AFETAM A SIC.

USUÁRIOS

- UTILIZAR CREDENCIAL DE ACESSO FÍSICO OSTENSIVO (CRACHÁ) EM LOCAL VISÍVEL QUANDONAS DEPENDÊNCIAS DO INSTITUTO;
- ZELAR PELA PROTEÇÃO E PRESERVAÇÃO DAS INSTALAÇÕES FÍSICAS DO INSTITUTO.

SEGURANÇA FÍSICA-ETAPAS E PROCEDIMENTOS

1º PROCEDIMENTOS: ACESSO ÀS INSTALAÇÕES

AO ADENTRAR AS INSTALAÇÕES DO INSTITUTO E DURANTE TODO O TEMPO EM QUE NELA PERMANECER, O SERVIDOR DO IPREVI, PESSOAL TERCEIRIZADO OU OUTRO COLABORADOR CONVENIADO DEVE PORTAR SUA CREDENCIAL DE ACESSO (CRACHÁ) EM LOCAL VISÍVEL.

OS VISITANTES DEVEM SE IDENTIFICAR NA ÁREA DO PROTOCOLO E MANIFESTAR SUA SOLICITAÇÃO PARA QUE SEJAM DEVIDAMENTE ATENDIDOS.

OS SERVIDORES DO IPREVI DEVEM INTERPELAR QUALQUER PESSOA ESTRANHA QUE NÃO ESTEJA ACOMPANHADA E QUALQUER PESSOA QUE NÃO ESTEJA USANDO UMA IDENTIFICAÇÃO VISÍVEL PARA SABER SE A MESMA ESTÁ PERDIDA, ENCAMINHANDO-A A ÁREA DE PROTOCOLO CASO NÃO ESTEJA SOB ATENDIMENTO NA DEPENDÊNCIA QUE ESTIVER LOCALIZADA.

A FIM DE PREVENIR O ACESSO NÃO AUTORIZADO, DANO OU INTERFERÊNCIA ÀS INFORMAÇÕES E I NSTALAÇÕES FÍSICAS DO IPREVI, DEVE-SE TOMAR AS SEGUINTES MEDIDAS:

- SITUAR AS ÁREAS CRÍTICAS OU SENSÍVEIS DO INSTITUTO EM LOCAIS SEGUROS COM PERÍMETRO DE SEGURANÇA DEFINIDO, ASSIM COMO MANTER BARREIRAS DE SEGURANÇA E CONTROLES DEENTRADA APROPRIADOS EM VOLTA DESSAS ÁREAS;
- LEVAR EM CONSIDERAÇÃO OS RISCOS IDENTIFICADOS NA DEFINIÇÃO DO GRAU DE PROTEÇÃO DOS PERÍMETROS DE SEGURANÇA E DEMAIS INSTALAÇÕES FÍSICAS DO INSTITUTO;
- VERIFICAR A EXISTÊNCIA DE FALHAS DE SEGURANÇA NO PERÍMETRO OU ÁREAS CRÍTICAS QUE PERMITAM O COMPROMETIMENTO DA SEGURANÇA FÍSICA;
- PROTEGER DEVIDAMENTE AS PORTAS EXTERNAS CONTRA O ACESSO NÃO AUTORIZADO, COM MECANISMOS DE CONTROLE, BARRAS, ALARMES, FECHADURAS E ETC;

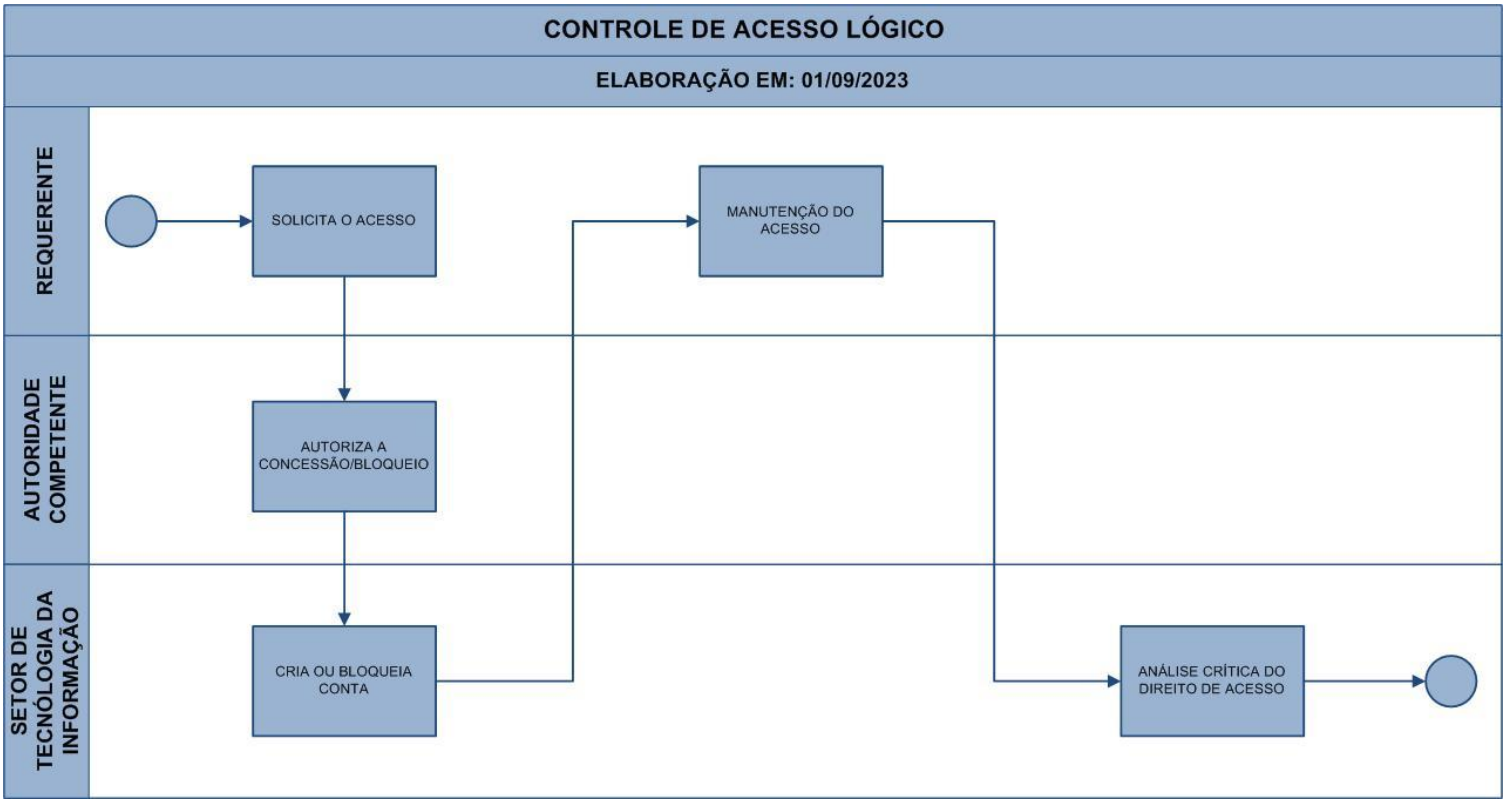
- GARANTIR QUE O ACESSO AO INSTITUTO SOMENTE OCORRA COM PESSOAL EXPRESSAMENTE AUTORIZADO;
- CONTROLAR E RESTRINGIR O ACESSO FÍSICO ÀS ÁREAS DE ARMAZENAMENTO DE INFORMAÇÕESE ÀS INSTALAÇÕES DE EQUIPAMENTOS SENSÍVEIS SOMENTE A PESSOAL AUTORIZADO;
- MONITORAR A UTILIZAÇÃO, POR PARTE DOS USUÁRIOS, DA CREDENCIAL DE ACESSO FÍSI CO (CRACHÁ) EM LOCAL VISÍVEL;
- REVER E ATUALIZAR REGULARMENTE OS DIREITOS DE ACESSO A ÁREAS CRÍTICAS E SENSÍVEIS; PERMITIR ATIVIDADES DE TERCEIROS SOMENTE QUANDO AUTORIZADO E A ATIVIDADE POSSA SER MONITORADA POR SERVIDOR DO QUADRO PRÓPRIO DO INSTITUTO;
- TRANCAR E INSPECIONAR PERIODICAMENTE AS ÁREAS DESOCUPADAS;
- CRIAR BARREIRAS E PERÍMETROS ADICIONAIS DE CONTROLE DE ACESSO FÍSICO ENTRE ÁREAS COM DIFERENTES REQUISITOS DE SEGURANÇA DENTRO DO PERÍMETRO DE SEGURANÇA;
- PROIBIR A PRESENÇA DE EQUIPAMENTO FOTOGRÁFICO, DE VÍDEO, ÁUDIO OU GRAVAÇÃO, A NÃO SER COM AUTORIZAÇÃO.

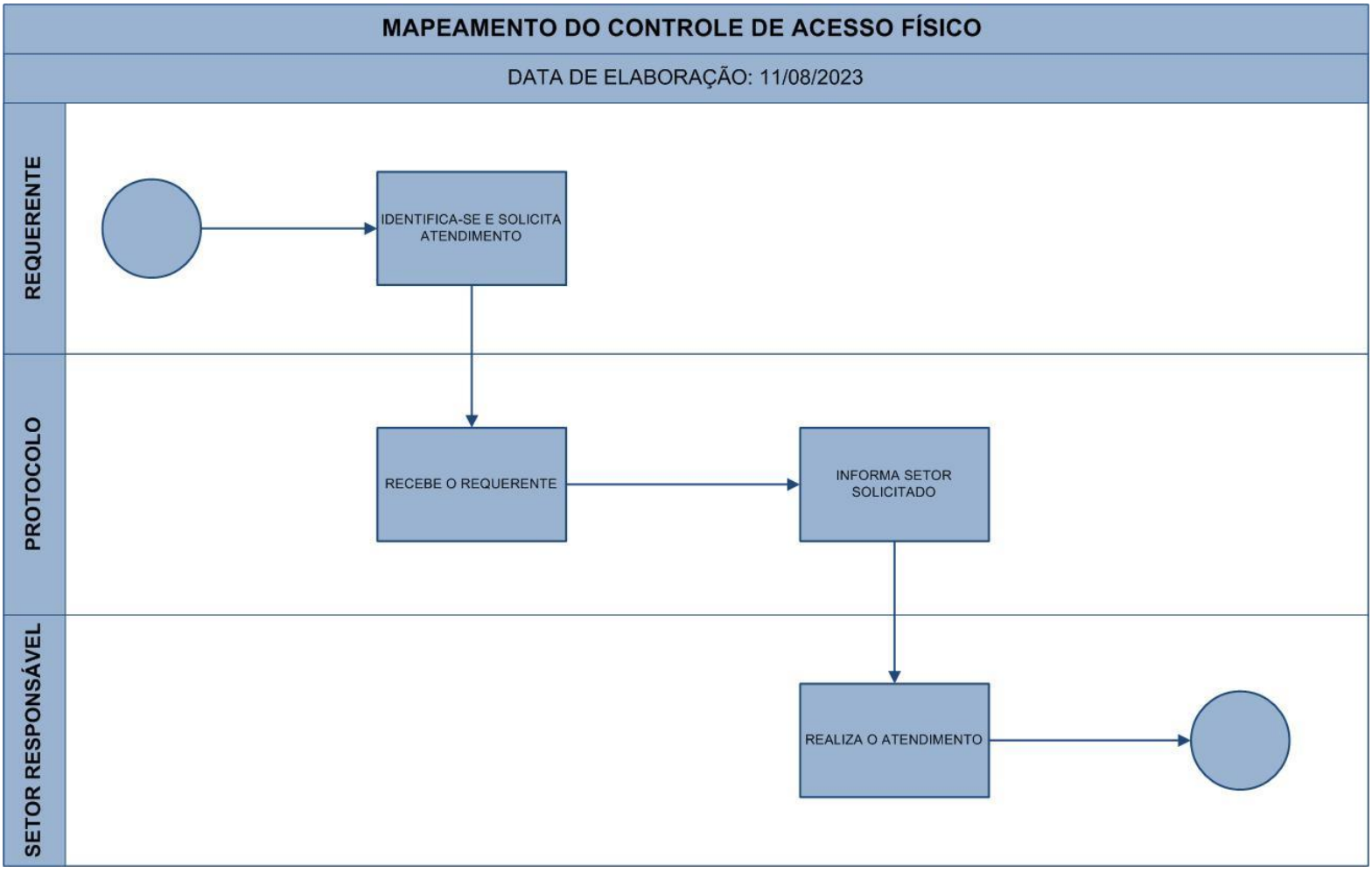
2º PROCEDIMENTO: REALIZAÇÃO DE ENTREGAS E CARREGAMENTOS

DEVEM-SE ESCOLHER ÁREA DE ARMAZENAGEM PROVISÓRIA (QUANDO PERTINENTE) DE FORMAQUE OS MATERIAIS POSSAM SER DESCARREGADOS/CARREGADOS SEM QUE O PESSOAL EXTERNO TENHA ACESSO INDEVIDO ÀS DEPENDÊNCIAS DA AUTARQUIA.

TODO O MATERIAL RECEBIDO/EXPEDIDO DEVE SER REGISTRADO AO DAR ENTRADA/SAÍDA NO INSTITUTO.

MAPEAMENTOS




MAPEAMENTO DO CONTROLE DE ACESSO FÍSICO
DATA DE ELABORAÇÃO: 11/08/2023
REQUERENTE
PROTOCOLO
SETOR RESPONSÁVEL
IDENTIFICA-SE E SOLICITA ATENDIMENTO
RECEBE O REQUERENTE
INFORMA SETOR SOLICITADO
REALIZA O ATENDIMENTO