

	<b>GOIANIAPREV - Instituto de Previdência dos Servidores do Município de Goiânia</b>  <b>PG – Procedimento de Gestão</b>	DATA: 20/03/2024 <b>VERSÃO: 01</b>
<b>TI - Gerenciamento da Segurança da Informação</b>		

## 1. OBJETIVO

Padronizar o processo de **Gerenciamento da Segurança da Informação** do **Instituto de Previdência dos Servidores do Município de Goiânia – GOIANIAPREV**, visando estabelecer as diretrizes estratégicas previstas na Política de Segurança da Informação e definir procedimentos de contingência.

## 2. ABRANGÊNCIA

- **ÁREAS GOIANIAPREV**
- **ASSESSORIA DE TECNOLOGIA DA INFORMAÇÃO**
- **CHEGAB** - Chefia de gabinete
- **DIRADM** - Diretoria Administrativa
- **SICTEC** - Secretaria Municipal de Inovação, Ciência e Tecnologia

## 3. DOCUMENTOS DE REFERÊNCIA

- Lei nº 9.609, de 19 de fevereiro de 1998.  
*Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências, da Lei 12.527 de 18/11/2011, atualizada pela lei 12.737 de 30/11/2012 – que dispõe sobre tipificação criminal de delitos informáticos, e da Lei 13.709 de 14/08/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) que regula o acesso à informação, Política de Segurança da Informação.*

## 4. DEFINIÇÕES / SIGLAS UTILIZADAS

### 4.1 SIGLAS

- **APP (Aplicativo)**: trata-se de um programa desenvolvido para executar uma função específica, basicamente para o usuário.

Elaborado/ revisado por	Diretoria Administrativa Assessoria de Tecnologia da Informação	Em: 20/ 03/2024
-------------------------	--	-----------------

	<b>GOIANIAPREV - Instituto de Previdência dos Servidores do Município de Goiânia</b>  <b>PG – Procedimento de Gestão</b>	DATA: 20/03/2024 <b>VERSÃO: 01</b>
<b>TI - Gerenciamento da Segurança da Informação</b>		

**TI - Gerenciamento da Segurança da Informação**

- **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, o que pode envolver apagamentos acidentais ou corrupção de dados.
- **COOKIES** - São pequenos arquivos que ficam armazenados no computador. Eles são feitos para guardar dados específicos de um cliente ou website, para serem acessados futuramente pelo servidor web de maneira mais rápida.
- **DASHBOARDS** - São painéis visuais que centralizam informações importantes para o negócio. Permitem, desta forma, entender o cenário em tempo real e tomar decisões baseadas em informações reais e que estão ocorrendo agora, monitoradas minuto a minuto.
- **FIREWALL** - É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
- **HTML** (hyper text markup language) - é a linguagem de marcação mais popular na internet.
- **http** (hypertext transfer protocol – protocolo de transferência de hipertexto) - é um protocolo de comunicação que decide como dois computadores ou programas transmitirão dados na Internet. Normalmente, o https utiliza a porta 80 se comunicando na linguagem HTML.
- **https** (hypertext transfer protocol secure – protocolo seguro de transferência de hipertexto ) - é uma implementação do protocolo https sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS (protocolos de segurança que protegem as telecomunicações via internet para serviços de transferência de dados.). Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais.
- **INTRANET** - É a rede interna de computadores de uma empresa.
- **IP** (internet protocol – protocolo de internet) é um endereço único que diferencia cada dispositivo conectado à internet.
- **IPv6** - É a versão mais atualizada do IP e possui mais números e protocolos. Surgiu para substituir gradativamente o IPv4, que já não suporta mais o cenário atual de IPs.
- **JAVA** - É uma linguagem de programação interpretada orientada a objetos. Diferente das linguagens de programação convencionais, que são compiladas para código nativo, é compilada para um bytecode (código de um programa escrito na linguagem Java) que é executado por uma máquina virtual (JVMs).
- **PDF** (portable document format) - significa formato de documento portátil.
- **HACK** - Local físico onde se monta um conjunto de equipamentos relacionados, como servidores, roteadores, switches, etc.

Elaborado/ revisado por	Diretoria Administrativa Assessoria de Tecnologia da Informação	Em: 20/ 03/2024
-------------------------	--	-----------------

	<b>GOIANIAPREV - Instituto de Previdência dos Servidores do Município de Goiânia</b>  <b>PG – Procedimento de Gestão</b>	DATA: 20/03/2024 <b>VERSÃO: 01</b>
<b>TI - Gerenciamento da Segurança da Informação</b>		

PROCESSO

- **TCP/IP** - É um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (transmission control protocol – protocolo de controle de transmissão) e o IP (internet protocol – protocolo de internet). O conjunto de protocolos pode ser visto como um modelo de camadas, onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior.
- **TI** - Tecnologia da informação;
- **TIC** (tecnologia da informação e comunicação) - Correspondem a um conjunto de recursos tecnológicos integrados entre si. O TIC consiste em todos os meios técnicos usados para tratar a informação e auxiliar na comunicação, o que inclui hardware e software.
- **VPN** (virtual private network – rede privada virtual) - É uma rede de comunicação privada. Por fornecer autenticação e confidencialidade na transmissão de dados, além de protocolos criptografados por tunelamento, as VPNs tornam-se mais seguras e confiáveis nas comunicações.
- **XML** (extensible markup language) - É uma linguagem de marcação capaz de descrever diversos tipos de dados. É um dos subtipos da SGML (standard generalized markup language) e sua principal finalidade é facilitar o compartilhamento de informações através da internet. Uma das características fundamentais do XML é possibilitar a criação de uma infraestrutura única para diversas linguagens, facilitando a definição de linguagens desconhecidas.
- **WEB** - WWW (world wide web) ou WEB é a sigla que denomina a rede mundial de computadores ligados em rede.

## 5. DETALHAMENTO DO PROCESSO

A execução deste processo deverá seguir as diretrizes estabelecidas abaixo:

**Atividade 1:** Solicitar ações de TI

**Responsável:** Todas as áreas do GOIANIAPREV

**Descrição da atividade:**

. As solicitações são recebidas via SEI, via memorando.

As áreas encaminham para o Gabinete da Presidência ou diretamente para a área de TI de acordo

Elaborado/ revisado por	Diretoria Administrativa Assessoria de Tecnologia da Informação	Em: 20/ 03/2024
-------------------------	--	-----------------



GOIANIAPREV - Instituto de Previdência dos  
Servidores do Município de Goiânia

DATA: 20/03/2024  
VERSÃO: 01

PG – Procedimento de Gestão

PROCESSO

TI - Gerenciamento da Segurança da Informação

com o tipo de solicitação:

### **TIPOS DE SOLICITAÇÕES**

#### **❖ Solicitações que dependem da autorização da Presidência**

(A solicitação vai para o Gabinete da Presidência e, se autorizado, é encaminhada para a área de TI)

### **CONTROLE DE ACESSOS LÓGICOS**

. Liberação ou bloqueio de acessos ao(s):

#### **SISTEMAS**

- COMPLETE
- SEI
- INTRANET
- SIGEP
- Portal do Servidor
- Correio eletrônico
- Internet

#### **REDE INTERNA (PASTAS DE REDE)**

#### **❖ Solicitações que NÃO dependem de autorização da Presidência**

### **CONTROLE DE ACESSOS LÓGICOS**

. Manutenção de senhas de acesso aos sistemas

### **ASSISTÊNCIAS TÉCNICAS:**

- . Falha nos sistemas
- . Falha na rede (elétrica e lógica)
- . Falha na rede elétrica (instalações)
- . Assistência técnica ao usuário
- . Assistência técnica (hardware e software)

### **CONTROLE DE ACESSO FÍSICO**

(Liberação de acessos às salas de hack de infraestrutura de rede)

Elaborado/ revisado por

Diretoria Administrativa  
Assessoria de Tecnologia da Informação

Em: 20/ 03/2024



## **Atividade 2:** Analisar solicitações

**Responsável:** DIRADM/TI

### **Descrição da atividade:**

A área de TI recebe a solicitação (do Gabinete da Presidência ou diretamente da área, conforme tipo de solicitação) e faz a identificação do tipo de solicitação, assim como, a distribuição para o responsável pelo atendimento.

#### ● **TIPOS DE SOLICITAÇÕES**

##### ❖ **Solicitações que dependem da autorização da Presidência**

#### **CONTROLE DE ACESSOS LÓGICOS**

. Liberação ou bloqueio de acessos ao(s):

##### **SISTEMAS**

###### ● **COMPLETE**

O administrador de senha deverá:

- Verificar se a solicitação está autorizada pela Presidência.
- Acessar o sistema COMPLETE com login e senha
- Para liberação de acesso: verificar se a lotação do servidor em questão está no GOIANIAPREV. (Caso não esteja não é possível liberar o acesso).
- Realizar a liberação de acesso.

```
EXISTEM MENSAGENS A SUA ESPERA, VERIFIQUE
20/03/2024                                PREFEITURA MUNICIPAL
                                           PROJETOS

Opcao : __

1 - Sistemas Administrativos
2 - Recursos Humanos
3 - Sistemas Especificos
4 - Sistema Eletronico de Processo
```

Opções: Sistemas Administrativos > Administracao De Senhas > Cadastro>Por Sistema. Colocar matrícula, após digite “Enter”.

- **SEI** - A liberação/bloqueio do acesso ao sistema SEI é feita pela Casa Civil, por meio de ofício encaminhado pela Secretaria Geral do GOIANIAPREV.
- **INTRANET** - A liberação/bloqueio do acesso à INTRANET é atendida pela área de TI, que recebe a solicitação e rege a senha.
- **SIGEP** - Atualmente a liberação de acesso/bloqueio/desbloqueio do SIGEP está sendo realizado por um prestador de serviços da empresa contratada. (*Sistema em fase de implementação*)
- **Portal do Servidor - SIGEP** - A liberação/bloqueio/desbloqueio de acesso é feito por



PROCESSO

**TI - Gerenciamento da Segurança da Informação**

um prestador de serviços na função de “gestor do SIGEP” e pelos servidores da recepção do GOIANIAPREV. *(Sistema em fase de implementação)*

- **Portal do Servidor** - A liberação de acesso é feita no ato da posse pela SEMAD e o desbloqueio pela Gerência de Pessoas do órgão.
- **Correio eletrônico** - A liberação do acesso é feita pela área de TI. Acessar o sistema COMPLETE

Opções: Sistemas Administrativos> Administração de Senhas>Pedidos de User-id/Rede/E-mail>Criação de E-mail > digitar a matrícula e o primeiro nome do servidor e F5 (para enviar o pedido para a SICTEC)

O Bloqueio do acesso é feito via OS no sistema de INTRANET para a SICTEC.

- **Internet** - A liberação/acesso da internet é concomitante com o acesso à rede.

**REDE INTERNA (PASTAS DE REDE)**

A liberação ou bloqueio de acesso à pasta de rede é feita mediante solicitação via OS na INTRANET para a SICTEC.

❖ **Solicitações que NÃO dependem de autorização da Presidência**

**CONTROLE DE ACESSOS LÓGICOS**

. Manutenção de senhas de acesso aos sistemas

- **COMPLETE**

Entrar no COMPLETE - Opções: Sistemas Administrativos > Administração De Senhas>Pedidos de User-id/Rede/E-mail

Em caso de desbloqueio de senha “2 - Desbloqueio de User-id”

Em caso de gerar nova senha: “3 - Regeração de Senha”

- **SEI, INTRANET, correios eletrônico, acesso a rede:**

Acessar a INTRANET (<https://outprod01.goiania.go.gov.br/Intranet>)

Abrir uma OS via INTRANET para a SICTEC, solicitando uma nova senha de rede.

Na Aba “Sistemas” clicar em “Atendimento”, “Incluir uma nova solicitação”, preencher os dados da solicitação, preencher o campo “Serviço” (Serviços de Rede e Micro Informática - Suporte Técnico) e “Gravar”.



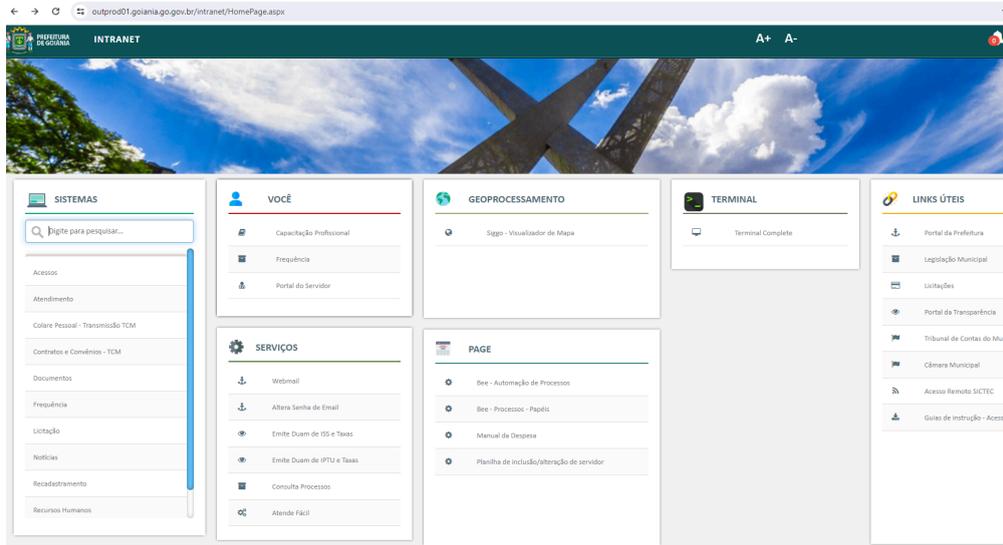
GOIANIAPREV - Instituto de Previdência dos Servidores do Município de Goiânia

DATA: 20/03/2024  
VERSÃO: 01

PG – Procedimento de Gestão

PROCESSO

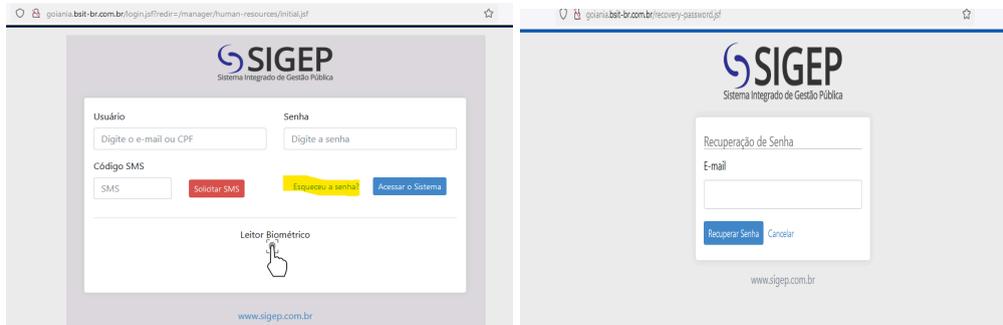
TI - Gerenciamento da Segurança da Informação



#### • SIGEP

Acessar o link:

<http://goiania.bsit-br.com.br/login.jsf?redir=/manager/human-resources/initial.jsf>



#### • Portal do Servidor

Acessar o Portal do Servidor:

<https://www.goiania.go.gov.br/sistemas/saces/asp/saces00000f0.asp?sigla=sipsm>

Clicar em “Regerar Senha pra outros usuários”, digitar a matrícula do servidor, “confirmar dados” e clicar em “regerar senha”.

Elaborado/ revisado por

Diretoria Administrativa  
Assessoria de Tecnologia da Informação

Em: 20/ 03/2024



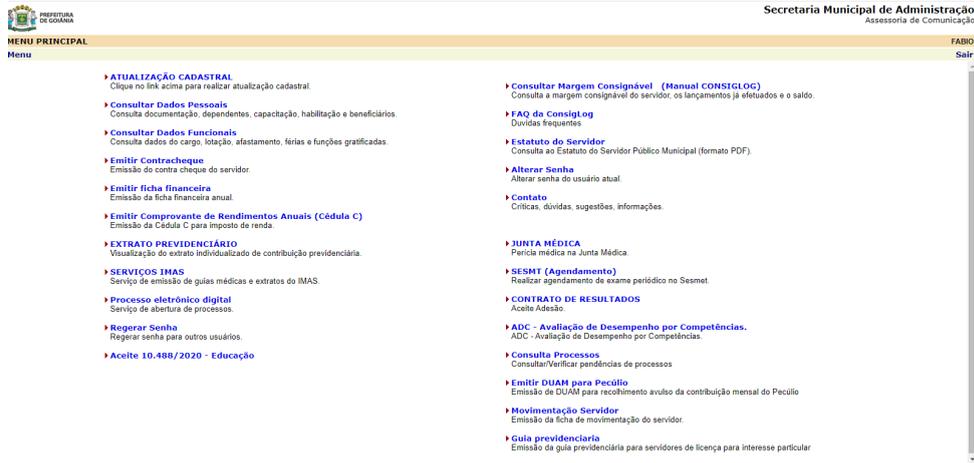
GOIANIAPREV - Instituto de Previdência dos  
Servidores do Município de Goiânia

DATA: 20/03/2024  
VERSÃO: 01

PG – Procedimento de Gestão

PROCESSO

TI - Gerenciamento da Segurança da Informação



## ASSISTÊNCIAS TÉCNICAS:

- . **Falha nos sistemas** - Se a falha for nos sistemas da Prefeitura - abrir OS na Intranet. Se a falha for no sistema operacional ou softwares em geral (windows, pacote office, etc) a área de TI dá o primeiro suporte e, caso não seja solucionado, abre OS para providências do suporte técnico da SICTEC.
- . **Falha na rede (elétrica e lógica)** - A área de TI tenta solucionar o problema, caso não seja possível, abre OS para providências do suporte técnico da SICTEC.
- . **Falha na rede elétrica (instalações)** - A área de TI tenta solucionar o problema, caso não seja possível, a DIRADM abre OS para providências do suporte técnico do órgão responsável (SINFRA ou SICTEC).
- . **Assistência técnica ao usuário** - A área de TI dá suporte interno, solucionando dúvidas dos servidores;
- . **Assistência técnica (hardwares)** - A área de TI dá suporte interno quanto a manutenção de equipamentos e, caso não seja solucionado, abre OS para providências do suporte técnico da SICTEC.

## CONTROLE DE ACESSO FÍSICO

(Liberação de acessos às salas de hack de infraestrutura de rede)

O controle e a liberação de acesso às salas de hack de infraestrutura de rede e nobreak - para servidores ou prestadores de serviços - é feito pela assessoria de TI, que detém as chaves do local.

Elaborado/ revisado por

Diretoria Administrativa  
Assessoria de Tecnologia da Informação

Em: 20/ 03/2024

	<p align="center"><b>GOIANIAPREV - Instituto de Previdência dos Servidores do Município de Goiânia</b></p> <p align="center"><b>PG – Procedimento de Gestão</b></p>	<p align="right">DATA: 20/03/2024 <b>VERSÃO: 01</b></p>
<p><b>TI - Gerenciamento da Segurança da Informação</b></p>		

**Atividade 3:** Atender solicitações

**Responsável:** DIRADM/TI

**Descrição da atividade:**

A área de TI atende às áreas, conforme o tipo de solicitação e as diretrizes previstas na Política de Segurança da Informação (anexo 6.2)

**Atividade 4:** Fazer o Plano de Contingência

**Responsável:** DIRADM/TI

**Descrição da atividade:**

Conforme a PSI:

- . Cabe à alta gestão tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas da T.I.
- . Instituir o Comitê Gestor da PSI o qual deverá, entre outras atribuições previstas na PSI, instituir o modelo de gestão previsto na PSI e alinhar as ações de TI com o Planejamento Estratégico do GOIANIAPREV.
- . Em casos de incidentes de segurança, os gestores da informação devem participar da investigação das informações sob sua responsabilidade;

**CÓPIA DE SEGURANÇA(BACKUP)**

**BACKUP - Servidores**

Todos os dados pertinentes ao GOIANIAPREV deverão ser armazenados no Servidor de Rede. É de responsabilidade de cada servidor do GOIANIAPREV este armazenamento. A integridade e não perda dos dados armazenados no Servidor de Rede é de responsabilidade da SICTEC.

**BACKUP - BANCO DE DADOS**

Atualmente existem 03 (três) Banco de Dados: o ADABAS, o DB2 e o SQL Server. Nestes bancos estão armazenados todos os dados dos sistemas corporativos da prefeitura de Goiânia/GOIANIAPREV. Estes bancos possuem cópias de segurança diária de segunda a sexta-feira, com a seguinte retenção: 12 (doze) dias, dia-a-dia e uma cópia mensal com retenção de 05 (cinco) anos.

Elaborado/ revisado por	Diretoria Administrativa Assessoria de Tecnologia da Informação	Em: 20/ 03/2024
-------------------------	--	-----------------



GOIANIAPREV - Instituto de Previdência dos  
Servidores do Município de Goiânia

DATA: 20/03/2024  
VERSÃO: 01

PG – Procedimento de Gestão

PROCESSO

TI - Gerenciamento da Segurança da Informação

### **CONTROLE DE ACESSO FÍSICO (para o hacks de banco de dados)**

O Data Center da **SICTEC** possui um controle de acesso através de verificação digital e câmeras de videomonitoramento, de tal forma que somente pessoas autorizadas conseguem adentrar ao Data Center e é possível recuperar a imagem de todas as pessoas que adentraram ao local.

## **CONTROLE DE ACESSOS LÓGICOS**

### **SISTEMAS**

Os Sistemas da Intranet são executados em equipamentos virtualizados, tolerante a falhas, ou seja, mesmo que o servidor ou disco que está executando os Sistemas da Intranet venham falhar ele será executado em um novo servidor acessando outro disco.

O mesmo acontece para o controle de acesso à rede, que possui diversos servidores de “login” (Controladores de Domínio) em paralelo.

O Data Center onde estão os computadores servidores possui energia estabilizada e tolerante a falhas através de Nobreak de 15 minutos e gerador de energia através de motor a diesel. A temperatura do Data Center é controlada por um sistema de refrigeração com alerta para falhas.

Para falhas catastróficas, semanalmente, uma cópia dos principais dados de backup são retirados do Data Center e enviados a uma outra localidade.

**Internet** - Sua contingência é entrar em contato com a SICTEC e aguardar a prestadora de serviços de fibra óptica corrigir o problema.

### **REDE INTERNA (PASTAS DE REDE)**

O Plano de Contingência é o mesmo para os sistemas, porém o backup é realizado diariamente e a guarda das informações é de sete dias.

## **ASSISTÊNCIAS TÉCNICAS**

. Falha nos sistemas - Ligar no ramal 3838, ramal da SICTEC, e abrir uma ordem de serviço.

. Falha na rede (elétrica e lógica) - O GOIANIAPREV conta com um nobreak com autonomia de 2 hs para os desktops, bem como ao hack da sala de servidores.

Elétrica:

Acionar a EQUATORIAL.

Alertar aos usuários sobre a autonomia do nobreak e pedir para que finalizem as sessões nos desktops.

Lógica:

Elaborado/ revisado por

Diretoria Administrativa  
Assessoria de Tecnologia da Informação

Em: 20/ 03/2024

	<b>GOIANIAPREV - Instituto de Previdência dos Servidores do Município de Goiânia</b>  <b>PG – Procedimento de Gestão</b>	DATA: 20/03/2024 <b>VERSÃO: 01</b>
<b>TI - Gerenciamento da Segurança da Informação</b>		

Acionar a SICTEC via ramal 3838 e os mesmos acionam a prestadora de serviços de fibra óptica. Alertar aos usuários sobre a instabilidade da rede lógica.

. **Falha na rede elétrica (instalações)** - A sede do GOIANIAPREV conta com um nobreak ligado a todos os desktops da sede, bem como ao rack da sala de servidores, com tempo de autonomia mínima de quarenta minutos.

Em caso de interrupção de energia elétrica, acionar a concessionária de energia elétrica e alertar aos usuários sobre a autonomia do nobreak, assim como, pedir para que finalizem as sessões nos desktops.

. **Assistência técnica ao usuário/servidor** - O servidor/usuário entra em contato com o Ramal 5803, da área de TI. É feita uma verificação da solicitação. Se necessário o servidor de TI (Fábio/Sheila/Marcilene) vai in loco para atendimento, caso seja mais simples é resolvido pelo telefone e o atendimento encerrado.

. **Assistência técnica (hardware)** - O servidor da área de TI faz a verificação da correção. Caso o equipamento tenha assistência técnica ativa é acionado o prestador de serviço. Não tendo, verifica-se se há a possibilidade de conserto no GOIANIAPREV ou, se precisar, encaminhar para a SICTEC.

### **CONTROLE DE ACESSO FÍSICO**

O controle de acesso físico é regulamentado pela PSI, conforme as seguintes diretrizes:

*IV –Segurança Física: Toda entrega de materiais, inclusive equipamentos e suprimentos, deve ser comunicada antecipadamente à área administrativa responsável pelo patrimônio/almoxarifado, com indicação do tipo de material e da unidade a que se destina e nome do servidor responsável pelo recebimento.*

*O acesso ao GOIANIAPREV será somente permitido para pessoas autorizadas, pelo monitoramento da recepção, acompanhado pelo guarda municipal ou vigilante terceirizado, de modo a controlar entrada e saída de visitantes, pessoal interno e estabelecer perímetros de segurança;*

Elaborado/ revisado por	Diretoria Administrativa Assessoria de Tecnologia da Informação	Em: 20/ 03/2024
-------------------------	--	-----------------



**GOIANIAPREV - Instituto de Previdência dos  
Servidores do Município de Goiânia**

DATA: 20/03/2024

**VERSÃO: 01**

**PG – Procedimento de Gestão**

PROCESSO

**TI - Gerenciamento da Segurança da Informação**

**Elaborado/ revisado em \_\_\_/\_\_\_/\_\_\_\_, por:**

*Dono do processo:*

\_\_\_\_\_  
*Diretoria Administrativa*

*Líder(es) do Processo (Responsáveis por comunicar ao Escritório de Processos as necessidades de  
atualização do fluxo/PG – Procedimento de Gestão):*

\_\_\_\_\_  
*AAssessoria de Tecnologia da Informação*

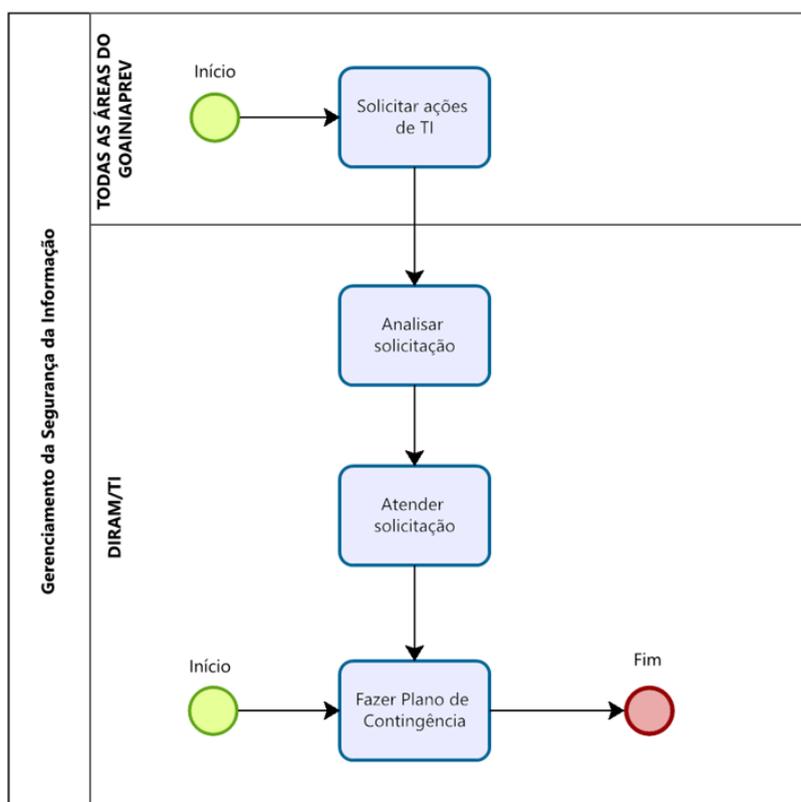
Elaborado/ revisado por

Diretoria Administrativa  
Assessoria de Tecnologia da Informação

Em: 20/ 03/2024

## 6. ANEXO

### 6.1. FLUXOGRAMA



### 6.2. POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

*[Publicação no Diário Oficial do Município de Goiânia](#)*