POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA GESTÃO DOS RPPS

Instituto de Previdência do Município de Aparecida de Goiânia

Abril - 2022

Vilmar Mariano

Prefeito de Aparecida de Goiânia

Diretoria Executiva do Instituto de Previdência de Aparecida de Goiânia – APARECIDAPREV

Presidente:

Einstein Almeida Ferreira Paniago

Diretor Administrativo:

Sandro Rogério Lima Belo

Diretor de Benefícios:

Epitácio Barbosa dos Reis

Diretor Financeiro:

Khayo Eduardo Pires de Oliveira

Diretora Jurídica:

Keila Mirian Afonso Martins

Pesquisa e Produção de Conteúdo:

Gesinópolis Ramos do Carmo

Elaboração e Revisão:

Gesinópolis Ramos do Carmo

Thamara Kellen de Melo Pires

Keila Mirian Afonso Martins Pereira

Sobre o APARECIDAPREV

O regime proprio de previdencia social do município de Aparecida de Goiânia, instituído pela Lei nº 001, de 1 de novembro de 2001 e regulado pela Lei Complementar nº 007, de 30 de dezembro de 2002, passou a ser regido pela pesente lei complementar.

De acordo com a Lei Complementar nº 010 de 20 de junho de 2005, o APARECIDAPREV, dispõe- se a adequação à Emenda Constitucional nº 41/03 e se torna uma autarquia municipal, com personalidade jurídica propria para gerir o Regime Próprio de Previdência Social do Município de Aparecida de Goiânia.

Apresentação

Este documento tem por objetivo divulgar, no ambiente interno do APARECIDAPREV, a Politica de Segurança da Informação, busca orientar os usuários para a utilização segura dos recursos de tecnologia da informação disponibilizadas pela instituição do APARECIDAPREV.

Sumário

1. INTRODUÇÃO

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação de forma a garantir a continuidade dos serviços, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição. Atualmente, a tecnologia é primordial em qualquer ambiente empresarial e público, independentemente do porte ou da área de atuação das empresas e órgãos públicos. Nas últimas décadas, houve significativo aumento da quantidade de informações sensíveis circulando d eum ponto a outro, tanto dentro da organização como dela para o mundo todo, via internet.

À vista disso, o termo tecnologia da informação (TI), pode ser definido como o conjunto de recursos tecnológicos e computacionais para a geração e uso da informação, abrangendo todas as atividades desenvolvidas na sociedade pelos recursos da informática.

E por mais que a proliferação dos dispositivos móveis e dos serviços de nuvem e recursos relacionados a TI, como internet, correio eletrônico, redes sem fio, entre outros, sejam atualmente ferramentas de trabalho indispensáveis no desempenho das mais diversas atividades. Tais recursos podem ser explorados parafins ilícitos, como roubo de informações, disseminação de vírus, envio de spam, etc.

Porfim,é questão de primeira necessidade ter políticas que, documentadas detalhem procedimentos e diretrizes para eliminar a subjetividade ao lidar com informações sensíveis e confidenciais, tanto em relação a erros quanto a vazamentos deliberados.

A Política de Segurança da Informação (PSI), por sua vez, é o documento formal que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação.

A presente Política de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos servidores e fornecedores do APARECIDAPREV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal do instituto e do

indivíduo. Nortear a definição de normas e procedimentos específicos de segura da informação, bem como a implementação de controles e processos para seu atendimento. Preservar as informações do APARECIDAPREV quanto à:

I - 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.

II - Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

III - Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

IV - Autenticidade: identificar e registrar o usuário que está enviando ou modificando a informação.

3. CAMPO DE APLICAÇÃO

3.1. Dos Servidores e Fornecedores em Geral

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público ou por livre nomeação e exoneração, que exerça alguma atividade dentro ou fora da instituição. Entende-se por fornecedor o prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada servidor ou fornecedor todo prejuízo ou dano que vier a sofrer ou causar ao APARECIDAPREV e/ou a terceiros, em decorrência da não obediência às diretrizes e normas referidas.

3.2. Dos Servidores em Regime de Exceção (Temporários e Estagiários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Política de Segurança de Informações. A concessão de acesso poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de

exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas nesta política.

3.3. Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão.

Os objetivos e diretrizes estabelecidos nesta Política de Segurança da Informação serão aplicados em toda a organização, deverão ser observados por todos servidores, órgãos colegiados, parceiros, fornecedores, prestadores de serviços e usuários que utilizem o ambiente informacional do APARECIDAPREV, ou acesso às informações pertencentes ao instituto. As políticas de segurança da informação aqui tratadas observam o cumprimento das normas constantes. O descumprimento dessas normas,a exemplo de fraudes e invasão ou violação da integridade dos dados e informações do instituto, ficará submetido à legislação nacional emvigor.

Aplicam-se ainda ao gerenciamento de quaisquer equipamentos, programas, meios físicos de tráfego e sistemas de armazenamento digital de dados,informações incluídas em notebooks, tablets, unidades móveis de armazenamento como smartphones, impressoras, além das estações de trabalho, inseridos nas dependências do APARECIDAPREV.

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo APARECIDAPREV pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entreas partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas, serviços e andamento das atividades do Instituto.

O APARECIDAPREV, por meio de sua equipe de tecnologia de informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DE APARECIDA DE GOIÂNIA - APARECIDAPREV.

4.1. PRINCÍPIOS E OBJETIVOS

Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade; são objetivos da Política de Segurança da Informação do **APARECIDAPREV**:

I - Estabelecer diretrizes para a disponibilização e utilização de recursos de informação,serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.

II - Designar e definir ações e responsabilidades a serem tomadas por parte dos servidores pertinentes.

III - Apoiar a implantação das iniciativas relativas à Segurança da Informação.

IV - Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

4.2. São Princípios da Política de Segurança da Informação do APARECIDAPREV

Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao APARECIDAPREV. As exceções devem ser explicitas e formalizadas entre as partes.

I - Todos os recursos de informação do APARECIDAPREV devem ser projetados para que seu uso seja consciente e responsável. Os recursos de comunicação e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalistícos;

II - Deverão ser criados e instituídos controles apropriados, registros de atividades e afins, em todos os pontos e sistemas em que a instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação;

III - Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade. Todo o acesso a redes e sistemas do órgão devera ser feito, preferencialmente, por meio de login de acesso único, pessoal ei ntransferível;

IV - O APARECIDAPREV pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada em sua infraestrutura;

V - Cada usuário é responsável pela segurança das informações dentro do APARECIDAPREV, principalmente daquelas que estão sob sua responsabilidade;

VI - A gestão da segurança da informação no APARECIDAPREV será realizada pela Presidência, bem como pela Coordenadoria de Tecnologia da Informação e Diretoria Administrativa.

VII - Deverá constar em todos os contratos do APARECIDAPREV, quando o objeto for pertinente, cláusula de confidencialidade e de obediência as normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no APARECIDAPREV.

VIII - Esta Política de Segurança da Informação será implementada no APARECIDAPREV por meio de normas e procedimentos específicos, obrigatórios para Todos os usuários, independentemente do nível hierárquico ou função, bem como de vinculo empregatício ou de prestação de serviço .

5. PAPÉIS E RESPONSABILIDADES

Descrições de Papéis em Segurança da Informação:

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO

Usuário Interno	Servidores públicos e demais funcionários e colaboradores internos.	Todos os servidores, gestores, técnicos, estagiários, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do APARECIDAPREV.
Usuário Externo	Prestadores de Serviços, órgãos colegiados e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pelo APARECIDAPREV e Demais colaboradores externos que fazem uso deseus recursos informacionais e computacionais.
Áreade TI	Presidente e Diretoria Administrativa	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.

5.1. Responsabilidades Gerais

São responsabilidades gerais de todos os usuários e gestores de serviços da rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do APARECIDAPREV:

I - Promover a segurança de seu usuário (login) corporativo, departamental ou de rede local, bem como a de seus respectivos dados e credenciais de acesso, o que inclui o não compartilhamento dessas informações de acesso, bem como a troca periódica de sua senha.

II - Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do APARECIDAPREV

III - Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do APARECIDAPREV.

Os modelos de declaração de compromisso e de ciência das normas de Segurança da Informação vigentes no APARECIDAPREV estão presentes no ANEXO Ie II.

5.2. Responsabilidades Específicas

5.2.1. Usuários internos e externos.

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar ao APARECIDAPREV em decorrência da não obediência as diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes. Os usuários externos devem entender os riscos associados a sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. O APARECIDAPREV poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da política de SI ou das normas e procedimentos específicos dela decorrentes.

5.2.2. Gestores de Pessoas e Processos.

Os diretores e Presidência do APARECIDAPREV devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes as políticas, normas e procedimentos específicos de segurança da informação do APARECIDAPREV, tomando as ações necessárias para cumprir tal responsabilidade.

5.3. Área de Tecnologia da Informação.

Quanto à gestão de segurança da informação, serão responsabilidade sespecíficas

da área de Tecnologia da Informação:

I - Zelar pela eficácia dos controles de Segurança de Informação utilizados e informar aos gestores e demais interessados os riscos residuais.

II - Negociar e acordar com os gestores, níveis de serviço relacionados à Segurança de Informação, incluindo os procedimentos de resposta a incidentes.

III - Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.

IV - Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

V - Administrar e proteger cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o APARECIDAPREV.

VI - Informar previamente sobre o fim do prazo de retenção de informações, para que se tenha a alternativa de alterá-lo ou postergá-lo,antes que a informação seja definitivamente descartada pelo custodiante.

VII – Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases dedados e qualquer outro ativo de informação a um responsável identificável como pessoafísica, responsável pelo uso da conta (a responsabilidade pela gestão dos "logins" de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades).

6. DIRETRIZES GERAIS.

6.1. Tratamentos da informação.

São diretrizes específicas e procedimentos próprios de tratamento da informação corporativa do APARECIDAPREV:

I - Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos no servidor de arquivos da rede. Tais arquivos, se gravados apenas

localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

II - Arquivos pessoais e/ou não pertinentes as atividades institucionais do APARECIDAPREV (fotos, musicas, vídeos, etc..) não deverão ser copiados ou movidos para o servidor de arquivos, pois podem sobrecarregar o armazenamento nos servidores. Caso identificado, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

III - É de responsabilidade de cada setor a verificação e organização de seus respectivos dados no servidor de arquivos, especialmente para a detecção e remoção de dados duplicados objetivando a eficiência do armazenamento, economia de espaço e redução de tráfego de rede e de tempo de backup.

6.2.Controles de Acesso.

O controle de acesso observará as seguintes diretrizes específicas e procedimentos próprios:

I - Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o APARECIDAPREV e/ou terceiros.

II - O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art.307-falsa identidade).

III -Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

IV - Todos os dispositivos de identificação utilizados no APARECIDAPREV, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas,os certificados e assinaturas digitais, os dados biométricos tem de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

V - O usuário, vinculado a tais dispositivos identificadores,será responsável pelo seu uso

correto perante a instituição e a legislação (cível e criminal).

VI - Todo e qualquer dispositivo de identificaçãopessoal, portanto, não poderá ser compartilhado comoutras pessoas em nenhuma hipótese.

VII - Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o APARECIDAPREV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor sobre o uso compartilhado, ele deverá ser responsabilizado.

VIII - É proibido o compartilhamento de login para funções de administração de sistemas.

IX - O setor de Recursos Humanos é responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores e o departamento de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na instituição.

X - Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, servidores efetivos e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

XI - É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

XII - As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word,Excel,etc.), não devem ser compreensíveis por linguagem humana (não criptografados); não devem ser baseado em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias deteclado, como "abcdefgh", "87654321", entre outras.

XIII - Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtivessem acesso indevido ao seu Login/senha.

XIV - Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, assim que algum usuário for demitido ou solicitar demissão, a Presidência deverá imediatamente comunicar tal fato a Gerencia de Pessoal, e este à

Coordenadoria de Tecnologia da Informação a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

XV - Caso o colaborador esqueça sua senha, ele devera requisitar formalmente a troca ou comparecer pessoalmente a área técnica responsável para cadastrar uma nova.

6.3. Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade do APARECIDAPREV, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumpriras recomendações constantes nesta PSI.

a) É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento técnico da área de Tecnologia da Informação do APARECIDAPREV.

b) O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o responsável técnico mediante registro de chamado.

c) A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

d) Arquivos pessoais e/ou não pertinentes ao negócio do APARECIDAPREV (fotos,musicas, vídeos, etc..) não deverão ser copiados/movidos para o servidor de arquivos, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem aviso prévio.

e) Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos no servidor de arquivos. Tais arquivos, se gravados apenas

localmente nos computadores (por exemplo, no driveC:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

f) Os colaboradores do APARECIDAPREV e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prevista solicitação e a autorização da Presidência.

g) No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os colaboradores devem informar ao departamento de Tecnologia da Informação qualquer identificação de dispositivo estranho conectado ao seu computador.

- E vedada à abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por técnico responsável do APARECIDAPREV ou por terceiros devidamente contratados para o serviço.

- Todos os modems/roteadores internos ou externos devem ser removidosda rede ou desativados para impedir a invasão/evasão de informações,programas, vírus e conflitos de rede que geram lentidão ou interrupção de comunicação. Em alguns casos especiais, conforme regra específica será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

- O colaborador deverá manter a configuração do equipamento disponibilizado pelo APARECIDAPREV, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade com a custodiante dei nformações.

- Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

- Todos os recursos tecnológicos adquiridos pelo APARECIDAPREV devem ter imediatamente suas senhas padrões (default) alterados.

- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

- Pendrives ou drives externos de propriedade particular devem ser evitados, pois é um dos principais vetores de disseminação de vírus.

- Notebooks ou computadores particulares ou de terceiros não devem ser, em hipótese alguma, conectados à rede lógica do APARECIDAPREV por meio de cabo de rede. Tais equipamentos, se infectados, podem disseminar ameaças eletrônicas via rede e contaminarem todas as máquinas e apagarem todos osarquivos da rede. Tais equipamentos, se realmente necessários, devem ter a autorização previa da presidência do órgão e se precisarem se conectar a internet, o acesso deve ser feito via rede sem fios especialmente configurada para esse acesso.Tal rede está segregada da rede corporativa e não apresenta possibilidade de contaminação para a rede interna. Em caso de infecção em massa de nossos equipamentos e perda dos arquivos da rede, o responsável responderá nos termos da legislação aplicável.

- Não é permitido se conectar remotamente (via internet) aos computadores d oInstituto, nem possibilitar o acesso de terceiros às maquinas da rede, implicando em violação de segurança. Tal procedimento, se necessário, deve ser feito com a autorização e acompanhamento dos técnicos da Coordenadoria de Tecnologia da Informação.

- Aos usuários não são permitidas instalações de softwares estranhos aos homologados no Instituto por serem meios de transmissão de malware.

g) Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do APARECIDAPREV:

h) Tentar obter ou obter acesso não autorizado a outro computador, servidor ou rede.

i) Burlar quaisquer sistemas de segurança.

j) Acessar informações confidenciais sem explícita autorização do proprietário.

k) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

l) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

m) Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assedio sexual ou perturbação.

n) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

6.4. Correio Eletrônico.

O objetivo desta norma é informar aos colaboradores do APARECIDAPREV quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

a) O uso do correio eletrônico do APARECIDAPREV é permitido para fins corporativos e relacionado às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feito com bom senso, não prejudique o APARECIDAPREV e também não cause impacto no tráfego da rede.

b) Acrescentamos que é proibido aos colaboradores no uso do correio eletrônico do APARECIDAPREV:

- Enviar mensagens não solicitadas para múltiplos destinatários, excetos e relacionadas ao uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado autilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o APARECIDAPREV ou suas unidades vulneráveis a ações civis ou criminais;

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder aidentidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do APARECIDAPREV estiver sujeita a algum tipo de investigação;

- Produzir, transmitir ou divulgar mensagem que contenha qualquer ato ou que forneça orientação que conflite ou contrarie os interesses do APARECIDAPREV;

- Contenha ameaças eletrônicas, como: spam, e-mail bombing, vírus de computador ;

- Contenha arquivos com código executável (.exe..com,.bat,.pif,.js,.vbs,.hta,.src, .cpl,.reg.,.dll,.inf.) ou qualquer outra extensão que represente um risco a segurança;

- Vise obter acesso não autorizado a outro computador, servidor ou rede;

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Vise burlar qualquer sistema de segurança;

- Vise vigiar secretamente ou assediar outro usuário;

- Vise acessar informações confidenciais sem explícita autorização do proprietário;

- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

- Inclua imagens criptografadas ou de qualquer forma mascaradas;

- Contenha anexo(s) superior(es) a 15MB para envio (interno e internet) e 15MB para recebimento (internet);

- Tenha conteúdo considerado impróprio, obsceno ou ilegal;

- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Contenha perseguição preconceituosa baseada em sexo, raça, incapacida defísica ou mental ou outras situações protegidas;

- Tenha fins políticos locais ou do pafs (propaganda política);

- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

c) As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerencia ou departamento
- Nome da empresa
- Telefone(s)

6.5. Serviços de Backup.

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" - períodos em que não ha nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

a) 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.

b) Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do APARECIDAPREV, exigem uma regrad e retenção especial, conforme previstonos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

c) Na situação de erro de backup é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

d) Testes de restauração de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com acriticidade do backup.

6.6.Data Center

a) Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração da PSI - Política de Segurança da Informação – aliberação do acesso.

b) O Data Center deverá ser mantido limpo. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

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

d) A entrada ou retirada de quaisquer equipamentos do Data Center somente se dará com a autorização desse instrumento pelo responsável do Data Center.

6.7. Monitoramentos do Ambiente.

Para garantir a aplicação das diretrizes mencionadas nesta PSI, além de fixar normas e procedimentos complementares sobre o tema, o APARECIDAPREV poderá:

a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou sem fio e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser

usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

b) Tornar públicas as informações obtidas pelos sistemas de monitoramento e registros de atividade, no caso de exigência judicial;

c) Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

d) Instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança da informação e dos perímetros de acesso;

e) Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

7. USO E ACESSO À INTERNET.

Todas as regras atuais doAPARECIDAPREV visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

a) Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet esta sujeita a divulgação e auditoria. Portanto, o APARECIDAPREV, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela quando necessário.

b) Os equipamentos, tecnologia e serviços fornecidos para o acesso a 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 da sua Política de Segurança da Informação.

c) O APARECIDAPREV, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e autorização para tal, será julgada

inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderão acarretar as ações administrativas e as penalidades decorrentes de processos civis e criminais, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

d) O acesso à internet disponibilizado pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizado para fins pessoais, desde que não prejudique o andamento dos trabalhos.

e) Como é do interesse do APARECIDAPREV que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

f) Somente os colaboradores que estão devidamente autorizados a falar em nome do APARECIDAPREV para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

g) Apenas os colaboradores autorizados pela instituição poderão copiar captar, imprimir ou enviar imagens da tela para terceiros, devendo atender a norma interna de uso de imagens, a Lei de Direitos Autorais, a proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

h) É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

i) Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no APARECIDAPREV, diretamente do site do fabricante do software, evitando sites como baixaki ou outros que não os oficiais dos respectivos softwares, pois esses sites embutem malware nos programas a serem baixados, e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela

Presidência.

j) O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado poderá ser excluído, sem aviso prévio.

k) Os colaboradores não poderão em hipótese algumautilizar os recursos do APARECIDAPREV para fazer o download, uso ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

l) Como regra geral, materiais de cunho sexual não poderão se rexpostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

m) Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao APARECIDAPREV ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

n) Os colaboradores não poderão utilizar os recursos do APARECIDAPREV para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de tróia, spam, assedio, perturbação ou programas de controle de outros computadores.

8. GESTÃO DE RISCOS.

A "Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e programar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seusativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos". As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações do APARECIDAPREV deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação.

9. PENALIDADES.

O APARECIDAPREV, ao gerir e monitorar seus ativos de informação pretende garantir a integridade destes, juntamente com suas informações e recursos. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem faltas graves, as quais o APARECIDAPREV responderá com a aplicação de todas as medidas administrativas, cíveis e criminais cabíveis. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperaraativamente com as autoridades competentes.

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o APARECIDAPREV e/ou terceiros.

10. ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

Os documentos que comporão a estrutura normativa de gestão de segurança da informação se darão pela Política de Segurança da Informação que: constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o APARECIDAPREV decidiu incorporar a 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.

a. Divulgação e acesso à estrutura normativa.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os servidores, órgãos colegiados, colaboradores, estagiários, aprendizes e prestadores de serviços do APARECIDAPREV quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

b. Aprovação e revisão.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação do APARECIDAPREV poderão ser revisados e alterados conforme deliberação do Conselho Administrativo.

11. REFERÊNCIAS LEGAIS E NORMATIVAS.

Referências legais e normativas:

- Lei Federal 8.159/1991, de 08/01/1991- Dispõe sobre a política nacional de arquivos públicos e privados.
- Lei Federal 9.610/1998, de 19/02/1998 - Dispõe sobre o direito autoral.
- Lei Federal 9.279/1996, de 14/05/1996 - Dispõe sabre marcas e patentes.
- Lei Federal 10.406/2002, de 10/01/2002 – Institui o Código Civil brasileiro.
- Decreto - Lei 2.848/1940, de 07/12/1940 – Instituio Código Penal brasileiro.

12. DISPOSIÇÕES FINAIS.

Para a uniformização da informação organizacional, esta Política de Segurança da Informação deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do APARECIDAPREV - a fim de que seja cumprida dentro e fora da autarquia.

O não cumprimento dos requisitos previstos nesta política acarretará violação àsregras internas da instituição e sujeitará o usuário às medidas administrativas e legaiscabíveis.

Aparecida de Goiânia, abril de 2022.

Aprovada pelo Conselho Deliberativo.

EINSTEIN FERREIRA ALMEIDA PANIAGO

PRESIDENTE

ANEXO I

TERMO DE COMPROMISSO CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO	
IDENTIFICAÇÃO DO CONTRATO	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA EMPRESA CONTRATADA	
OBJETO RESUMIDO	
VIGENCIA CONTRATUAL	

TERMO:

O <Contratante>, sediado em <Endereço Contratante>, CNPJ nº <CNPJ Contratante>,doravante denominado CONTRATANTE, e, de outro lado, a <Contratada>, sediada em <Endereço Contratada>, CNPJ nº <CNPJContratada>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO Nº <n° contrato / ano> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na **Política de Segurança da Informação** da CONTRATANTE;

Resolve celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES,** doravante TERMO, vinculado Ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira- DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições especificas para regulamentar as obrigações a serem observadas pela CONTRATADA , no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE – por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes – Segundo a Politica de Segurança da Informação.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, as estabelecidos os seguintes conceitos e definições:

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades especificas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, cientifico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da Sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V. Contrato Principal: contrato celebrado entre as partes, o qual este TERMO DE COMPROMISSO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

São consideradas como informação sigilosa, toda e qualquer informação escrita ou oral revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo

INFORMAÇÃO abrangera toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how,* técnicas, especificações, relatórios, publicações, compilações, código fonte de programas de computador na integra ou em partes, fórmulas desenhos, projetos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre a atividade da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominadas INFORMAÇÕES, a que, diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

§ 1º - Comprometem-se as partes a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

§ 2° - As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste Termo de Compromisso não serão aplicadas àquelas informações que:

I. Sejam comprovadamente de domínio público no momento da revelação;

II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO DE COMPROMISSO.

§ 1° - A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§ 2º - A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO DE COMPROMISSO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando a garantir o cumprimento de todas as disposições do presente TERMO DE COMPROMISSO e dará ciência à CONTRATANTE dos documentos comprobatórios.

§ 3º - A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

§ 4º - Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste.

TERMO DE COMPROMISSO

I. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer copias eventualmente existentes.

§ 5º - A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios em prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

§ 6º - A CONTRATADA, na forma disposta no parágrafo primeiro acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras empresas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III. Comunicar À CONTRANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretratável permanecendo em vigor desde a data da sua assinatura até expirar o prazo de classificação da informação que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitara a imediata aplicação das penalidades previstas conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de

responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº 8.666/93.

Cláusula Sétima - DISPOSIÇÕES GERAIS

Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL.

§ 1º - Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

§ 2º - O disposto no presente TERMO DE COMPROMISSO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações tais como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. A CONTRATANTE terá direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II. A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III. A omissão ou tolerância das partes em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO DE COMPROMISSO somente poderá ser alterado mediante TERMO ADITIVO firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO DE COMPROMISSO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessária a formalização de TERMO ADITIVO ao CONTRATO PRINCIPAL;

VIII. Este TERMO DE COMPROMISSO não deve ser interpretada como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES SIGILOSAS para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A contratante elege o foro da cidade de Aparecida de Goiânia – GO, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renuncia expressa a qualquer outro, por mais privilegiado que seja.

DE ACORDO

E, por assim estarem justas e estabelecidas às condições, o presente TERMO DE COMPROMISSO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

CONTRATANTE	**CONTRATADA**
APARECIDA DE GOIANIA, xxx de xxx de 2022	APARECIDA DE GOIANIA, xxx de xxx de 2022

Nome Cargo	Nome Cargo

ANEXO II

TERMO DE CIENCIA INDIVIDUAL **CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO**	
IDENTIFICAÇÃO DO CONTRATO:	
Nº CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGENCIA CONTRATUAL	

TERMOS:

O (s) funcionário (s) abaixo qualificado (s) declara(m) ter pleno conhecimento de sua(s) responsabilidade (s) no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas, bem como sobre todas as informações que eventualmente ou por força de sua(s) função (ões) venha (m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do

CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.
OBSERVAÇÕES:
DE ACORDO E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIENCIA é assinado em 02 (duas) vias de igual teor e um só efeito.
APARECIDA DE GOIÂNIA , XX de xxx de 2022.
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S):

NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA