CODEMGE
Companhia de Desenvolvimento de Minas Gerais

POLÍTICA CORPORATIVA

PC 004 – Política de Segurança da Informação

REGISTRO DAS REVISÕES

Nº	Data	MOTIVO DAS REVISÕES
0	**06/10/2017**	Criação da Política
1	**12/06/2018**	Alterações realizadas: a) acrescentado no tópica 8.6 - Política de Backups, página 22 itens VI e VII o Procedimento em relação as caixas de e-mails de colaboradores desligados.
2	**18/12/2018**	Revisão para padronização da norma e adequação à reestruturação societária.
3	**20/03/2020**	Atualização da Política: i) atualização item 8.6 VI e VII; e ii) atualização do item 8.4 – alteração do item IV e acréscimo do item VII.
4	**19/06/2020**	Acréscimo do item 8.7 – Segurança Cibernética e definições relacionadas e do item 8.8 – Plano de Contingência de TI
5	**26/05/2021**	Atualização da PSI em detrimento da elaboração da Política de Privacidade, sendo alterados os seguintes itens: 3) Fundamentação Legal e Normativa: Inclusão da Lei Geral de Proteção de Dados e Política de Privacidade; 4) Definições: Inclusão do conceito dos termos Dados Pessoais, Dados Pessoais Sensíveis, Comitê de Segurança da Informação, Cookie e Tratamento de Dado Pessoal; 5) Princípio: Inclusão do item VII; Responsabilidades: Inclusão dos itens 6.1 VII, 6.1 VIII, 6.2 V, 6.5 e demais incisos; 7) Diretrizes: alteração dos itens: III, VI e VII; inclusão do item 8.4 na íntegra; inclusão do item 8.5.VIII e inclusão do item 8.11; 9) Disposições Finais: inclusão da Política de Privacidade.
6	**25/05/2022**	Ajustes relacionados às mudanças de organograma da CODEMGE, no intuito de verificar se havia menção a algum setor que tenha sido extinto; adequação aos padrões definidos na IN 059 e para prever o uso de ferramenta de monitoramento do uso dos equipamentos da empresa.
7	**11/12/2023**	-Adequações na PSI seguindo as diretrizes apontadas pela Consultoria em Segurança da Informação, como parte do plano de ação para mitigação dos riscos de segurança da informação. São elas: **Item 8.5 (inclusão do item V)** - Bloqueio dos logins de colaboradores inativos por mais de 90 dias.

		Item 8.6 (inclusão do item XV) - Bloqueio do acesso à VPN por meio de computadores pessoais; - Adequação da sigla e nome da gerência que mudou de “GETIN-Gerência de Tecnologia da Informação” para “GETID-Gerência de Tecnologia e Inteligência de Dados”

VERIFICAÇÃO	**APROVAÇÃO**
DATA: 11/12/2023 Vagner Augusto Monteiro Rabelo **Gerência de Tecnologia e Inteligência de Dados**	**DATA: 14/12/2023** **Ata da 240ª Reunião de Diretoria**
ESTE PROCEDIMENTO ENTRA EM VIGOR NA DATA DE SUA APROVAÇÃO.	
REQUER TREINAMENTO: SIM X NÃO	

SUMÁRIO

1. ABRANGÊNCIA:

Esta política se aplica a todos os empregados, administradores, conselheiros, acionistas e, na medida do cabível, a terceiros e quaisquer outras pessoas que prestem serviços à Codemge e tenham acesso ao ambiente de tecnologia da informação da Empresa.

Onde for mencionado, Codemge ou Empresa entende-se Codemge, suas subsidiárias e filiais.

2. FINALIDADE:

Estabelecer as linhas-mestras a serem observadas na implementação da segurança da informação, formalizando todos os aspectos relevantes para a proteção, o controle e o monitoramento dos ativos

de informação da Empresa, de acordo com os requisitos do negócio e com as leis e regulamentações vigentes.

3. **FUNDAMENTAÇÃO LEGAL E NORMATIVA**

a) **Lei nº 12.527, de 18 de novembro e 2011**: Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

b) **Lei Estadual nº 22.257, de 27 de julho 2016**: Estabelece a estrutura orgânica da administração pública do Poder Executivo do Estado e dá outras providências.;

c) **Lei nº 13.709, de 14 de agosto de 2018:** Lei Geral de Proteção de Dados Pessoais (LGPD)

d) **Decreto 45.969**, **de 24 de maio de 2012**: Regulamenta o acesso à informação no âmbito do Poder Executivo **Estadual**Ementa sem negrito];

d) **Decreto nº 47021, de 12 de julho de 2016**: Institui comitê para elaboração e acompanhamento da Política de Gestão da Informação no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo Estadual.;

e) **PC 016** - Política de Privacidade da Codemge

4. **DEFINIÇÕES:**

Para melhor compreensão desta política, ficam estabelecidos os seguintes conceitos e definições:

I. **Ameaça:** evento com potencial intrínseco de comprometer os objetivos da organização, acarretando danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas e/ou imprevisíveis.

II. **Ameaça cibernética:** são estratégias digitais que usam os crimes cibernéticos para entrar na rede de uma empresa. Elas podem sequestrar ou acessar informações confidenciais, no intuito de obter benefícios econômicos, que podem trazer consequências graves para a empresa. São exemplos: *malware, ransomware, phishing*.

III. **Ataque cibernético:** é qualquer tentativa de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo. É qualquer tipo de manobra ofensiva voltada para sistema de
informações de computadores, infraestruturas, redes de computadores ou dispositivos de computadores pessoais.

IV. **Ativo:** qualquer bem, material ou intangível, dotado de valor para a organização.

V. **Backup:** cópias de segurança de arquivos.

VI. **Bots**: (palavra que vem da redução de "*robots*") são programas que executam tarefas pré-programadas e muitas vezes repetitivas. Os bots maliciosos são programas que causam problemas a um computador ou a um dispositivo móvel, igual aos vírus, porém com uma diferença, eles podem ser reprogramados para realizarem várias tarefas.

VII. **Cavalo de Troia:**é um tipo de malware que, frequentemente, está disfarçado de *software* legítimo. Eles podem ser empregados por criminosos virtuais e hackers para tentar obter acesso aos sistemas dos usuários. Em geral, os usuários são enganados por alguma forma de engenharia social para carregar e executar cavalos de Troia em seus sistemas.

VIII. **Codemge**: compreende a Companhia de Desenvolvimento de Minas Gerais, suas filiais e subsidiárias.

IX. **Colaborador:** Toda e qualquer pessoa física que realize atividades de interesse da Codemge e de suas subsidiárias, sob regime celetista ou em cargo comissionado, bem como prestadores de serviços terceirizados.

X. **Comitê de Segurança da Informação (CSI):** órgão colegiado de natureza consultiva e de caráter permanente, instituído por meio da Portaria Codemig 41/17, que tem por finalidade formular e

conduzir diretrizes para a PSI, analisar periodicamente sua efetividade e propor normas e mecanismos institucionais visando a melhoria contínua.

XI. **Controle:** mecanismos de gerenciamento de riscos, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou jurídica.

XII. ***Cookie*:** é um arquivo que contém um identificador (uma sequência de letras e números), armazenado pelo navegador. O identificador é enviado de volta ao servidor toda vez que o navegador solicita uma página do servidor. Os *cookies* normalmente não contêm informações que identifiquem pessoalmente um usuário, mas as informações pessoais armazenadas sobre o usuário podem estar vinculadas àquelas armazenadas e obtidas de *cookies*.

XIII. ***Cracking*:** ruptura de um sistema de segurança por meio da utilização de *software*, cuja utilização vise à transformação de programas em versões limitadas, seja no tocante à sua funcionalidade ou tempo de uso.

XIV. **CSI:** sigla referente às iniciais de Comitê de Segurança da Informação.

XV. **Dados pessoais:** informação relacionada a pessoa natural identificada ou identificável.

XVI. **Dados pessoais sensíveis:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de
caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

XVII. **Evento de segurança da informação:** ocorrência identificada em um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

XVIII. ***Firewall*:** é uma solução de segurança baseada em *hardware* ou *software* (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

XIX. **Incidente de segurança da informação:** um incidente de segurança da informação é indicado por um simples evento ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

XX. **Informação:** conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que esteja inserido, físico ou virtual, ou da forma pela qual seja veiculado.

XXI. **Lei Geral de Proteção de Dados (LGPD):** a Lei Geral de Proteção de Dados Pessoais (LGPD), de número 13.709/18, que entrou em vigor em agosto de 2020, dispõe, conforme o artigo 1º, sobre o tratamento de dados pessoais, por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

XXII. ***Malware*:** é um *software* mal-intencionado que tem como objetivo se infiltrar em um sistema de informações sem o consentimento do seu proprietáriocom o intuito de causar danos, alterações ou roubo de informações (confidenciais ou não). Há diferentes tipos de *malware*, como os cavalos de Troia, *worms, bots, spyware, ransomware*, entre outros.

XXIII. **PSI:** sigla corresponde às iniciais de Política de Segurança da Informação.

XXIV. ***Phishing*:** Também conhecido como roubo de identidade. É uma fraude eletrônica, na qual o criminoso cibernético tenta obter informações confidenciais de forma fraudulenta. Normalmente, é realizado por falsificação de e-mail ou mensagem instantânea, e muitas vezes, direciona usuários a inserir informações pessoais em um site falso, que corresponde à aparênciado site legítimo. Esse método é muito usado para roubar senhas e números de cartões de crédito, entre outros dados confidenciais.

XXV. ***Ransomware***: é um *malware* que restringe o acesso a determinadas informações ou a determinadas funções do sistema infectado e pede um resgate em troca da remoção dessa restrição. É muito semelhante a um sequestro digital.

XXVI. **Risco:** combinação da probabilidade de ocorrência ou materialização de um evento e de suas consequências.

XXVII. **Segurança cibernética**: é um conjunto de ações sobre pessoas, tecnologias e processos contra ataques cibernéticos. Inclui as práticas para proteger as informações armazenadas nos computadores e aparelhos de computação e transmitidas através das redes de comunicação, incluindo a internet e telefones celulares.

XXVIII. **Segurança da Informação:** proteção da informação contra ameaças à sua confidencialidade, integridade, disponibilidade e autenticidade, visando minimizar os riscos e maximizar a eficiência e a efetividade das ações.

XXIX. ***Spyware*:**como indica o termo em inglês, é um *software* espião que costuma ser instalado no celular ou no computador sem o consentimento do usuário. O programa monitora as atividades online, o histórico e os dados pessoais, para repassar as informações para terceiros. Esse tipo de *malware* é um dos mais perigosos, pois ele busca informações confidenciais que podem ser usadas para diversos fins, inclusive para roubo de senhas pessoais, informações bancárias ou de cartões de crédito.

XXX. **Tratamento de dado pessoal:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XXXI. **VPN:** sigla para o termo em inglês *Virtual Private Network* (Rede Privada Virtual). Trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores através de uma rede pública, como a Internet.

XXXII. **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

XXXIII. ***Worm*:** é um tipo de malware mais perigoso que um vírus comum, pois sua propagação é rápida e ocorre sem controle da vítima. Assim que ele contamina um computador, o programa malicioso cria cópias de si mesmo em diferentes locais do sistema e se espalha para outras máquinas, seja por meio de Internet, mensagens, conexões locais, dispositivos USB ou arquivos. O objetivo, em geral, é roubar dados do usuário ou de empresas.

5. PRINCÍPIOS:

5.1 A PSI da Codemge está fundamentada nos seguintes princípios:

I. **Confidencialidade**: garantia de que a informação será acessada somente por aqueles que tiverem autorização específica;

II. **Integridade**: garantia da não violação das informações, com o objetivo de protegê-las contra alteração, gravação, duplicação, armazenagem ou exclusão indevida, acidental ou proposital;

III. **Disponibilidade**: garantia de que as informações estejam acessíveis aos usuários segundo sua demanda e em conformidade com a Política de Segurança;

IV. **Conformidade**: garantia de que o processo e o sistema estarão em conformidade com as normas e regulamentações respectivas;

V. **Autenticidade**: garantia da autenticidade da origem da informação, de modo que não tenha sofrido alterações entre a origem (geração) e o destino (consumidor da informação);

VI. **Não repúdio**: garantia de que o emissor da informação não poderá refutar ou negar sua autoria.

VII. **Privacidade**: garantia de que os dados pessoais e sensíveis serão tratados com o devido sigilo e proteção, com acesso somente a pessoas autorizadas, e vinculado a finalidades específicas, amparada pela LGPD.

5.2 A Empresa se compromete a implementar um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*, garantindo a Política de Segurança da Informação. Os controles serão estabelecidos, implementados, monitorados, analisados, criticados e melhorados, quando necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

5.3 Autoridades, empregados, estagiários, prestadores de serviços terceirizados e quaisquer outros destinatários ou usuários de informações da Codemge sujeitam-se às diretrizes, normas e

procedimentos de segurança da informação de que trata esta Política e serão responsáveis por garantir a segurança das informações a que tenham acesso.

5.4 A Política de Segurança da Informação da Codemge foi baseada na norma ABNT NBR ISSO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

6. RESPONSABILIDADES

6.1 Dos Colaboradores em Geral

I. Conhecer e cumprir as diretrizes estabelecidas nesta Política e demais documentos que compõem a Política de Segurança da Informação.

II. Informar aos membros do CSI as situações, de seu conhecimento, que comprometam a segurança das informações da Codemge.

III. Quando da criação e/ou modificação de informação no exercício das funções qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da Codemge, não devendo ser considerada como pessoal, particular, mesmo que arquivadas em pasta pessoal.

IV. É proibido compartilhar ou negociar suas credenciais (ID, senha e crachá);

V. Haverá responsabilização integral do (s) colaborador (es) que der (em) causa a eventuais danos ou prejuízos à Codemge em decorrência da inobservância dos preceitos e diretrizes ora referenciados.

VI. Não divulgar a pessoas não autorizadas informações confidenciais da Codemge, seja por meio digital, verbal, por meio de ligações telefônicas ou
presencialmente, estando o colaborador dentro ou fora das instalações da empresa.

VII. Não divulgar a pessoas não autorizadas informações relacionadas a pessoas físicas sejam elas empregados ou prestadores de serviços cujos dados a Codemge tenha acesso, observando os dispositivos da LGPD.

VIII. Dar ciência aos prestadores de serviços sobre as diretrizes estabelecidas nesta Política e demais documentos que a compõem.

6.2 Dos Gestores de Pessoas e/ou Processos

No que concerne à presente política, os gestores de pessoas e/ou processos envidarão os melhores esforços para adotar e disseminar as seguintes condutas:

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

II. Orientar os colaboradores e terceiros sob sua responsabilidade, quanto ao cumprimento dos Regulamentos, Normas e Procedimentos que compõem a Política de Segurança da Informação.

III. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação da Codemge.

IV. Não divulgar a pessoas não autorizadas informações confidenciais da Codemge seja por meio digital, verbal, por meio de ligações telefônicas ou presencialmente, estando o gestor dentro ou fora das instalações da empresa.

V. Não divulgar a pessoas não autorizadas informações relacionadas a pessoas físicas sejam elas empregados ou prestadores de serviços cujos dados a Codemge tenha acesso, observando os dispositivos da LGPD.

6.3 Do Comitê de Segurança da Informação

O Comitê de Segurança da Informação tem as seguintes atribuições:

I. Acompanhar, avaliar e formular propostas normativas, procedimentos complementares à PSI e políticas de uso dos recursos de tecnologia da informação, tais como:

a) Utilização do correio eletrônico;

b) Gestão de acesso aos sistemas corporativos;

c) Controle de acesso à Internet;

d) Controle de acesso à rede;

e) Utilização de equipamentos de tecnologia da informação;

f) Utilização de programas e aplicativos;

g) Utilização de armazenamento lógico;

h) Monitoração e auditoria de recursos tecnológicos;

i) Controle de acesso físico; e

j) Contingência e Continuidade do Negócio.

II. Propor a adoção de medidas corretivas e procedimentais necessárias à prevenção de situações de vulnerabilidade à Segurança da Informação.

III. Propor ações de conscientização e capacitação de pessoal, visando à difusão dos conhecimentos, conferindo efetividade à PSI.

IV. Solicitar, sempre que necessário, a realização de auditorias em relação ao uso dos recursos de tecnologia da informação, no âmbito da Empresa.

V. Receber e analisar eventuais ocorrências de descumprimento das normas referentes à Política de Segurança da Informação desta Companhia, propondo as medidas cabíveis e apresentando parecer à Diretoria.

VI. Buscar o alinhamento dos objetivos institucionais e de Tecnologia da Informação com a Segurança da Informação.

6.4 Da Alta Direção

A Alta Direção da Codemge, representada pelo Diretor Presidente e pelos demais Diretores, terá as seguintes atribuições:

I. Deliberar sobre questões relacionadas ao planejamento de políticas e estratégias direcionadas à Segurança da Informação.

II. Prover os meios necessários, visando à ampla divulgação das ações de Segurança da Informação da Codemge.

III. Designar os integrantes do Comitê de Segurança da Informação.

6.5 Dos Prestadores de Serviços Terceirizados

I. Conhecer e cumprir as diretrizes estabelecidas nesta Política e demais documentos que compõem a Política de Segurança da Informação.

II. Não compartilhar ou negociar suas credenciais (ID, senha e crachá);

III. Não divulgar a pessoas não autorizadas informações confidenciais da Codemge, seja por meio digital, verbal, por meio de ligações telefônicas ou presencialmente, estando o prestador de serviço dentro ou fora das instalações da empresa, observando inclusive os dispositivos da LGPD.

7. **DIRETRIZES GERAIS:**

I. O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas pela Auditoria Interna, buscando a certificação do cumprimento dos requisitos de segurança da informação.

II. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

III. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de TI, a qual, por sua vez, fica responsável pelo encaminhamento posterior ao Comitê de Segurança da Informação e à Gerência de Integridade, Conformidade e Gestão de Riscos (GICOR), para análise.

IV. Os sistemas de informação e as aplicações da Codemge devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

V. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

VI. Os contratos emitidos ou firmados pela Codemge deverão conter Cláusula ou Acordo de Confidencialidade como condição imprescindível para que seja concedido acesso aos ativos de informação disponibilizados pela Companhia.

VII. Os contratos emitidos ou firmados pela Codemge, em que exista a possibilidade de acesso e tratamento de dados pessoais, deverão conter cláusulas específicas de privacidade, conforme definido na Política de Privacidade e os dispositivos da LGPD.

VIII. A responsabilidade pela segurança da informação deve ser comunicada na fase de contratação dos colaboradores e terceirizados, que deverão ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de se reduzir riscos.

IX. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, devem ser condicionados à ciência e ao aceite dos termos desta Política.

8. **DIRETRIZES ESPECÍFICAS:**

8.1 Controle de acesso lógico:

I. Os usuários da Codemge são responsáveis por todos os atos praticados por meio de suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.

II. A identificação do usuário, qualquer que seja o meio e a forma, é pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

III. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

IV. A definição e a manutenção das senhas de acesso aos ambientes computacionais da Codemge e suas subsidiárias deve seguir a norma **IN 032 – Senhas de Acesso ao Ambiente computacional**, vigente desde 1º de junho de 2017.

V. Havendo incidente relevante, investigação, sindicância, procedimento administrativo, desligamento ou outra situação a que o usuário esteja submetido, que exija medida restritiva para fins de salvaguardar os ativos da Codemge, deve-se garantir, da forma mais rápida possível, o bloqueio de acesso do usuário em questão.

8.2 Utilização do correio eletrônico:

O uso do correio eletrônico da Codemge destina-se a fins corporativos e relacionados às atividades do colaborador no âmbito da Companhia. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, em obediência a padrões morais e éticos, de modo a não representar qualquer prejuízo à Codemge e também não cause impacto no tráfego da rede.

Embora os servidores de e-mail da Codemge estejam protegidos contra vírus e códigos maliciosos, alguns preceitos e recomendações são de observância obrigatória pelos usuários:

I. Estar ciente de que os vírus atuais são enviados automaticamente, o que significa que um e-mail recebido de um cliente, parceiro ou amigo não terá sido necessariamente enviado pelos mesmos, de forma voluntária.

II. Não abrir anexos caso não tenha certeza absoluta do conteúdo ou da procedência do e-mail.

III. Desconfiar de todos os e-mails com assuntos estranhos ou inusitados em língua nacional ou estrangeira.

IV. Não reenviar e-mails do tipo “corrente”, “aviso de vírus”, “criança desaparecida”, “criança doente”, “pague menos em alguma coisa”, “não pague alguma coisa”, ou similares, independentemente da vontade do destinatário de receber tais mensagens.

V. Não utilizar o e-mail para assédio ou perturbação de terceiros, seja através de linguagem utilizada, frequência ou tamanho das mensagens.

VI. Não enviar e-mail a qualquer pessoa que não o deseje receber, especialmente caso o destinatário solicite a interrupção de envio e-mails, devendo o usuário acatar tal solicitação e cessar o envio de qualquer e-mail.

VII. Não divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário do referido ativo de informação.

VIII. Não falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas.

IX. Não produzir, transmitir ou divulgar qualquer mensagem ou comunicação que:

a) Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Codemge.

b) Contenha grande quantidade de mensagens de e-mail ("*spam*") que gere sobrecarga dos servidores ou reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.

c) Contenha linguagem inapropriada em respostas aos e-mails comerciais, tais como abreviações de palavras.

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

e) Vise a obtenção de acesso não autorizado a outro computador, servidor ou rede.

f) Vise a interrupção de um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

g) Vise a burla de qualquer sistema de segurança.

h) Vise a observação secreta ou ao assédio de outro usuário.

i) Vise ao acesso de informações confidenciais sem explícita autorização do proprietário.

j) Vise acessar indevidamente informações que possam causar prejuízos aqualquer pessoa.

k) Contenha anexo(s) superior(es) a 10 MB para envio (interno e internet) e 10 MB para recebimento (internet).

l) Tenha conteúdo considerado impróprio, obsceno ou ilegal.

m) Contenha manifestação preconceituosa baseada em gênero, orientação sexual, etnia, deficiência física ou mental ou quaisquer outras formas de preconceito.

n) Contenha teor ou fins políticos relacionados a qualquer esfera, seja local, regional ou nacional (propaganda política).

o) Inclua material protegido por direitos autorais sem a permissão de seu titular.

X. As mensagens internas de correio eletrônico deverão incluir assinatura padronizada, com o seguinte formato:

[NOME COMPLETO] I[Cargo]
email@codemge.com.brI+55 31 [Telefone Corporativo]

CODEMGE
Companhia de Desenvolvimento de Minas Gerais

Rodovia Papa João Paulo II, 4001
6º Andar, Edifício Gerais
Cidade Administrativa de Minas Gerais
31630-901 | Belo Horizonte – MG
www.codemge.com.br

Classificação: ( )Reservada (X)Restrita ( )Pública
Grupo de Acesso: destinatários desta mensagem

XI. Conforme definido e detalhado na **IN 023- Diretrizes para Classificação e Tratamento da Informação**, abaixo da assinatura do e-mail, deve constar a classificação da correspondência, conforme exemplo acima. A classificação da informação e o grupo de acesso devem ser avaliados conforme os critérios estabelecidos na referida norma, a cada envio de e-mail. O exemplo acima é meramente ilustrativo.

8.3 Controle de acesso à Internet:

I. Este controle visa ao desenvolvimento de um comportamento ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da Codemge com a Internet ofereça um grande potencial de benefícios, também propicia uma série de riscos significativos para os ativos de informação.

II. Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a Codemge, em total conformidade com o ordenamento jurídico vigente, reserva-se o direito de monitorar e registrar todos os acessos a ela.

III. Ao monitorar a rede interna, a Codemge pretende garantir a integridade dos dados e dos programas.

IV. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será tida por inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor para providências cabíveis.

V. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Codemge cooperará ativamente com as autoridades competentes.

VI. O acesso à internet é restrito à observância das seguintes condições:

a) O uso recreativo da internet não deverá se dar no horário de expediente.

b) Somente a navegação de *sites* é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente à equipe de Tecnologia da Informação com prévia autorização da chefia imediata.

c) O acesso a *sites* com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados será monitorado e sujeito às penalidades cabíveis, de acordo com as normas internas da Codemge, bem como a legislação trabalhista, cível e penal aplicáveis.

d) O acesso a *site* de redes sociais, tais como *Facebook, Twitter, Instagram,* ou similares será bloqueado, por padrão. O acesso poderá ser concedido pela equipe de suporte da Gerência de Tecnologia e Inteligência de Dados, desde
que seja justificado o uso a trabalho, mediante autorização formal da chefia imediata do colaborador.

e) É proibido o uso de ferramentas P2P, tais como, *Torrent*, *Popcorn* ou similares.

f) É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, sendo cabível a aplicação das penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei, independentemente de dolo ou culpa.

g) Somente poderão ser baixados programas ligados diretamente às atividades da empresa, salvo em casos devidamente justificados e autorizados pela chefia imediata do colaborador. É proibido utilizar os recursos da empresa para fazer o download ou distribuição de *software* ou dados ilegais ou não legalizados.

h) Colaboradores com acesso à Internet não poderão efetuar upload de qualquer *software* licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem a expressa autorização do gerente responsável pelo *software* ou pelos dados.

8.4 Política de *Cookies*:

I. Em todos os sites disponibilizados pela Codemge que fizerem o uso de *cookies* deverá conter um aviso informando sobre a utilização do recurso, para que o usuário tenha a opção de prosseguir ou de desistir da navegação.

II. É vedada a coleta de dados pessoais e/ou sensíveis por meio de *cookies* nos *sites* desenvolvidos pela Codemge.

III. O Titular dos Dados poderá configurar seu navegador para que bloqueie a utilização dos *cookies* não essenciais durante a sua navegação.

IV. Os sites desenvolvidos/contratados pela Codemge fazem uso de *cookies* dos seguintes tipos:

a) *Cookies* essenciais: necessários para que o site funcione, permitindo navegar e utilizar as suas funcionalidades. Sem eles, o site não funcionaria da forma desejada e o Titular dos Dados não poderia utilizar alguns serviços ou recursos.
b) *Cookies* de preferências: são aqueles que coletam informações sobre as escolhas e preferências do titular dos dados pessoais, permitindo que a página lembre as configurações e possa personalizar algumas informações.
c) *Cookies* analíticos: recolhem informações sobre a utilização do site, permitindo melhorar seu funcionamento. Por exemplo, os *cookies* analíticos mostram quais são as páginas mais visitadas no site e ajudam a registar quaisquer dificuldades que os usuários sintam na navegação.
d) *Cookies* de marketing: são *cookies* de publicidade utilizados para fins de marketing.

8.5 Gestão de acesso aos sistemas corporativos:

I. Todos os sistemas de informação da Codemge devem ter um ou mais administradores, dentre os colaboradores da equipe de analistas da Gerência de Tecnologia e Inteligência de Dados, responsáveis pela concessão dos privilégios de acesso às informações, mediante autorização da chefia imediata do usuário para o qual será dado o acesso.

II. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento da Codemge ou bloqueados, em caso de afastamento.

III. Caberá aos gerentes a definição, com apoio da equipe de TI, quanto à matriz de acessos dos colaboradores da gerência às funcionalidades dos sistemas.

IV. Caberá à GETID realizar o bloqueio do acesso à rede, ao e-mail e aos sistemas corporativos dos colaboradores afastados por mais de 30 (trinta) dias. Neste caso, a GERHU deverá comunicar à GETID, por meio do sistema de Help Desk, todos os afastamentos que se enquadrarem nesta situação, informando o período em que o colaborador ficará afastado das suas atividades, para que seja configurado o período de bloqueio. O fato de bloquear o acesso à rede garantirá, automaticamente, o bloqueio do acesso aos sistemas corporativos, uma vez que o login de acesso a esses sistemas está integrado ao login da rede através do recurso *Active Directory* (AD). Portanto, não será necessário realizar o bloqueio específico de acesso aos sistemas, neste caso.

V. Os colaboradores ativos, cujo usuário permanecer inativo por mais de 90 (noventa) dias, terão o seu login bloqueado, bem como o acesso aos sistemas corporativos, integrados ao Active Directory (AD).

VI. Deverão ser criados e implementados controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Companhia julgar necessário, para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas utilizados na Codemge.

VII. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento e homologação.

VIII. Anualmente, os gestores de cada área deverão realizar a revisão dos perfis de acesso dos colaboradores da sua gerência aos sistemas corporativos da Companhia. A GETID encaminhará para cada gestor (Gerente ou Diretor) um documento no qual serão listados os grupos de acesso associados a cada colaborador. O gestor avaliará a pertinência ou não dos acessos e informará os acessos que deverão ser mantidos ou retirados. Mediante a resposta do gestor, a GETID fará as adequações necessárias.

IX. Visando à proteção e ao monitoramento dos dados pessoais e sensíveis armazenados nos sistemas de informação, nas funcionalidades que armazenam esses dados, deverão ser habilitados os logs de auditoria, para que se possa ter a rastreabilidade dos acessos em caso de vazamento destes.

8.6 Utilização de equipamentos de tecnologia da informação:

I. Os equipamentos disponibilizados aos colaboradores são de propriedade da Codemge, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Empresa.

II. É proibida a utilização de todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da GETID ou de seu subordinado.

III. Os computadores deverão conter versões do *software* antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a equipe de suporte técnico da Gerência de Tecnologia e Inteligência de Dados.

IV. 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.

V. A pasta PÚBLICO ou similar não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível.

VI. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo, que não seja realizado por um técnico da equipe de suporte técnico de TI da Codemge ou por terceiros devidamente contratados para o serviço.

VII. O usuário deverá efetuar, periodicamente, manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis.

VIII. As estações de trabalho possuem códigos internos que permitem que elas sejam identificadas e monitoradas por tudo que venha a ser executado pelo usuário, podendo acarretar-lhe a respectiva responsabilidade, em caso de violação das regras de segurança estabelecidas.g

IX. Ao se ausentar do local de trabalho, recomenda-se que o usuário feche todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e efetuar o logout/logoff da rede ou o bloqueio do desktop por meio de senha.

X. Não poderão ser utilizados, nos equipamentos da Codemge, programas que não tenham sido cedidos pela empresa ou cujo uso não tenha sido prévia e formalmente autorizado. Na hipótese de necessidade de instalação de programas que não estejam de acordo com padrão normal de funcionamento da empresa, será necessário obter autorização da chefia imediata do colaborador da área interessada e pela equipe de suporte em Tecnologia da Informação.

XI. Material de natureza ilícita (pornográfica, racista dentre outros) não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede.

XII. É vedada a instalação, utilização, duplicação ou armazenamento de MP3, filmes, fotos e *softwares* com direitos autorais ou qualquer outro tipo de pirataria.

XIII. Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a algum servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

XIV. É vedado o uso de Pen Drives ou CDs de fora da Empresa. Caso isso seja extremamente necessário, deve-se encaminhar o dispositivo para a equipe de suporte técnico de TI, que fará a verificação e descontaminação de vírus, se for o caso.

XV. É vedada a conexão a VPN por computadores pessoais. O acesso à VPN só será autorizado por meio de computadores fornecidos pela empresa.

XVI. Deverão ser reportados à equipe técnica quaisquer comportamentos suspeitos do equipamento ou dos sistemas, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.

XVII. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

8.7 Política de Backups:

I. 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 há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

II. As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

III. As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

IV. O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

V. Na situação de erro de *backup* e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

VI. Em caso de desligamento de algum colaborador, a Gerência de Recursos Humanos deverá comunicar o fato à Gerência de TI, por e-mail. Na medida do possível, a comunicação deverá ser feita com antecedência mínima de dois dias

úteis da data do desligamento, cabendo à equipe técnica da Gerência de TI manter sigilo até a formalização para toda a empresa.

A Gerência de TI realizará um *backup* da caixa de e-mail e da pasta de arquivos pessoal do colaborador, existente na rede corporativa. Em virtude de questões de espaço em disco no storage, do tempo para realização do procedimento e do melhor local de armazenamento dos dados, não serão feitos backup, por padrão, dos dados armazenados nas máquinas dos usuários.

O gestor do funcionário desligado deverá, no prazo de 2 (dois) dias úteis da data informada para desligamento do funcionário, acionar à GETID caso seja necessária a retenção de dados e/ou informações presentes nos recursos computacionais utilizados pelo empregado ou quaisquer outras ações que o gestor julgar necessárias, tais como: backup da máquina do colaborador, redirecionamento de e-mails, resposta automática de e-mail informando o desligamento, concessão de acesso à caixa de e-mail e aos backups para outro(s) empregados.

Os dados serão retidos em *backup*, conforme a seguinte política de retenção:

a) Estagiários: não haverá **backup**, salvo mediante solicitação formal do gestor;
b) Analistas e técnicos: armazenamento do backup por 90 dias;
c) Gerentes, Diretores, Vice-Presidente e Presidente: armazenamento do *backup* por 5 anos.

VII. No caso do desligamento de prestadores de serviços terceirizados, a Gerência Administrativa deverá comunicar, por e-mail, a Gerência de Recursos Humanos, que por sua vez deverá comunicar a Gerência de TI, que deverá seguir os mesmos procedimentos adotados para os empregados, conforme descrito no item anterior.

8.8 Segurança Cibernética:

Visando à proteção contra ataques cibernéticos, a Codemge deverá utilizar ferramentas e procedimentos para prevenir, detectar e/ou mitigar os riscos gerados por esses ataques, que podem causar prejuízos, gerar instabilidade e até mesmo a indisponibilidade do ambiente computacional, tais como:

I. Manter os *softwares* de antivírus atualizados em todas as estações de trabalho.

II. Toda e qualquer instalação de *software* nas máquinas dos usuários deverá ser feita somente por técnicos e analistas de Tecnologia da Informação, de modo que não deve ser concedido acesso de administradores das estações de trabalho aos demais colaboradores. Desta forma, não será possível a instalação de *softwares* sem o consentimento e acompanhamento da GETID.

III. Uso de proxy para bloqueio de acesso a sites não autorizados. Tratamentos de exceção deverão ser formalizados por meio do CAC e devidamente autorizados pela chefia imediata.

IV. Uso de *Firewalls*, que impedem a entrada de IPs não autorizados na rede.

V. Uso de VPN para acessos externos: todos os acessos externos à rede corporativa, sejam de pessoas externas à empresa ou de colaboradores acessando de casa devem ser estabelecidos de forma segura, por meio de VPN (Virtual Private Network), cuja função é garantir o tráfego de dados de forma segura e permitir o acesso remoto protegido à rede interna de uma empresa.

VI. Os acessos aos sistemas web corporativos devem ser realizados utilizando protocolos HTTPS (*HyperTextTransferProtocolSecure*).

VII. Todos os servidores críticos tais como: servidores de aplicação dos sistemas corporativos, servidores de banco de dados, servidores de e-mails, entre outros, devem ser hospedados em *data centers* seguros. Atualmente, os servidores críticos da Codemge estão hospedados na Prodemge, cujos acessos são monitorados constantemente.

VIII. Devem ser realizados backups diários de todos os servidores críticos.

8.9 Plano de Contingência de TI:

O Plano de Contingência de TI define um conjunto de ações preventivas e corretivas para tornar possível a continuidade das operações das áreas de negócio, no que se refere aos recursos de Tecnologia da Informação, no caso da ocorrência de um evento ou desastre que impossibilite a utilização parcial ou total desses recursos. O plano de contingência da Codemge está descrito na IN 052 – Plano de Contingência de TI.

8.10 Classificação das informações:

A IN 023 – DIRETRIZES PARA CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO
estabelece as diretrizes básicas para classificação e tratamento das informações, de acordo com sua sensibilidade e criticidade para a Codemge e suas subsidiárias, visando ao estabelecimento de níveis adequados de proteção, nos âmbitos internos e externos da Empresa.

8.11 Tratamento de Dados Pessoais:

Todos os colaboradores e terceiros que estiverem atuando em nome da Codemge e tratando dados pessoais para tal deverão observar as diretrizes, orientações, bases legais e finalidades definidas na Política de Privacidade que deverão ser aplicadas em conjunto com a Política de Segurança da Informação.

9. DISPOSIÇÕES FINAIS

Essa política deve ser lida e aplicada em conjunto com as normas IN 023 – Diretrizes para Classificação e Tratamento da Informação, IN 032 – Senhas de Acesso ao Ambiente computacional, a PC 002 Política Corporativa Compliance e a PC 016 – Política de Privacidade.

10. APROVAÇÃO

Esta política entra em vigor na data de sua aprovação revogadas as disposições em contrário.

Documento assinado eletronicamente por **Vagner Augusto Monteiro Rabelo**, **Gerente**, em 22/12/2023, às 12:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **79336641** e o código CRC **A192C84B**.

Referência: Processo nº 5030.01.0002577/2023-46 SEI nº 79336641