Seção 2

Atos

ATO DA MESA DIRETORA Nº 125, DE 2020

Dispõe sobre a Política de Segurança da Informação Digital da Câmara Legislativa do Distrito Federal – POSID CLDF.

A MESA DIRETORA DA CÂMARA LEGISLATIVA DO DISTRITO FEDERAL, no uso de suas atribuições regimentais, RESOLVE:

TÍTULO I

DAS DISPOSIÇÕES GERAIS

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º Este Ato estabelece um conjunto de medidas institucionais a serem tomadas para:

I - cumprir o estabelecido no Ato da Mesa Diretora nº 57, de 30 de junho de 2016, que regulamenta o acesso à informação pública no âmbito da Câmara Legislativa do Distrito Federal – CLDF;

II - instituir Normas da Política de Segurança da Informação Digital da Câmara Legislativa do Distrito Federal.

CAPÍTULO II

DO OBJETIVO

Art. 2º O objetivo da Política de Segurança da Informação Digital - POSID é estabelecer normas gerais, princípios, diretrizes estratégicas, responsabilidades, competências e subsídios para a implantação do sistema de gestão de segurança da informação digital, a fim de viabilizar e assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas pela CLDF.

CAPÍTULO III

DO ESCOPO

Art. 3º O escopo da Política de Segurança da Informação Digital da Câmara Legislativa do Distrito Federal pretende:

I - definir os princípios para a proteção dos dados, informações e conhecimentos gerados na CLDF, sendo a base para o estabelecimento dos padrões, normas e procedimentos de segurança da informação digital;

II - estabelecer o comprometimento da Mesa Diretora e demais autoridades da CLDF vinculadas a esta Política com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação digital da CLDF;

III - sensibilizar, conscientizar e orientar os usuários sobre os dados e informações providas pela CLDF para o uso seguro dos ativos de informação digital, bem como dos ambientes físicos ou informatizados envolvidos;

IV - viabilizar e assegurar a confidencialidade, disponibilidade, integridade e autenticidade da informação digital.

Art. 4º A POSID terá a seguinte abrangência:

I - deverá ser adotada por todas as unidades da CLDF, tanto as de caráter político quanto às de caráter técnico-administrativo;

II - será observada por Deputados, servidores, estagiários, prestadores de serviços e todos os demais indivíduos que tenham acesso à informação digital da CLDF.

CAPÍTULO IV

DA CONCEITUAÇÃO GERAL

Art. 5º Para os efeitos da terminologia usada neste Ato, entende-se por:

I - administrador de *backup*: servidor efetivo responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de *backup* e restauração;

II - agente público: todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente à CLDF;

III - áreas seguras e instalações físicas críticas: áreas físicas e instalações classificadas como de acesso restrito, em função de ações e processos ali desempenhados, de informações ali armazenadas e da possibilidade de impactos em pessoas ou atividades de negócio;

IV - autenticidade: propriedade que assegura que determinada informação digital seja atribuída a um usuário ou processo;

V - *backup* diferencial incremental: modalidade de *backup* na qual todos os dados criados e modificados desde a última execução de *backup*, tanto incremental quanto completa, são copiados;

VI - *backup full* ou completo: modalidade de *backup* na qual todos os dados são copiados integralmente;

VII - banco de dados: é uma coleção de dados inter-relacionados, representando informações sobre um domínio específico;

VIII - caixa postal: área de armazenamento de mensagens eletrônicas, podendo ser pessoal, se ligada a um usuário, ou institucional, se referente a uma unidade organizacional da CLDF ou a um projeto, grupo de trabalho, comitê;

IX - certificado digital: assinatura eletrônica, em formato digital, com validade jurídica, que garante proteção a operações eletrônicas;

X - classificação da informação digital: processo que assegura que a informação digital seja adequadamente rotulada, de forma a indicar as necessidades, as prioridades e os níveis esperados de proteção quanto a seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade;

XI - Comitê de Segurança da Informação Digital – CSID: grupo de servidores com a responsabilidade de assessorar a implementação das ações de segurança da informação digital no âmbito da CLDF;

XII - confidencialidade: propriedade que assegura que a informação digital seja acessada somente por processos e usuários autorizados;

XIII - controlador de domínio: servidor que responde a requisições seguras de autenticação dentro de um domínio Windows;

XIV - criptografia: conjunto de princípios e técnicas utilizadas para cifrar a escrita, tornando-a ininteligível para os que não tenham acesso às convenções combinadas;

XV - disponibilidade: propriedade que assegura que a informação digital esteja disponível aos processos e usuários autorizados, sempre que necessário;

XVI - domínio da organização: base de identificação de um ente na internet, sendo, no caso da CLDF, o domínio cl.df.gov.br;

XVII - endereço de correio eletrônico ou endereço eletrônico: identificação única de uma caixa postal na rede, composta com a utilização do nome do endereço e do domínio da organização;

XVIII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: grupo de servidores com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores no âmbito da CLDF;

XIX - gestão da continuidade de negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem;

XX - gestão de riscos de segurança da informação digital: conjunto de processos que objetiva

identificar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação digital, priorizando seu tratamento com base em critérios para aceitação de riscos compatíveis com os objetivos institucionais;

XXI - incidente de segurança da informação digital: evento que comprometa ou possa comprometer a segurança ou violação a normas de segurança da informação digital ou à legislação vigente referente ao assunto, que acarrete efeito negativo à CLDF;

XXII - informação digital: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato digital;

XXIII - informação sigilosa: categoria de informação enquadrada em uma das hipóteses de sigilo previstas na Constituição, em leis, no Regimento Interno da Câmara Legislativa do Distrito Federal, em Atos da Mesa Diretora da Câmara Legislativa do Distrito Federal, ou em outras resoluções, cujo acesso deve ser restrito a pessoas que, por seu cargo ou função, tenham necessidade de tomar conhecimento de seu teor;

XXIV - integridade: propriedade que assegura que a informação digital seja alterada somente por processos e usuários autorizados;

XXV - *logs* de aplicativos: processo de registro de eventos relevantes num sistema computacional;

XXVI - *logs* de dados: processo de registro de eventos relevantes num sistema computacional;

XXVII - mensagem eletrônica: informação criada pelos usuários que trafega pelos sistemas eletrônicos de comunicação;

XXVIII - nome do endereço da caixa postal: identificação dada ao recurso dentro da organização, podendo ser:

a) no caso de uma caixa postal pessoal, a identificação do usuário na rede (*login*);

b) no caso de uma caixa postal institucional, a sigla da unidade ou o nome do comitê, grupo de trabalho, a atividade em desenvolvimento;

XXIX - retenção: período de tempo em que o conteúdo da mídia de *backup* deve ser preservado;

XXX - risco: combinação da probabilidade da ocorrência de um evento e de suas consequências;

XXXI - segurança da informação digital: conjunto de ações com a finalidade de proteger a informação digital contra os vários tipos de ameaças, a fim de garantir a continuidade do negócio e mitigar seus riscos;

XXXII - servidor de arquivos: área de armazenamento que possibilita o compartilhamento de pastas e arquivos com o devido controle de acesso, segurança e auditoria para seus usuários;

XXXIII - servidor de e-mail: serviço de hospedagem no qual os e-mails são armazenados;

XXXIV - sistema de gestão da segurança da informação digital: conjunto de recursos, estruturas, normas, métodos e ferramentas cuja finalidade é estabelecer, implementar, operar, monitorar, analisar criticamente e melhorar a segurança da informação digital;

XXXV - SPAM: mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo;

XXXVI - tratamento da informação digital: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação digital;

XXXVII - unidades organizacionais (UOs): tipo de objeto de diretório contido no domínio para o qual podem ser atribuídas configurações de Política de Grupos de Usuários ou delegar autoridade administrativa;

XXXVIII - usuários colaboradores: empregados de empresas prestadoras de serviço à CLDF, estagiários, servidores do GDF lotados na Chefia Executiva de Assuntos Legislativos e conveniados que utilizem a estrutura física e recursos da CLDF;

XXXIX - usuários externos: pessoas físicas ou jurídicas que tenham acesso, de forma autorizada,

aos recursos e instalações da CLDF e que não sejam caracterizadas como usuários internos ou usuários colaboradores;

XL - usuários internos: deputados, servidores efetivos e comissionados.

CAPÍTULO V

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º As ações da Política de Segurança da Informação Digital deverão observar os seguintes requisitos legais e normativos:

I - Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

II - Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade;

III - Lei Distrital nº 2.572, de 20 de julho de 2000, que dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática;

IV - Decreto Distrital nº 25.750, de 12 de abril de 2005, que regulamenta a Lei nº 2.572, de 20 de julho de 2000;

V - Ato da Mesa Diretora nº 15, de 7 de fevereiro de 2007, que dispõe sobre a informatização da Câmara Legislativa do Distrito Federal.

CAPÍTULO VI

DOS PRINCÍPIOS

Art. 7º São princípios da POSID:

I - transparência das informações recebidas, produzidas, processadas, armazenadas e transmitidas pela Câmara Legislativa do Distrito Federal;

II - garantia da disponibilidade, integridade, autenticidade e confiabilidade das informações recebidas, produzidas, processadas, armazenadas e transmitidas pela CLDF;

III - definição de normas e procedimentos específicos de segurança da informação digital, bem como a implementação de controles e de processos para seu atendimento;

IV - planejamento das ações de segurança da informação digital por meio de sistema de gestão da segurança da informação digital que considere processos de trabalho e recursos humanos, materiais e tecnológicos;

V - avaliação contínua de conformidade de modo a identificar riscos advindos do descumprimento de legislações, normas e procedimentos de segurança da informação digital;

VI - avaliação da eficácia e da eficiência da aplicação das normas que subsidiam as ações de segurança da informação digital na CLDF.

CAPÍTULO VII

DAS NORMAS GERAIS

Seção I

Da Classificação e Tratamento da Informação Digital

Art. 8º A classificação da informação digital, disposta em norma específica, é pressuposto para seu correto tratamento e tem por objetivo assegurar nível adequado de proteção em relação a suas propriedades.

Parágrafo único. Os controles físicos, administrativos e tecnológicos necessários para assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade das informações deverão ser implementados conforme a classificação a elas atribuída.

Art. 9º As informações institucionais eletrônicas ficarão armazenadas em servidores de rede e

bases de dados sob gestão da Coordenadoria de Modernização e Informática - CMI.

Parágrafo único. As informações institucionais eletrônicas armazenadas nos servidores de rede estarão preservadas por meio de cópia de segurança sob gestão da CMI e mantidas em local protegido, conforme disposto no Capítulo VI do Título II.

Seção II

Do Tratamento de Incidentes de Rede

Art. 10. Cabe à CMI a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação digital no âmbito da rede corporativa da CLDF.

Art. 11. Será definida uma Equipe de Tratamento de Incidentes de Rede - ETIR, seguindo critérios a serem definidos pela CMI, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais na CLDF.

Art. 12. Todo agente público é responsável por notificar imediatamente, ao Comitê de Segurança da Informação Digital - CSID, incidentes que afetem a segurança da informação digital ou o descumprimento da POSID para que as providências necessárias sejam adotadas a fim de sanar as causas.

Art. 13. Os incidentes de segurança da informação digital devem ser gerenciados, monitorados e registrados.

Seção III

Da Gestão de Riscos de Segurança da Informação Digital

Art. 14. O processo de análise e avaliação de riscos é pressuposto para o estabelecimento de controles adequados ao tratamento dos principais riscos de segurança da informação digital.

Parágrafo único. Todos os mecanismos de segurança da informação digital deverão ser selecionados mediante observação dos fatores de risco, da tecnologia e dos aspectos de economicidade.

Art. 15. Deve ser assegurado que a informação digital receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Parágrafo único. Serão adotadas medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Art. 16. Devem-se identificar e implementar medidas de proteção objetivando minimizar, eliminar, aceitar ou transferir os riscos a que estão sujeitos os ativos, processos, projetos e serviços.

Art. 17. Devem ser criados e estabelecidos mecanismos de proteção dos ativos de informação digital contra acesso, modificação, destruição ou divulgação não autorizados.

Art. 18. A CMI estabelecerá critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da Câmara Legislativa do Distrito Federal, assim como o controle, administração e requisitos mínimos desses recursos, zelando pela segurança da informação digital.

Seção IV

Da Gestão da Continuidade de Negócios

Art. 19. A gestão da continuidade de negócios tem por objetivo, em relação à segurança da informação digital, garantir níveis adequados de disponibilidade, integridade, autenticidade e confidencialidade às informações essenciais ao funcionamento dos processos críticos de negócio da CLDF.

Seção V

Da Gestão de Incidentes de Segurança da Informação Digital

Art. 20. A gestão de incidentes de segurança da informação digital deve:

I - priorizar a restauração do funcionamento adequado dos recursos de informação digital da Câmara Legislativa do Distrito Federal;

II - estabelecer responsabilidades e procedimentos de gestão para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação digital;

III - acordar os objetivos para a gestão de incidentes de segurança da informação digital com a alta direção e garantir que a Equipe de Tratamento e Resposta a Incidentes em redes computacionais - ETIR entenda as prioridades da organização ao tratar esses incidentes.

Seção VI

Da Gestão de Áreas Seguras e Instalações Físicas Críticas

Art. 21. A gestão de áreas seguras e instalações físicas críticas tem por objetivo, em relação à segurança da informação digital, prevenir danos e interferências nas instalações da CLDF que possam causar perda, furto ou comprometimento de informações.

Parágrafo único. As instalações físicas onde as informações críticas estão armazenadas deverão ter controle de acesso apropriado, protegidas por perímetros de segurança definidos, além da proteção de instalações de suporte, como a infraestrutura de suprimento de energia e de cabeamento.

Seção VII

Da Auditoria e Conformidade

Art. 22. A utilização dos recursos de rede e o acesso aos sistemas da CLDF são passíveis de monitoramento e auditoria, devendo os arquivos de *logs* ser analisados regularmente, preferencialmente com *softwares* específicos para monitoramento do uso dos sistemas, bem como mecanismos que permitam a rastreabilidade desse uso.

Seção VIII

Dos Controles de Acesso

Art. 23. O acesso aos recursos de rede e aos sistemas da CLDF deverá ser disponibilizado de acordo com as normas de segurança da informação digital em vigor e mediante a autenticação do usuário.

Parágrafo único. As regras para autenticação de usuários estão descritas no Capítulo I do Título II.

Art. 24. A concessão de acesso lógico e físico aos ativos de informação digital deverá ser sistematizada, a fim de se evitar a quebra de segurança, observado o seguinte:

I - o acesso ao correio eletrônico da CLDF, bem como o seu uso, só deverá ser possível mediante o uso de autenticação pessoal e deverá seguir as especificações estabelecidas no Capítulo II do Título II;

II - o acesso às informações armazenadas nos servidores de rede e nos computadores das unidades organizacionais da CLDF deverá seguir as especificações estabelecidas no Capítulo III do Título II;

III - o acesso aos serviços de internet na CLDF deverá seguir as especificações estabelecidas no Capítulo IV do Título II;

IV - o acesso ao serviço de arquivos da CLDF, bem como a sua utilização, só deverá ser possível mediante o uso de autenticação pessoal e deverá seguir as especificações estabelecidas no Capítulo V do Título II.

Art. 25. Deve-se assegurar que todos os tipos de permissões de acesso aos ativos de informação digital da Câmara Legislativa do Distrito Federal, fornecidos mediante senha, crachá, certificado digital, biometria ou outros tipos de permissão, sejam pessoais e intransferíveis.

Art. 26. O acesso de usuários colaboradores e usuários externos a dados, documentos ou instalações que contenham informações sensíveis, sigilosas ou de acesso restrito deve ser precedido de solicitação formal por parte de autoridade responsável e de assinatura de termo de confidencialidade.

Seção IX

Do Uso dos Recursos de Informação Digital

Art. 27. Os recursos de informação digital da Câmara Legislativa do Distrito Federal devem ser utilizados para os fins institucionais, respeitada a legislação vigente, a POSID, as normas de segurança da informação digital, as obrigações contratuais e os direitos autorais.

Art. 28. Deve-se zelar para que os recursos de informação digital colocados à disposição dos usuários sejam utilizados apenas para as finalidades a que se destinam.

Art. 29. Deve-se garantir que os processos de trabalho e ativos de informação digital sob responsabilidade ou uso dos usuários estejam adequadamente protegidos.

Art. 30. A cultura da segurança da informação digital deve ser consolidada na Câmara Legislativa do Distrito Federal, por meio da capacitação e certificação de profissionais em âmbito interno e externo, do incentivo ao autodesenvolvimento, da participação em grupos de trabalho, seminários, palestras, reuniões e outros eventos que contribuam para o constante processo de compartilhamento e absorção do conhecimento nos domínios da segurança da informação digital no contexto da CLDF.

CAPÍTULO VIII

DAS PENALIDADES

Art. 31. O descumprimento ou violação de algum item desta POSID caracterizará infração funcional e resultará no bloqueio temporário ou permanente de privilégios de acesso aos recursos da rede, além das penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais sanções cíveis e penais cabíveis.

CAPÍTULO IX

DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I

Do Comitê de Segurança da Informação Digital - CSID

Art. 32. A CLDF deverá instituir o Comitê de Segurança da Informação Digital, ao qual competirá:

I - planejar, coordenar, acompanhar, monitorar e avaliar, em conjunto com os setores competentes, a implementação da POSID e das normas complementares e as ações de segurança da informação digital;

II - analisar e formular ações de segurança da informação digital para a Câmara Legislativa do Distrito Federal, em conformidade com a legislação e as recomendações e boas práticas pertinentes;

III - fomentar a cultura de segurança da informação digital na CLDF;

IV - planejar a capacitação dos usuários em segurança da informação digital;

V - apresentar propostas de compatibilização das normas da Câmara Legislativa do Distrito Federal que tenham impacto em segurança da informação digital com a POSID;

VI - prestar assessoria em segurança da informação digital à CLDF;

VII - propor alocação de recursos necessários às ações de segurança da informação digital;

VIII - definir metodologias, processos e tecnologias em segurança da informação digital, contemplando a gestão de riscos, o uso dos recursos, a gestão da continuidade de negócios e a gestão de incidentes de segurança da informação digital;

IX - propor recursos necessários às ações de segurança da informação digital;

X - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação digital;

XI - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança no âmbito da Câmara Legislativa do Distrito Federal;

XII - formular, avaliar, monitorar e divulgar indicadores de segurança da informação digital no âmbito da CLDF;

XIII - propor alterações na POSID, quando necessário, e revisá-la anualmente.

Parágrafo único. A condução do CSID será responsabilidade de seu Coordenador, que poderá indicar o Gestor de Segurança da Informação ou acumular as funções.

Seção II

Do Gestor de Segurança da Informação Digital - GSID

Art. 33. Compete ao Gestor de Segurança da Informação Digital:

I - coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;

II - promover cultura de segurança da informação digital;

III - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

IV - propor recursos necessários às ações de segurança da informação digital;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação digital;

VI - propor normas e procedimentos relativos à segurança da informação digital no âmbito da CLDF;

VII - monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança.

Parágrafo único. O gestor de Segurança da Informação Digital deverá ser um servidor lotado na Coordenadoria de Modernização e Informática.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR

Art. 34. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais tem por competência:

I - tratar e encaminhar os incidentes de rede tomando as medidas necessárias para reprimir as ameaças, minimizando os impactos e evitando futuras ocorrências, restaurando a disponibilidade, a integridade, a autenticidade e confidencialidade das informações digitais;

II - suspender o acesso dos usuários ou processos aos recursos de tecnologia da informação digital, quando evidenciados riscos à segurança da informação, notificando de imediato o Gestor de Segurança da Informação Digital;

III - registrar, classificar e filtrar as notificações de incidentes de segurança;

IV - guardar as evidências para auxiliar a perícia computacional;

V - investigar as causas dos incidentes no ambiente computacional.

Seção IV

Das Unidades Administrativas da CLDF

Art. 35. Compete às unidades administrativas da Câmara Legislativa do Distrito Federal:

I - primar pela proteção dos ativos de informação digital sob sua responsabilidade contra acesso, modificação, destruição ou disseminação não autorizados;

II - zelar para que os recursos de informação digital colocados à sua disposição sejam utilizados apenas para as finalidades a que se destinam;

III - garantir que os processos de trabalho e ativos de informação digital sob sua responsabilidade estejam adequadamente protegidos;

IV - cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

V - reportar as ocorrências de incidentes de segurança da informação digital de que tenham conhecimento ao Comitê de Segurança da Informação Digital.

Seção V

Dos Usuários Internos, Externos e Colaboradores

Art. 36. Compete aos usuários internos, externos e colaboradores da Câmara Legislativa do Distrito Federal:

I - zelar para que os recursos de informação digital colocados à sua disposição sejam utilizados apenas para as finalidades a que se destinam;

II - comunicar ao Comitê de Segurança da Informação Digital qualquer descumprimento da POSID de que tenha conhecimento.

TÍTULO II

DAS POLÍTICAS DE USO

CAPÍTULO I

DAS POLÍTICAS DE USO DE CONTAS NA REDE

Art. 37. O acesso aos recursos de Tecnologia da Informação - TI destina-se à execução das atividades necessárias ao funcionamento da CLDF e à prestação de serviços aos usuários e será efetuado com a utilização de contas e respectivas senhas de acesso que serão criadas e gerenciadas pela Coordenadoria de Modernização e Informática.

Art. 38. O acesso aos recursos de TI será disponibilizado aos usuários internos, externos e colaboradores.

Art. 39. A solicitação da criação da conta de rede deverá ser realizada pelo titular da unidade ou substituto legal, mediante formulário próprio, ou pelo gestor do contrato no caso das empresas prestadoras de serviço à CLDF.

Art. 40. As contas dos usuários colaboradores serão configuradas para expiração automática ao fim da vigência do contrato, que deverá ser informada no formulário.

Art. 41. Para evitar a expiração automática das contas dos usuários colaboradores deverá ser solicitada a renovação com antecedência mínima de 72 horas, informando o novo prazo de validade do contrato.

Art. 42. É responsabilidade do gestor do contrato dos usuários colaboradores solicitar o cancelamento da conta de rede caso haja o desligamento do prestador de serviço ou estagiário antes do prazo final.

Art. 43. O nome do usuário e a senha são individuais e intransferíveis, sendo de responsabilidade do titular manter a confidencialidade de sua senha pessoal, não podendo permitir ou colaborar com o acesso aos recursos de TI da CLDF por terceiros.

Art. 44. Será bloqueado o acesso do usuário aos recursos da rede quando:

I - o servidor for exonerado, cedido ou aposentado;

II - o contrato de trabalho de usuário colaborador for rompido;

III - a senha provisória não for alterada no período de 30 dias;

IV - a rede interna não for acessada no período de 120 dias;

V - a rede interna sofrer mais de 3 tentativas sucessivas malsucedidas;

VI - o sistema detectar suspeita de violação das normas de uso por terceiros.

Art. 45. No caso do artigo anterior, as contas permanecerão bloqueadas até que haja nova solicitação para desbloqueio por parte do usuário.

Art. 46. O usuário é responsável por todos os acessos realizados por meio de sua conta e pelos eventuais custos e consequências decorrentes da má utilização dos recursos de TI.

Art. 47. Não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede, excetuando-se os casos de necessidade, justificados e acompanhados de parecer da CMI, acerca da

possibilidade de aceitação dos riscos associados.

Art. 48. As senhas devem ser configuradas com as seguintes exigências:

I - possuir no mínimo 8 caracteres;

II - combinar letras maiúsculas e minúsculas, números e símbolos;

III - ter validade máxima de 360 dias;

IV - ser significativamente diferente das 3 últimas senhas cadastradas.

Art. 49. Caso o usuário esqueça a senha, poderá solicitar cadastro de outra comparecendo à CMI portando documento de identificação com foto.

Art. 50. As contas de rede serão compostas por nome e sobrenome, sendo a forma padrão o nome e o último sobrenome, separados por ponto (".").

Art. 51. Caso a forma padrão incorra em homonímia com conta já existente, será escolhida forma alternativa, nesta ordem:

I - nome e qualquer sobrenome, separados por ponto (".");

II - nome e dois sobrenomes juntos, separados estes daquele por ponto (".");

III - nome e último sobrenome acrescidos de um numeral, separados por ponto (".").

Art. 52. Os administradores de rede devem possuir contas e senhas individualizadas com privilégios administrativos e somente deverão utilizá-las para o desempenho de suas atividades.

Art. 53. A admissão ao grupo de administração, bem como a concessão de contas e senhas de administração de recursos de TI de altíssimos privilégios, como "root" e "administrator", serão autorizadas e controladas pelo chefe da Seção de Infraestrutura de Tecnologia da Informação - SEINF.

CAPÍTULO II

DAS POLÍTICAS DE USO DO CORREIO ELETRÔNICO

Art. 54. Os serviços de correio eletrônico da CLDF serão norteados pelos seguintes princípios:

I - as caixas postais de correio eletrônico são de propriedade da CLDF e serão disponibilizadas para os usuários como instrumento de trabalho utilizado na realização de atividades de caráter profissional;

II - os usuários que utilizam os serviços de correio eletrônico devem considerar que o conteúdo das mensagens criadas, trafegadas e armazenadas no âmbito da organização será classificado de acordo com o grau de sigilo estabelecido pela Política de Segurança da Informação Digital adotada pela CLDF e que as mensagens terão sua privacidade definida conforme as práticas de segurança da informação digital em vigor.

Art. 55. O processo de concessão de caixas postais será orientado a partir dos seguintes parâmetros:

I - caixas institucionais criadas para as unidades administrativas da CLDF e para os deputados;

II - novas caixas institucionais criadas a partir da posse de novos deputados distritais ou da criação de unidades organizacionais;

III - composição do endereço eletrônico das caixas postais das unidades administrativas utilizando como nome do endereço a sua sigla (exemplo: drh@cl.df.gov.br);

IV - composição do endereço das caixas postais dos gabinetes parlamentares utilizando o prefixo "dep." seguido do nome parlamentar (exemplo: dep.nomesobrenome@cl.df.gov.br);

V - criação de outras caixas institucionais para atender às diversas demandas das unidades organizacionais;

VI - criação de novas caixas postais pessoais ou institucionais mediante solicitação formalizada por documento encaminhado pela unidade responsável, assinado pelo titular da unidade ou por seu substituto legal;

VII - endereço eletrônico das novas caixas institucionais indicado pela unidade responsável, obedecendo às seguintes disposições:

a) no caso de caixa postal de gabinete parlamentar, o nome do endereço eletrônico terá o seu prefixo composto por "dep" seguido pelo nome utilizado pelo deputado mais o caractere ponto (".") terminando com a identificação da caixa informada pela unidade organizacional (p.ex., para criar a caixa postal da agenda do Deputado X, o nome do endereço eletrônico seria depX.agenda);

b) no caso de caixa postal de unidade administrativa, o nome do endereço eletrônico terá como prefixo a sigla da unidade seguida do caractere ponto (".") terminando com a identificação informada pela unidade (p.ex.: para criar a agenda da Coordenadoria de Modernização e Informática - CMI, o nome do endereço eletrônico seria CMI.agenda);

c) mediante solicitação formal dos responsáveis pelas caixas encaminhada para análise e eventual registro por parte da CMI, um endereço eletrônico alternativo poderá ser atribuído a uma caixa postal para facilitar sua identificação (p.ex.: no caso do Setor de Biblioteca - sigla SBIB, endereço principal: sbib@cl.df.gov.br; endereço alternativo: biblioteca@cl.df.gov.br), podendo o remetente optar pelo envio da mensagem para qualquer dos endereços, a qual será recebida na mesma caixa postal;

VIII - caixas postais pessoais criadas para os seguintes usuários com conta na rede interna da CLDF:

a) deputados distritais;

b) servidores efetivos;

c) servidores comissionados;

d) empregados de empresas contratadas, na forma de serviço terceirizado, que necessitem de acesso a uma caixa postal para realizar o objeto de seus contratos;

e) estagiários;

f) servidores da administração pública requisitados;

g) outros usuários indicados pela Mesa Diretora.

IX - nome do endereço eletrônico das caixas postais pessoais composto pela identificação de seu usuário na rede interna da CLDF (p.ex.: para usuário de conta identificado por nome.sobrenome: endereço eletrônico "nome.sobrenome@cl.df.gov.br");

X - caixas postais classificadas em diversas categorias, que terão limites distintos para a área de armazenamento de mensagens, de tamanho máximo de anexo de mensagem e de número simultâneo de destinatários para uma mesma mensagem, com o objetivo de racionalizar o gerenciamento de recursos disponíveis para atender aos serviços de correio eletrônico;

XI - promoção de caixa postal para categoria superior mediante solicitação formal fundamentada da unidade organizacional responsável, realizada conforme a disponibilidade de recursos de TI existente para atender aos serviços de correio eletrônico.

Art. 56. Os usuários que utilizam os serviços de correio eletrônico devem seguir as seguintes regras:

I - as caixas postais pessoais são de exclusiva responsabilidade dos usuários detentores da conta na rede associada ao recurso, e somente por estes devem ser acessadas, cabendo-lhes zelar para que as informações referentes ao login e senha não sejam divulgadas a terceiros;

II - as caixas postais institucionais são de responsabilidade dos titulares das unidades administrativas ou dos gabinetes parlamentares, conforme o caso, e das pessoas designadas para tal finalidade, devendo a solicitação de acesso a elas ser formalizada em formulário próprio assinado pelo responsável, com especificação dos usuários que poderão utilizá-las e dos privilégios que terão, podendo ser de gerenciamento da caixa postal somente, ou também de envio de mensagens em nome dela;

III - o acesso à caixa postal será realizado, preferencialmente, por meio de produtos do fornecedor da solução de correio eletrônico em operação na CLDF, para os quais o setor responsável pelo atendimento aos usuários da CMI dará suporte operacional, vedado o suporte a outros produtos para o

uso em computadores ou equipamentos móveis;

IV - sempre que possível, os usuários das caixas postais deverão realizar a remoção de mensagens desnecessárias para preservar o espaço de armazenamento disponível e para facilitar a administração de suas rotinas de trabalho;

V - para a preservação da segurança de seu equipamento e da infraestrutura de rede da CLDF, os usuários das caixas postais, ao receberem mensagens de origem duvidosa, deverão verificar a real identidade do remetente antes de abrir o conteúdo e de clicar em links suspeitos;

VI - os usuários das caixas postais não poderão enviar mensagens em massa (SPAM) para diversos destinatários contendo propagandas, correntes, pedidos não autorizados ou pirâmides, nem receber, guardar ou transmitir mensagens individuais ou em massa contendo informações de caráter impróprio ou ilegal, abordando temas como a pornografia, a violência, o preconceito e o terrorismo;

VII - as unidades que prestam serviços que incluam encaminhar mensagens em massa para diversos usuários por meio de aplicativos ou programas instalados em computadores específicos devem solicitar seu cadastramento para que a infraestrutura de suporte aos serviços de correio eletrônico permita a transmissão das mensagens.

CAPÍTULO III

DAS POLÍTICAS DE USO DA REDE DE DADOS

Art. 57. As informações a serem armazenadas nos servidores de rede e nos computadores das unidades organizacionais consistem em *logs* de dados, documentos digitais, bancos de dados e e-mails.

Art. 58. A Coordenadoria de Modernização e Informática manterá por 1 ano os *logs* de dados armazenados nos servidores de rede da CLDF.

Art. 59. As informações guardadas nos computadores das unidades organizacionais são de responsabilidade dos usuários da rede da CLDF.

Parágrafo único. A CMI não é responsável pelo *backup* das informações armazenadas nesses equipamentos.

Art. 60. A solicitação de informações armazenadas nos servidores de rede e nos computadores das unidades organizacionais não precisará de fundamentação quando originada:

I - por deputado distrital no exercício do mandato parlamentar, conforme disposto no art. 15, inciso XI, do Regimento Interno da CLDF;

II - pela Comissão Permanente de Tomada de Contas Especial e Sindicância – CPTCES, para instauração de processo de tomada de contas especial, conforme previsto no art. 231 da Lei Complementar 840/2011 e artigos 16, IV e V e 18, I, do Ato da Mesa Diretora 31/2017;

III - por comissão parlamentar de inquérito – CPI, na investigação, análise e exame de irregularidades, de acordo com o art. 2º da Lei Federal 1.579/1952 e art. 68, § 3º, inciso III, da Lei Orgânica do Distrito Federal;

IV - pelo Serviço de Informação do Cidadão - SIC, sob responsabilidade da Ouvidoria, atendendo ao disposto na Lei Federal 12.527/2011 – Lei de Acesso à Informação, na Lei Distrital 4.990/2012 e no Ato da Mesa Diretora 57/2016;

V - por decisão judicial.

Art. 61. A solicitação de informações deverá ser formalmente fundamentada quando originada pelos demais órgãos integrantes da estrutura organizacional da CLDF.

Parágrafo único. Os Deputados Distritais, as CPI's e a CPTCES, quando solicitarem informações para fins diferentes dos citados no artigo anterior, deverão fundamentar a solicitação.

Art. 62. Salvo para o cumprimento de decisão judicial, todas as solicitações de informações armazenadas nos servidores de rede e nos computadores das unidades organizacionais deverão ser autorizadas pelo Gabinete da Mesa Diretora, na forma deste ato, para que a CMI possa atender à solicitação.

Parágrafo único. Nos pedidos de informações devem estar especificados os usuários, o período e o local de armazenamento dos dados solicitados, com a indicação dos servidores de rede ou computadores das unidades organizacionais.

Art. 63. As solicitações de informações armazenadas nos servidores de rede e nos computadores das unidades organizacionais da CLDF devem ser feitas mediante memorando.

Art. 64. Após avaliação da CMI quanto às recomendações contidas no art. 9º do Ato da Mesa Diretora 57/2016 – Lei de Acesso à Informação, os dados serão fornecidos na forma em que se encontram armazenados, sem tratamento, interpretação ou análise.

Art. 65. Salvo em cumprimento de decisão judicial, todas as informações requisitadas serão encaminhadas diretamente ao Gabinete da Mesa Diretora, que dará prosseguimento ao atendimento da solicitação.

CAPÍTULO IV

DAS POLÍTICAS DE USO DA INTERNET

Art. 66. O acesso à internet disponibilizado pela CLDF aos usuários da rede deve ser utilizado para os interesses de trabalho do Órgão.

Art. 67. A CLDF permite o uso da internet para fins particulares dos usuários da rede, desde que este uso não exceda os limites da ética, do bom-senso e da razoabilidade.

Art. 68. Todos os usuários que acessam a rede local da CLDF podem ter acesso à internet, desde que respeitem os termos estabelecidos neste Ato.

Art. 69. O cancelamento, o bloqueio e o desbloqueio do acesso à internet seguem as condições descritas no Capítulo I deste Título II.

Art. 70. O acesso à internet é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à CLDF por mau uso.

Art. 71. O usuário da rede deverá utilizar a internet de forma a não causar tráfego desnecessário na rede local da CLDF.

Art. 72. O acesso à internet, quando realizado pela rede local nas estações de trabalho ou equipamentos portáteis, não poderá ser feito mediante proxies externos, que permitam burlar as regras de acesso estabelecidas.

Art. 73. Todo serviço disponibilizado na internet, antes de ser disponibilizado na rede local da CLDF, deverá ser avaliado quanto à sua necessidade pelo Comitê de Segurança da Informação Digital - CSID, que deverá considerar os aspectos de segurança, o consumo de recursos tecnológicos e o comprometimento de outros serviços.

Art. 74. É vedada a utilização da internet para:

I - acessar sítios com códigos maliciosos e vírus de computador;

II - acessar sítios com materiais pornográficos ou atentatórios aos valores constitucionalmente protegidos;

III - acessar sítios ou arquivos com conteúdo ilegal ou criminoso ou que façam apologia ao crime, incluindo os de pirataria;

IV - acessar sítios ou arquivos com conteúdo de incitação à violência;

V - realizar *download* de arquivos que não estejam relacionados às necessidades de trabalho da CLDF, em especial arquivos que contenham materiais ilegais ou que não respeitem os direitos autorais;

VI - participar de jogos eletrônicos;

VII - escutar música ou assistir a programas de TV, acessar salas chat exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho da CLDF;

VIII - transferir ou armazenar informações sensíveis da CLDF em sítios com os quais não haja um contrato ou acordo de responsabilidade estabelecido com o Poder Legislativo.

Art. 75. É de responsabilidade da CMI garantir os serviços de transferência e compartilhamento de arquivos com informações da CLDF na internet de forma segura.

Art. 76. O usuário sempre deve certificar a procedência do sítio, verificando, quando cabível, seu certificado digital, principalmente para realizar transações eletrônicas via internet, devendo digitar o endereço do sítio diretamente no browser da estação de trabalho em vez de clicar em link existente em página ou em mensagem de correio eletrônico.

Art. 77. É vedado aos usuários disponibilizar informações de propriedade do CLDF em sítios da internet sem observar sua classificação e o público a que se destina.

Art. 78. Só será permitida a utilização da rede local por máquinas que atendam a todos os requisitos de segurança da informação digital estabelecidos pela CMI.

Art. 79. O acesso à internet deve ser monitorado, podendo ser divulgado e restringido pela CMI quanto a endereço, quantidade, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que esses controles sejam feitos por parâmetros gerais não personalizados, observado ainda o seguinte:

I - a CMI deverá registrar e monitorar os registros de conexão e o acesso às aplicações de internet, de modo a detectar o descumprimento dessas normas de segurança, respeitando o sigilo das informações protegidos por lei;

II - o registro deverá conter, no mínimo, os endereçamentos de origem e destino, data e hora do início e término das conexões, tipo e quantidade do tráfego gerado e outras informações necessárias para a otimização do link e realização de auditoria;

III - os registros de conexão bem como os de acesso às aplicações de internet ficarão guardados, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 ano.

Art. 80. A disponibilização de acesso à internet para o uso de visitantes deverá ser feita mediante cadastro junto ao setor responsável.

Art. 81. O acesso à internet com destino a portas TCP/UDP será limitado àquelas de uso comum e relacionadas ao uso institucional.

Parágrafo único. As exceções ao previsto no caput serão tratadas conforme o caso, e as liberações de acesso poderão ser solicitadas à CMI por memorando, justificando a necessidade.

Art. 82. Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação Digital à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Art. 83. Em casos de quebra de segurança da informação digital por qualquer meio, a ETIR deverá ser imediatamente acionada, para tomar as providências necessárias a fim de sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e ao uso dos recursos de tecnologia da informação.

Art. 84. Os usuários da rede que descumprirem as regras estabelecidas por este Ato poderão ter seu acesso à rede bloqueado até a apuração de responsabilidades.

Art. 85. A CMI poderá adotar, a qualquer momento, medidas excepcionais que sejam necessárias para garantir a segurança, a disponibilidade, a integridade, a confidencialidade e a estabilidade da rede.

CAPÍTULO V

DAS POLÍTICAS DE USO DO SERVIDOR DE ARQUIVOS

Art. 86. O acesso ao Servidor de Arquivos bem como a criação de pastas deverão ser solicitados à CMI pelo responsável do setor mediante formulário específico.

Art. 87. Os acessos serão concedidos em níveis de grupos.

Parágrafo único. Haverá dois grupos de acesso a cada pasta, um de escrita, que terá permissão de criar, modificar e excluir os dados, e outro de leitura, que poderá apenas visualizar o conteúdo.

Art. 88. O nome da pasta será a sigla do setor, observado o seguinte:

I - caso haja necessidade de novas pastas, será utilizado o modelo Sigla do Setor e o Nome Sugerido, separados por um traço inferior ("_");

II - não será permitido dar acesso a subpastas;

III - caso seja imprescindível o acesso a subpasta, deverá ser solicitada, mediante formulário próprio, a criação de outro compartilhamento com a Sigla do Setor e o nome da subpasta, separados por um traço inferior ("_").

Art. 89. No servidor deverão ser gravados apenas arquivos relacionados ao trabalho cotidiano.

Art. 90. É vedada a gravação de dados e informações de natureza particular no servidor de Arquivos.

Parágrafo único. Todas as criações, gravações e exclusões serão auditadas, mantendo-se o histórico por um período de 5 anos para o caso de necessidade de averiguação.

Art. 91. É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas no servidor de Arquivos para garantir o *backup* diário.

Art. 92. Não é permitido o compartilhamento de pastas e arquivos em computadores ou qualquer outro equipamento de TI que não seja no servidor de Arquivos.

Art. 93. Identificada ocorrência em desacordo com o disposto nos artigos anteriores, a Coordenadoria de Modernização e Informática poderá, após notificar o responsável e resguardar as evidências necessárias, excluir ou isolar arquivos e revogar acessos, relatando o fato imediatamente à autoridade responsável pela apuração da infração.

Art. 94. Quando o servidor mudar de lotação e possuir acesso às pastas do setor de lotação anterior, é de responsabilidade do chefe deste comunicar à CMI, mediante formulário próprio, solicitando que as permissões de acesso sejam retiradas.

CAPÍTULO VI

DA POLÍTICA DE USO DO SERVIÇO DE *BACKUP*

Art. 95. São atribuições do Administrador de *Backup*:

I - propor modificações visando ao aperfeiçoamento da política de *backup*;

II - configurar a ferramenta de *backup* e *restore*;

III - criar, testar e manter os *backups* pelo período de retenção;

IV - gerenciar mensagens e *logs* diários dos *backups*, corrigindo os erros de forma que o procedimento de *backup* possa ser completado e os erros eliminados;

V - comunicar à chefia imediata os erros e ocorrências nos *backups*;

VI - testar o *restore* periodicamente e restaurar os *backups* em caso de necessidade;

VII - fazer o carregamento das mídias necessárias para os *backups* programados;

VIII - armazenar as mídias de *backup* em cofre próprio, localizado em prédio diferente do local onde o *backup* é realizado.

Art. 96. São atribuições do Chefe da Seção de Infraestrutura de Tecnologia da Informação – SEINF:

I - contratar ou adquirir os recursos necessários para o armazenamento e para a implementação das rotinas de cópias de segurança;

II - considerar as necessidades, as prioridades e os níveis esperados de proteção quanto a seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade na implementação das rotinas de cópia de segurança, além das normas e práticas vigentes;

III - definir quais diretórios e arquivos serão incluídos no *backup*, tendo como prioridade:

a) arquivos de usuários gravados no Servidor de Arquivos e no Servidor de E-mail;

b) arquivos de *logs* dos aplicativos;

c) arquivos de *logs* de segurança dos Controladores de Domínio e Servidores de Arquivos;

d) informações e configurações de Banco de Dados;

e) arquivos de aplicações desenvolvidas na CLDF;

f) excepcionalmente, qualquer informação que se julgar importante, que esteja armazenada nos Servidores da CLDF.

Art. 97. A retenção dos *backups*, com exceção dos bancos de dados, deve observar os seguintes prazos:

I - diário – 7 últimos dias;

II - semanal – 4 últimas semanas;

III - mensal – 12 últimos meses;

IV - anual – 5 últimos anos.

Art. 98. Os *backups* dos bancos de dados ficarão retidos pelo prazo de:

I - diário – 2 semanas;

II - quinzenal – 1 ano;

III - mensal – 5 anos.

Art. 99. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando-se sempre seu estado de utilização e número de leitura/gravação.

Art. 100. As fitas que forem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou o acesso indevido às informações por pessoas não autorizadas.

Art. 101. A rotina de realização de *backup* obedecerá aos seguintes procedimentos:

I - *backups* com início diário, preferencialmente, às 22h;

II - *backup* diferencial-incremental diário de domingo a sábado, com retenção de 7 dias, com exceção dos bancos de dados que sempre serão *full*;

III - *backup full* semanal com retenção mínima de duas semanas;

IV - *backup full* mensal, na primeira sexta-feira do mês, com retenção de 365 dias;

V - *backup full* anual, na primeira sexta-feira do ano, com retenção de 5 anos.

Parágrafo único. Casos particulares podem ter configurações diferentes desde que devidamente justificados.

Art. 102. As restaurações de cópias deverão ser solicitadas por meio de memorando encaminhado à CMI, observado o seguinte:

I - apenas o chefe ou substituto legal da unidade proprietária da informação poderá solicitar a restauração;

II - deve constar da solicitação, da forma mais precisa possível, a indicação do momento da perda dos dados e do seu caminho completo;

III - preferencialmente, a CMI restaurará os dados para uma pasta diferente da original à qual o solicitante tenha acesso, para que este faça a verificação e a devida organização dos dados restaurados;

IV - a restauração dos arquivos somente será possível nos casos em que tenham sido atingidos pela estratégia de *backup* diária que se inicia às 22h, não sendo passíveis de recuperação no mesmo dia da criação os arquivos criados e eventualmente apagados ou alterados;

V - Após a solicitação, o prazo para resposta acerca da possibilidade de restauração dos dados será de até 3 dias úteis;

VI - caso os arquivos estejam disponíveis e se encontrem armazenados no *robot*, o prazo será de

mais 3 dias úteis para a restauração;

VII - caso sejam informações mais antigas que não estão no *robot*, o prazo será de até 7 dias úteis.

Art. 103. Os *backups* mensais e anuais deverão ser testados no prazo máximo de uma semana após a execução e, caso seja detectada falha no *backup* ou se estiver incompleto, novo *backup* deverá ser executado com vista ao armazenamento

TÍTULO III

DAS DISPOSIÇÕES FINAIS

CAPÍTULO I

DA ATUALIZAÇÃO

Art. 104. Esta Política de Segurança da Informação Digital e todos os instrumentos normativos gerados deverão ser revisados anualmente, ou sempre que se fizer necessário.

CAPÍTULO II

DA DIVULGAÇÃO

Art. 105. A CLDF deverá promover ações permanentes de conscientização dos agentes públicos visando à disseminação das diretrizes e normas estabelecidas nesta Política.

Art. 106. A POSID deverá estar disponível na Intranet da CLDF para conhecimento de todos os servidores.

CAPÍTULO III

DOS CASOS NÃO PREVISTOS E DA VIGÊNCIA

Art. 107. Os casos não previstos neste Ato serão resolvidos pelo Comitê de Segurança da Informação Digital.

Art. 108. Este Ato entra em vigor na data de sua publicação.

Sala de Reuniões, 13 de novembro de 2020.

DEPUTADO RAFAEL PRUDENTE
Presidente

DEPUTADO DELMASSO
Vice-Presidente

DEPUTADO IOLANDO
Primeiro Secretário

DEPUTADO ROBÉRIO NEGREIROS
Segundo Secretário

DEPUTADA JAQUELINE SILVA
Terceira Secretária

Documento assinado eletronicamente por **RODRIGO GERMANO DELMASSO MARTINS - Matr. 00134**, **Vice-Presidente da Câmara Legislativa do Distrito Federal**, em 13/11/2020, às 15:55, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **ROBERIO BANDEIRA DE NEGREIROS FILHO - Matr. 00128**, **Segundo(a) Secretário(a)**, em 13/11/2020, às 16:40, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

00149, **Primeiro(a) Secretário(a)**, em 13/11/2020, às 17:48, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **RAFAEL CAVALCANTI PRUDENTE - Matr. 00139**, **Presidente da Câmara Legislativa do Distrito Federal**, em 16/11/2020, às 15:42, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **JAQUELINE ANGELA DA SILVA - Matr. 00158**, **Terceiro(a) Secretário(a)**, em 17/11/2020, às 18:18, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

A autenticidade do documento pode ser conferida no site:
http://sei.cl.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0
Código Verificador: **0259187** Código CRC: **53EE748E**.