GOVERNO DO DISTRITO FEDERAL

SECRETARIA DE ESTADO DE DESENVOLVIMENTO SOCIAL DO DISTRITO FEDERAL

PORTARIA Nº 39, DE 09 DE NOVEMBRO DE 2021

Dispõe sobre a Política de Segurança da Informação e Comunicações da Secretaria de Estado de Desenvolvimento Social (POSIC/SEDES).

A SECRETÁRIA DE ESTADO DE DESENVOLVIMENTO SOCIAL DO DISTRITO FEDERAL, no uso das atribuições que lhe conferem os incisos I e III do parágrafo único do art. 105 da Lei Orgânica do Distrito Federal, resolve:

Art. 1º Instituir, no âmbito da Secretaria de Estado de Desenvolvimento Social, a Política de Segurança da Informação e Comunicações da SEDES (POSIC/SEDES), regida pelos objetivos, princípios e diretrizes estabelecidos nesta Portaria.

Art. 2º Os Agentes Públicos que tiverem acesso a informações da SEDES estarão sujeitos às diretrizes e aos objetivos desta Política e serão responsáveis por garantir a segurança das informações a que tenham acesso.

CAPÍTULO I

DOS OBJETIVOS

Art. 3º A POSIC/SEDES tem por objetivos:

I. estabelecer os princípios e as diretrizes que devem ser observados na elaboração das normas e na definição de procedimentos relacionados à segurança da informação e às comunicações;

II. definir instruções normativas que prontifiquem a SEDES a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e das informações;

III. atribuir responsabilidades, bem como disseminar boas práticas para o manuseio, o tratamento, o controle e a proteção contra a divulgação, a modificação e o acesso não autorizados a dados e informações.

CAPÍTULO II

DA ABRANGÊNCIA

Art. 4º Esta Política aplica-se a todas as unidades da estrutura administrativa da SEDES e suas diretrizes, normas complementares e manuais de procedimentos devem ser observados por todos os servidores públicos, colaboradores, estagiários, consultores externos e prestadores de serviço.

CAPÍTULO III

CONCEITOS E DEFINIÇÕES

Art. 5º Para fins desta Portaria entende-se por:

I. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do órgão;

II. Acordo de Cooperação: instrumento por meio do qual são formalizadas as parcerias estabelecidas pela administração pública com organizações da sociedade civil para a consecução de finalidades de interesse público e recíproco que não envolvam a transferência de recursos financeiros;

III. Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública. Equipara-se a agente público quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida na Secretaria de Estado de Desenvolvimento Social;

IV. Alta Administração: ocupantes dos cargos de Secretário de Estado, Chefe de Gabinete, Secretário Adjunto, Secretário Executivo e Subsecretários de Estado da SEDES;

V. Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, por meio de danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

VI. Análise de Risco: processo de identificação de ameaças e vulnerabilidades associadas a um ativo de modo a estimar a probabilidade e o impacto na ocorrência de um incidente;

VII. Ativo: é tudo aquilo que tem valor para a organização e consequentemente exige proteção;

VIII. Autenticidade: propriedade segundo a qual a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. Relaciona-se com a confirmação de autoria, a certificação e a originalidade da informação;

IX. Backup / Cópia de Segurança: é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar proteção contra a perda dos originais;

X. CeTIC: é o centro de dados corporativo privado do Distrito Federal, ambiente com soluções integradas de hardware e software, que provê serviços de nuvem corporativa privada, armazenamento de dados, hospedagem de aplicações e sistemas a todos os órgãos e entidades da Administração Direta e Indireta do Distrito Federal, compreendendo os sistemas estruturantes, as bases de dados e os serviços corporativos de tecnologia da informação e comunicação;

XI. Classificação da Informação: é o processo de identificar e definir níveis e critérios de proteção adequados para as informações de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a importância para a organização;

XII. Confidencialidade: garantia de que a informação não esteja disponível ou seja revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XIII. Controle de Acesso: são restrições de acesso a um ativo da organização;

XIV. Controle de Segurança: são práticas de gestão de risco que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades, limitar o impacto de um incidente ou ajudar na sua detecção;

XV. Credencial de segurança / credencial de acesso: certificado, dispositivo ou recurso, tais

como senhas, tokens ou documentos, concedido por autoridade competente, que habilita determinado usuário ou processo a ter acesso a dados ou informações em diferentes graus de sigilo;

XVI. Direito de Acesso: privilégio associado a um usuário para ter acesso a um ativo;

XVII. Disponibilidade: propriedade relativa à acessibilidade e utilização da informação, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

XVIII. Gestor da Informação: servidor que, em virtude de suas funções ou atribuições legais, tenha poder de decisão para identificar e classificar as informações geradas por sua área de gerência;

XIX. Gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação e comunicações no âmbito da SEDES;

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 resida ou da forma pela qual seja veiculado;

XXI. Incidente de Segurança: ocorrência de um ou mais eventos de segurança da informação;

XXII. Integridade: garantia de que a informação e os métodos de processamento não sejam modificados, suprimidos ou destruídos de maneira não autorizada ou acidental, de modo a salvaguardar sua exatidão e completeza;

XXIII. Recursos de Tecnologia da Informação e Comunicação (TIC): conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio de hardware e software, a criação, o acesso, o armazenamento, a transmissão e o processamento de dados e informações;

XXIV. Rede GDFNet: é a rede corporativa metropolitana privada de comunicação de alta velocidade dos órgãos e entidades da Administração Direta e Indireta do Distrito Federal, que interliga as unidades administrativas e as unidades operacionais, permitindo a comunicação e a troca de informações seguras entre si e com o CeTIC-DF e acesso aos sistemas corporativos e à rede mundial de computadores;

XXV. Risco: é a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará;

XXVI. Segurança da Informação: é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio;

XXVII. Termo de Colaboração: instrumento por meio do qual são formalizadas as parcerias estabelecidas pela administração pública com organizações da sociedade civil para a consecução de finalidades de interesse público e recíproco propostas pela administração pública que envolvam a transferência de recursos financeiros;

XXVIII. Termo de Fomento: instrumento por meio do qual são formalizadas as parcerias estabelecidas pela administração pública com organizações da sociedade civil para a consecução de finalidades de interesse público e recíproco propostas pelas organizações da sociedade civil, que envolvam a transferência de recursos financeiros;

XXIX. Termo de Responsabilidade: termo assinado pelo usuário no qual ele manifesta concordância em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XXX. Tratamento da informação: conjunto de ações que englobam a recepção, a produção, a reprodução, a utilização, o acesso, o transporte, a transmissão, a distribuição, o

armazenamento, a eliminação e o controle da informação;

XXXI. Usuário: qualquer pessoa, física ou jurídica, ou processo em um sistema computacional que faça uso dos recursos de tecnologia da informação relativos à SEDES;

XXXII. Vulnerabilidade: fragilidade associada aos ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO IV

REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º As ações de Segurança da Informação e Comunicações da Secretaria de Desenvolvimento Social deverão observar os seguintes requisitos legais e normativos:

I. Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

II. Lei Federal nº 12.965, de 23 de abril de 2014 – Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil;

III. Lei Federal nº 12.737, de 30 de novembro de 2012 - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências;

IV. Lei Federal nº 12.735, de 30 de novembro de 2012 - Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências;

V. Lei Federal nº 12.527, de 18 de novembro de 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;

VI. Decreto Federal nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

VII. Lei Distrital nº 4.990, de 12 de dezembro de 2012 - Regula o acesso a informações no Distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal nº 12.527, de 18 de novembro de 2011, e dá outras providências;

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

IX. Decreto Distrital nº 42.036, de 27 de abril de 2021 - Dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018- Lei Geral de Proteção de Dados Pessoais - LGPD, no âmbito da Administração Pública Direta e Indireta do Distrito Federal e dá outras providências;

X. Decreto Distrital nº 42.070, de 05 de maio de 2021 - Dispõe sobre o uso do meio eletrônico para a realização de atos processuais administrativos, no âmbito dos órgãos e entidades do Distrito Federal, dos serviços sociais autônomos e das organizações sociais, com contrato de gestão firmado com o Distrito Federal;

XI. Decreto Distrital nº 40.015, de 14 de agosto de 2019 - Dispõe sobre a obrigatoriedade de

elaboração e publicação dos Planos Diretores de Tecnologia da Informação e Comunicação e sobre a centralização e utilização da rede GDFNet, da infraestrutura do Centro de Tecnologia da Informação e Comunicação do Distrito Federal - CeTIC-DF e dos sistemas de informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências;

XII. Decreto Distrital nº 38.354, de 24 de julho de 2017 - Institui a Política de Dados Abertos da Administração Pública direta, autárquica e fundacional Distrito Federal;

XIII. Decreto Distrital nº 37.085, de 27 de janeiro de 2016 - Dispõe sobre produtos institucionais de comunicação digital do Governo do Distrito Federal e dá outras providências;

XIV. Decreto Distrital nº 37.667, de 29 de setembro de 2016 - Dispõe sobre a contratação de bens e serviços de Tecnologia da Informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências;

XV. Decreto Distrital nº 35.382, de 29 de abril de 2014 - Regulamenta o art. 42, da Lei nº 4.990, de 12 de dezembro de 2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento, institui o Comitê Gestor de Credenciamento de Segurança, e dá outras providências;

XVI. Decreto Distrital nº 34.276, de 11 de abril de 2013 - Regulamenta a Lei nº 4.990, de 12 de dezembro de 2012, que dispõe sobre 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, todos da Constituição Federal de 1988;

XVII. Decreto Distrital nº 25.750, de 12 de abril de 2005 - Regulamenta a Lei 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;

XVIII. Resolução nº 03, de 06 de novembro de 2018 - Aprova a revisão da Política de Segurança da Informação e Comunicação (PoSIC) do Governo do Distrito Federal;

XIX. Norma ISO 22301:2019 - Segurança e resiliência - Sistemas de gestão de continuidade de negócios - Requisitos;

XX. Norma ISO 31000:2018 – Informações básicas, princípios e diretrizes para a implementação da gestão de riscos;

XXI. Norma ISO/IEC 27001:2013 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação documentado dentro do contexto dos riscos de negócio globais da organização;

XXII. Norma ISO/IEC 27002:2013 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação - estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

CAPÍTULO V

PRINCÍPIOS

Art. 7º As ações relacionadas com a Segurança da Informação e Comunicações na SEDES são norteadas pelos seguintes princípios:

I. Auditabilidade: garantia de que uma informação é passível de auditoria, isto é, de que é possível rastrear e levantar os diversos passos do processo dessa informação, além de

identificar itens como participantes, ações, data e horário de cada etapa;

II. Equidade: as normas e regras de segurança da informação devem ser obedecidas por todos, sem distinção de cargo ou função;

III. Ética: os direitos dos agentes públicos são preservados sem comprometimento da segurança da informação e comunicações;

IV. Privilégio mínimo: os usuários só devem receber os privilégios necessários para concluir a tarefa que lhes foi designada, de modo a reduzir as chances de eles consultarem ou alterarem, de forma acidental ou mal-intencionada, dados aos quais não devem ter privilégio de acesso;

V. Privacidade desde a concepção: qualquer projeto que envolva o processamento de dados pessoais deve manter a proteção e a privacidade dos dados desde o seu planejamento;

VI. Publicidade: dar transparência no tratamento das informações, observados os critérios legais. Divulgar a todos os agentes públicos da SEDES as diretrizes e a normas de segurança da informação;

VII. Resiliência: os controles de segurança deverão ser projetados para que possam resistir e se recuperar dos efeitos de um desastre;

VIII. Simplicidade: as informações e seus controles devem ser cada vez mais simples, objetivos e de fácil absorção.

CAPÍTULO VI

DIRETRIZES

Art. 8º É condição para acesso aos ativos de informação da SEDES a adesão formal aos termos desta Portaria, mediante assinatura de Termo de Responsabilidade.

Art. 9º Todos os agentes públicos da SEDES são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede, crachá, carimbo, endereço de correio eletrônico ou assinatura digital.

Art. 10. Os recursos de TIC disponibilizados pela SEDES devem ser utilizados estritamente dentro do seu propósito.

Art. 11. Os contratos de prestação de serviços, termos de colaboração, termos de fomento e acordos de cooperação firmados pela SEDES conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo, ainda, exigir da(s) entidade(s) contratada(s)/parceira(s) a assinatura de Termo de Manutenção do Sigilo.

Art. 12. Esta Política aplica-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação e rege-se pelas seguintes diretrizes:

I - Propriedade da Informação:

a. toda informação criada, armazenada, transportada ou descartada pelos agentes públicos da SEDES, no exercício de suas atividades, é de propriedade do órgão e é protegida segundo as diretrizes descritas na POSIC/SEDES e nas regulamentações em vigor;

b. o Gestor da Informação deverá providenciar a documentação formal relativa à cessão ou autorização de acesso antes da cessão de bases de dados nominais e de informação custodiada ou de propriedade da SEDES a terceiros;

c. nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será

utilizada deverá, se necessário, providenciar com a concedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

II - Tratamento da Informação:

a. toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pela SEDES é de sua responsabilidade e é classificada e protegida adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita, conforme o Decreto nº 34.276, de 11 de abril de 2013;

b. a classificação da informação é atribuição do Gestor da Informação;

c. toda informação institucional, se eletrônica, estará armazenada nos servidores de arquivo e bases de dados sob gestão do CeTIC e administração da área de TIC da SEDES. Se não eletrônica, a informação será mantida em local que a salvaguarde adequadamente;

d. toda informação institucional, sob a forma eletrônica, estará salvaguardada por meio de cópia de segurança sob administração do CeTIC e mantida em local que a proteja adequadamente e garanta sua recuperação em caso de perda da informação original;

e. no descarte de informações institucionais, são observados os procedimentos internos, as políticas, a classificação e as normas atinentes à informação, bem como a temporalidade prevista na legislação.

III - Tratamento de Incidentes em Rede:

a. cabe ao CeTIC a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação no âmbito da rede corporativa GDFNet;

b. todo agente público da SEDES é responsável por notificar imediatamente à área de TIC da SEDES i) incidentes que afetem a segurança da informação por meio de recursos de TIC ou ii) o descumprimento da POSIC/SEDES, para que as causas possam ser sanadas.

IV - Gestão de Risco

a. fica estabelecido o Processo de Gestão de Riscos de Segurança da Informação e Comunicações (PROSIC), com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações;

b. o PROSIC baseia-se nas melhores práticas presentes na Norma ISO 31000:2009.

V - Gestão de Continuidade:

a. fica estabelecido o Programa de Gestão de Continuidade de Negócio (PGCON) em segurança da informação e comunicações no âmbito da SEDES, a fim de reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações da Secretaria;

b. todo sistema ou serviço crítico da SEDES deverá estar suportado pelo PGCON;

c. o PGCON baseia-se nas melhores práticas presentes na Norma ISO 22301:2019.

VI - Auditoria e Conformidade:

a. o uso dos recursos de TIC disponibilizados pela SEDES é passível de monitoramento e auditoria, e serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso;

b. serão mantidos procedimentos como trilhas de auditoria, rastreamento, acompanhamento,

controle e verificação de acessos para todos os sistemas corporativos e para a rede interna da SEDES.

VII - Controles de Acesso:

a. o agente público da SEDES que utilizar os recursos de TIC terá uma conta, única e intransferível, cuja concessão de acesso será regulamentada em norma específica, expedida pela Subsecretaria de Gestão da Informação, Formação, Parcerias e Redes;

b. o gestor da informação é responsável pela concessão e revogação dos privilégios de acesso às informações, considerando sempre o princípio do menor privilégio;

c. a identificação do agente público, qualquer que seja o meio e a forma, é pessoal e intransferível e permite o reconhecimento de maneira inequívoca.

VIII - Uso de E-mail

a. o correio eletrônico da SEDES tem seu uso exclusivo por servidores públicos no exercício de suas funções. As regras de acesso e utilização são definidas por norma específica, em conformidade com esta POSIC/SEDES e demais orientações e diretrizes de governo.

IX - Acesso à Internet:

a. o acesso à Internet no ambiente de trabalho da SEDES está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por norma específica, em conformidade com esta POSIC/SEDES, demais orientações governamentais e legislação em vigor.

X - Gestão de Ativos de Informação:

a. a Subsecretaria de Gestão da Informação, Formação, Parcerias e Redes e as unidades responsáveis pela gestão patrimonial manterão um processo de Inventário e Mapeamento dos Ativos de Informação objetivando a segurança das infraestruturas críticas que garantam suas informações;

b. o processo de Inventário e Mapeamento de Ativos de Informação subsidiará o conhecimento, valoração, proteção e manutenção de seus ativos de informação, assim como será dinâmico, periódico, e estruturado, para manter a Base de Dados de Ativos de Informação atualizada.

XI - Dispositivos Móveis:

a. o uso dos dispositivos móveis portáteis pelos agentes públicos usuários da rede da SEDES deverá ser realizado no interesse do órgão;

b. todo dispositivo móvel usado para acessar a rede corporativa da SEDES estará submetido aos padrões estabelecidos pelo CeTIC;

c. O CeTIC proverá uma rede segregada da rede corporativa para acesso à Internet pelos visitantes.

XII - Computação em Nuvem:

a. o ambiente de computação em nuvem, sua infraestrutura e seu canal de comunicação devem adequar-se às diretrizes e normas de SIC, estabelecidas pelas legislações vigentes

b. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a

disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

XIII - Redes Sociais:

a. o uso institucional das redes sociais nos aspectos relacionados à Segurança da Informação e Comunicações deverá ser objeto de norma interna expedida pela Subsecretaria de Gestão da Informação, Formação, Parcerias e Redes (SUGIP);

b. a normatização interna de uso seguro das redes sociais deverá estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social a partir da infraestrutura das redes de computadores da SEDES.

XIV - Desenvolvimento de Software Seguro - DSS:

a. deverão ser identificados os responsáveis pela definição e validação dos requisitos de segurança que o *software* deve atender;

b. logo no início de qualquer projeto de desenvolvimento de *software*, deverão ser definidos os requisitos de segurança que observem, no mínimo, os 10 principais riscos de segurança para aplicações web, segundo o "*Open Web Application Security Project*" (OWASP);

c. deverá ser definida a execução de testes e homologação antes da instalação do *software* em ambiente de produção;

d. os sistemas mantidos pela SEDES disponibilizados na Internet deverão possuir certificado digital válido;

e. o tratamento das vulnerabilidades constitui um dos requisitos para a aceitação do sistema.

XV - Preservação de Evidências:

a. os equipamentos servidores de rede, bem como todo e qualquer outro ativo de informação semelhante, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados e das operações de seus administradores;

b. os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos;

c. os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio de tecnologia aplicável.

CAPÍTULO VII

COMPETÊNCIAS E RESPONSABILIDADES

Art. 13. Compete à alta administração da SEDES:

I. apoiar e exigir o cumprimento da Política, normas e procedimentos de segurança da informação e comunicação;

II. zelar para que contratos, convênios e outros instrumentos similares elaborados pela SEDES estejam alinhados à presente Política e suas normas adjacentes;

III. fomentar a capacitação contínua dos servidores, de modo a promover a aptidão para gestão e execução das atividades de segurança da informação e comunicação.

Art. 14. Compete ao(a) Subsecretário(a) da Subsecretaria de Gestão da Informação, Formação, Parcerias e Redes:

I. designar a Comissão de Segurança da Informação e Comunicação - CSIC da SEDES;

II. designar o(a) Gestor(a) da Segurança da Informação e Comunicação.

Art. 15. A Comissão de Segurança da Informação e Comunicação (CSIC) é responsável por:

I. elaborar e atualizar a POSIC/SEDES, em conformidade com as normas, objetivos estratégicos e com as leis e regulamentos pertinentes;

II. elaborar e aprovar Normas e Procedimentos de Segurança da Informação e Comunicação;

III. coordenar a execução da POSIC, mediante a mobilização dos gestores para o cumprimento da Política;

IV. promover a cultura de segurança da informação e comunicação;

V. estabelecer o Processo de Gestão de Riscos de Segurança da Informação e Comunicações (PROSIC), atualizando-o quando necessário;

VI. desenvolver o Programa de Gestão de Continuidade de Negócio (PGCON), que deverá ser testado periodicamente;

VII. estabelecer tanto mecanismo de registro e controle de não conformidade desta Política quanto Normas e Procedimentos de Segurança da Informação e Comunicação.

Art. 16. Ao Gestor da Segurança da Informação e Comunicação compete:

I. coordenar a Comissão de Segurança da Informação e Comunicações (CSIC);

II. monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. propor recursos necessários às ações de segurança da informação e comunicações;

IV. realizar e acompanhar estudos de novas tecnologias concernentes a possíveis impactos na SIC.

Art. 17. São obrigações do usuário:

I. observar rigorosamente esta POSIC/SEDES, bem como as normas e procedimentos a ela aplicados;

II. assegurar o uso racional dos recursos de tecnologia da informação colocados à sua disposição, de modo a priorizar o interesse público e institucional;

III. comunicar à CSIC quaisquer riscos ou incidentes de segurança sobre os quais tome conhecimento;

IV. assegurar que suas senhas e credenciais para acesso aos ativos de processamento e de informações estejam de acordo com os procedimentos estabelecidos, que elas sejam protegidas e confidenciais e que não sejam compartilhadas;

V. manter, obrigatoriamente, os dados críticos da Secretaria nos compartilhamentos de rede, disponibilizados pela área de TIC.

Art. 18. São obrigações da unidade administrativa da SEDES responsável pela área de TIC:

I. assegurar o pleno e efetivo funcionamento dos recursos de tecnologia da informação disponibilizados pela SEDES;

II. assegurar a integridade e disponibilidade dos ativos que se encontram no ambiente computacional da SEDES;

III. dar assistência ao CSIC na elaboração de normas e procedimentos de Segurança da Informação;

IV. realizar trabalhos de análise de vulnerabilidade, a fim de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente da SEDES;

V. requisitar informações às demais áreas da SEDES e realizar testes e averiguações em sistemas e equipamentos, no intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação e Comunicação.

CAPÍTULO VIII

DIVULGAÇÃO E CAPACITAÇÃO

Art. 19. A POSIC/SEDES, bem como suas normas e regulamentos, deverá ser disponibilizada e agrupada, com a data de sua publicação e/ou revisão, em sítio institucional, em local de fácil acesso, com vistas a proporcionar ampla difusão e atualização simplificada.

Art. 20. A SEDES deverá promover ações permanentes de capacitação dos servidores públicos visando à disseminação das diretrizes e normas estabelecidas nesta Política.

Parágrafo único. Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação devem receber capacitação especializada.

CAPÍTULO IX

ATUALIZAÇÃO

Art. 21. A POSIC/SEDES e as normas e procedimentos que dela se originem devem ser atualizadas sempre que se fizer necessário, o que não deve exceder o período máximo de 2 (dois) anos.

CAPÍTULO X

PENALIDADES

Art. 22. O descumprimento das diretrizes desta POSIC/SEDES, assim como das suas normas e procedimentos vinculados, acarretará sanções administrativas, sem prejuízo das demais medidas administrativas, cíveis e criminais cabíveis.

CAPÍTULO XI

VIGÊNCIA

Art. 23. Esta Portaria entra em vigor na data de sua publicação.

Art. 24. Revogam-se as disposições em contrário.

MAYARA NORONHA ROCHA
Secretária de Estado de Desenvolvimento Social do Distrito Federal

Documento assinado eletronicamente por **MAYARA NORONHA DE ALBUQUERQUE ROCHA - Matr.0276895-X**, **Secretário(a) de Estado de Desenvolvimento Social do Distrito Federal**, em 09/11/2021, às 18:06, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **73270957** código CRC= **20E71858**.