POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

E COMUNICAÇÃO DA SECRETARIA DE ESTADO

DESENVOLVIMENTO HUMANO E SOCIAL DO DISTRITO FEDERAL

(PoSIC/SEDHS)

Brasília – setembro de 2015

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

SUMÁRIO

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

1. OBJETIVO

1.1 A Política de Segurança da Informação e Comunicação da Secretaria de Estado de Desenvolvimento Humano e Social do Distrito Federal - PoSIC/SEDHS tem por finalidade estabelecer as diretrizes e princípios para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, no âmbito da Secretaria, limitando a níveis aceitáveis a exposição ao risco e garantindo a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam seus objetivos estratégicos da SEDHS.

1.2 A Gestão de segurança da informação e comunicação deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicação.

2. ABRANGÊNCIA

2.1 A Política de Segurança da Informação e Comunicação – PoSIC/SEDHS aplica-se a todas as unidades da estrutura administrativa da Secretaria, devendo suas diretrizes, normas complementares e manuais de procedimentos ser observados por todos os servidores públicos, colaboradores, estagiários, consultores externos e prestadores de serviço, sob pena de responsabilidade, na forma da lei.

2.2 Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações.

2.3 Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela SEDHS devem atender ao disposto na PoSIC/SEDHS.

2.4 Esta política também se aplica no que couber, ao relacionamento da SEDHS com terceiros.

3. CONCEITOS E DEFINIÇÕES

Para efeito da Política de Segurança da Informação e Comunicação – PoSIC/SEDHS, adotam-se os seguintes conceitos e definições:

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

I. **Aceitação de Risco**: decisão de aceitar um risco (item 3.34) e seus resultados. A aceitação pode ser necessária em razão do custo-benefício para se proteger um ativo ou devido ao risco residual remanescente após o tratamento de riscos;

II. **Alta Administração**: para efeitos desta política, considera-se alta administração os ocupantes dos cargos de Secretário de Estado, Secretário Adjunto e Subsecretários de Estado da SEDHS;

III. **Ameaça**: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas. Exploram as vulnerabilidades, ocasionando perda de confidencialidade, integridade ou disponibilidade;

IV. **Análise / Avaliação 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;

V. **Ativo**: é tudo aquilo que tenha valor para a organização e consequentemente exige proteção;

VI. **Autenticidade**: propriedade de que a informação seja 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.

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

VIII. **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;

IX. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

X. **Contramedida**: vide Controle de Segurança.

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

XII. **Controle de Segurança**: são práticas de gestão de risco (políticas, normas, procedimentos ou mecanismos) que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades, limitar o impacto de um incidente ou ajudar na sua detecção;

XIII. **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;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

XIV. **Custódia**: responsabilidade pela guarda de um ativo para terceiros. A custódia não permite automaticamente o direito de acesso ao ativo, nem a capacidade de conceder direito de acesso a outros;

XV. **Custodiante**: indivíduo a quem é dada a custódia de um ativo;

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

XVII. **Diretriz:** o que deve ser feito e como, para atender aos objetivos declarados na política;

XVIII. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido;

XIX. **Grupo de Resposta a Incidentes de Segurança em Computadores (CSIRT – *Computer Security Incident Response Team*)**: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança em computadores;

XX. **Evento de Segurança da Informação**: ocorrência de uma violação à Política de Segurança da Informação e Comunicação ou falha nos Controles de Segurança;

XXI. **Gestão de Riscos: a**tividade contínua de identificação, análise, tratamento, aceitação e comunicação de riscos;

XXII. **Gestor de Segurança da Informação**: é o responsável pelas ações de segurança da informação e comunicações no âmbito da SEDHS;

XXIII. **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;

XXIV. **Impacto**: alteração no meio ou em algum de seus componentes por determinada ação ou atividade.

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

XXVI. **Integridade**: propriedade de que a informação e os métodos de processamento não sejam modificados, suprimidos ou destruídos de maneira não autorizada ou acidental, salvaguardando-se sua exatidão e completeza;

XXVII. **Monitoramento**: atividade de verificação manual ou automática de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes da Política, normas ou procedimentos de segurança da informação e comunicação;

XXVIII. **Privacidade:** é a limitação do acesso às informações;

XXIX. **Processo**: instruções executadas por um programa de computador;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

XXX. **Programa de Computador**: sequência finita de instruções bem definidas e não ambíguas, disponibilizadas, normalmente, por meio de um arquivo executável, para realizar uma tarefa determinada num ambiente computacional;

XXXI. **Proprietário**: indivíduo que, em virtude de suas funções ou atribuições legais é responsável e tem poder de decisão para identificar e classificar as informações geradas por sua área de abrangência;

XXXII. **Proteção**: vide Controle de Segurança (item 3.12);

XXXIII. **Recursos de Tecnologia da Informação**: conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio de *hardware e software,* a criação, acesso, armazenamento, transmissão e processamento de dados e informações;

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

XXXV. **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;

XXXVI. **Servidor Público**: é a pessoa legalmente investida em cargo público (LC nº840/2011);

XXXVII. **Tratamento da informação:** conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

XXXVIII. **Tratamento do risco**: processo de seleção e implementação de controles de segurança;

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

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

4. REFERÊNCIAS LEGAIS E NORMATIVAS

Dispositivos legais e normativos que subsidiaram a elaboração e aplicáveis à Política de Segurança da Informação e Comunicação – PoSIC/SEDHS:

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

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

II. **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;

III. **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;

IV. **Decreto Federal nº 7724 de 16 de maio de 2012 -** regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º no inciso II do § 3º do art. 37 e no § 2ºdo art. 216 da Constituição;

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 4.553, de 27 de dezembro de 2002** - dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

VII. **Instrução Normativa nº 04 de 12 de novembro de 2010 – IN 04/SLTI/MPOG** - dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal;

VIII. **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;

IX. **Decreto Distrital nº 34.637, de 06 de setembro de 2013** - 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;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

X. **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;

XI. **Decreto Distrital nº 33.528, de 10 de fevereiro de 2012** – dispõe sobre a aprovação de Estratégia Geral de Tecnologia da Informação – EGTI, elaborada pelo Comitê Gestor de Tecnologia da Informação e Comunicação e dá outras providências;

XII. **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";

XIII. **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;

XIV. **ABNT NBR 15999-1:2007 - Gestão de continuidade de negócios** - estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN);

XV. **ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.** Especifica os requisitos e 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;

XVI. **ABNT NBR ISO/IEC 27002:2005 - 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;

XVII. **ABNT ISO GUIA 73:2009 - Gestão de riscos – Vocabulário** - fornece as definições de termos genéricos relativos à gestão de riscos;

XVIII. **Norma Complementar nº 03/IN01/DSIC/GSIPR** – estabelece diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

5. PRINCÍPIOS

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

A PoSIC/SEDHS obedece aos princípios constitucionais, administrativos e do arcabouço legislativo vigente, que regem a Administração Pública, destacando-se:

I. **Simplicidade:** ausência de artifícios, extravagâncias e excessos. As informações e seus controles devem ser cada vez mais simples, objetivos e de fácil absorção. Esses atributos são necessários para garantir que a informação chegue a todos de uma forma passível de compreensão imediata, além de reduzir a ocorrência de erros.

II. **Privilégio Mínimo:** é fundamental para a segurança da informação e defende que devemos realizar as tarefas necessárias com os mínimos privilégios. Significa que os usuários só devem receber os privilégios necessários para concluir a tarefa que lhe foi designada, reduzindo assim, as chances de que eles consultem ou alterem de forma acidental ou mal-intencionada, dados aos quais não devem ter privilégio de consulta ou alteração.

III. **Segregação de função:** é um princípio derivado do Princípio da Moralidade Administrativa, ínsito no art. 37, caput, da Constituição Federal. De acordo com o princípio da segregação de funções, nenhum servidor ou unidade administrativa deve participar ou controlar todas as fases inerentes a uma despesa (Empenho - Liquidação - Pagamento), ou seja, cada fase deve, preferencialmente, ser executada por pessoas e setores independentes entre si, possibilitando a realização de uma verificação cruzada. É oportuno destacar o entendimento consubstanciado pelo Tribunal de Contas da União-TCU sobre a matéria, no sentido de que a segregação de funções é princípio básico do sistema de controle interno, que consiste na separação de funções, nomeadamente de autorização, aprovação, execução, controle e contabilização das operações. (TCU, Portaria n.º 63/96, Glossário). Assim, em relação à informação e seus processos, as funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos, bem como permitir maior eficácia dos controles de segurança;

IV. **Auditabilidade:** característica da Segurança da Informação que garante que tal informação é passível de auditoria, possibilitando que sejam rastreados e levantados os diversos passos de um processo que a informação sofreu, identificando itens como participantes, ações, data e horário de cada etapa. Assim, todos os eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;

V. **Mínima dependência de segredos:** os controles devem ser efetivos, ainda que se conheça a existências deles e como eles funcionam;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

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

VII. **Defesa em profundidade**: os controles de segurança devem ser concebidos em múltiplas camadas, de tal forma que, quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança;

6. ESTRUTURA NORMATIVA

A presente política é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

6.1 Política de Segurança da Informação e Comunicação (PoSIC): define a estrutura, diretrizes gerais e as obrigações referentes à segurança da informação e comunicação, servindo de base para elaboração dos demais documentos da estrutura normativa e possui caráter estratégico;

6.2 Normas de Segurança da Informação e Comunicação (NOSIC): de caráter tático, as normas estabelecem regras para a utilização de ativos e recursos de tecnologia da informação com o intuito de atingir os objetivos da Política;

6.3 Procedimentos de Segurança da Informação e Comunicação (PROSIC): descreve, detalhadamente, as medidas de caráter operacional necessárias para atingir os resultados estabelecidos nas normas e na Política, abordando aspectos técnicos e práticos, adaptados à realidade do ambiente.

6.4 O cumprimento da PoSIC/SEDHS e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas pelo Comitê de Segurança da Informação e Comunicação (CSIC) da SEDHS, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

7. CICLO DE VIDA DA INFORMAÇÃO

As medidas de proteção devem ser adotadas durante todo o ciclo de vida da informação, compreendendo as fases de criação, manipulação, armazenamento, transporte e descarte.

8. NORMAS E PROCEDIMENTOS COMPLEMENTARES

As normas e procedimentos que complementam a PoSIC/SEDHS devem abordar, mas não limitados a estes, os seguintes aspectos: segurança física; gestão de mudanças; privacidade; criptografia; acesso à rede;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

gestão de senhas e contas de usuário; dispositivos móveis; gestão de incidentes; plano de continuidade de negócios; proteção à propriedade intelectual; treinamento e sensibilização para segurança;

9. DIVULGAÇÃO

9.1 A PoSIC/SEDHS, bem como suas normas e regulamentos, deverão ser disponibilizadas e agrupadas em sítio institucional, em local de fácil acesso, proporcionando ampla difusão e atualização simplificada, explicitando-se em todos os documentos, a data de sua publicação e/ou revisão.

9.2 Os procedimentos de segurança da informação, por conter informações sensíveis, devem ser classificados na forma da lei e divulgados àqueles cujas atribuições requerem conhecimento das mesmas.

10. SEGURANÇA FÍSICA E DO AMBIENTE

10.1 As instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física.

10.2 Os equipamentos deverão ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora da instalação.

11. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO E COMUNICAÇÃO

11.1 Deverão ser desenvolvidas ações que garantam que a segurança seja parte integrante dos sistemas de informação e comunicação existentes, bem como dos que vierem a ser desenvolvidos.

11.2 Entende-se por sistemas de informação os sistemas operacionais, infraestrutura, aplicações de negócio, produtos de prateleira, serviços e aplicações desenvolvidas.

11.3 Todos os requisitos de segurança deverão ser identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados como parte do caso geral de negócios para um sistema de informações.

12. EDUCAÇÃO CONTINUADA

Para uma efetiva proteção das informações, deverão ser instituídos planos e/ou programas permanentes e regulares de conscientização, sensibilização e capacitação em Segurança da Informação e

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

Comunicação - SIC, buscando, inclusive, parcerias com outros órgãos e entidades, de modo a promover maior responsabilidade individual dos usuários e maior independência do Estado na contratação de serviços de segurança.

13. PENALIDADES

O descumprimento às diretrizes desta PoSIC/SEDHS, assim como às suas normas e procedimentos vinculados, acarretará em sanções administrativas em primeira instância, sem prejuízo às ações cíveis e criminais cabíveis.

14. COMPETÊNCIAS E RESPONSABILIDADES DA GESTÃO EM SEGURANÇA DA INFORMAÇÃO

A gestão corporativa de segurança da informação deverá ser realizada por servidores públicos efetivos.

14.1 COMPETÊNCIAS DA ALTA ADMINISTRAÇÃO DA SEDHS

14.1.1 Compete à alta administração da SEDHS:

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 SEDHS estejam alinhados a presente política e suas normas adjacentes.

III. Priorizar a capacitação contínua dos servidores, de modo a promover maior independência do Estado na gestão e execução das atividades de segurança da informação e comunicação.

14.2 COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

14.2.1 O Comitê de Segurança da Informação e Comunicação (CSIC) da SEDHS é responsável por:

I. Elaborar e atualizar a Política de Segurança da Informação e Comunicação (PoSIC) da Secretaria de Desenvolvimento Humano e Social do Distrito Federal (SEDHS), 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, mobilizando gestores para o cumprimento da Política;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

IV. Promover cultura de segurança da informação e comunicação;

V. Estabelecer um Programa de Gestão de Riscos, atualizando-o quando necessário;

VI. Desenvolver um Plano de Continuidade de Negócios, que deverá ser testado periodicamente;

VII. Instituir grupos de trabalho específicos relacionados à segurança da informação;

VIII. Acionar os respectivos proprietários para que procedam à classificação tempestiva das informações de área de abrangência;

IX. Desempenhar outras atividades decisórias afetas à Gestão de Segurança da Informação e Comunicações no âmbito da SEDHS a ele delegadas;

X. Estabelecer mecanismo de registro e controle de não conformidade desta Política, Normas e Procedimentos de Segurança da Informação e Comunicação.

14.2.2 O CSIC será designado pelo titular da Secretaria e terá a seguinte formação:

I. Gestor de Segurança da Informação, que coordenará as atividades do Comitê;

II. Um membro da área de Segurança Física;

III. Um membro da área de Segurança Digital;

IV. Um membro da área de Processos Administrativos;

V. Um membro da área de Normas e Legislação.

15. GESTOR DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Compete ao Gestor da Segurança da Informação e Comunicação:

I. Coordenar o Comitê 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, quanto a possíveis impactos na segurança da informação e comunicações;

V. Propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito da SEDHS;

VI. Definir, juntamente com o CSIC, métricas que permitam aferir a eficiência e eficácia dos controles de segurança.

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

16. USUÁRIO

São obrigações do usuário:

I. Observar rigorosamente esta Política de Segurança de Informação e Comunicação, bem como as normas e procedimentos a ela aplicados;

II. Assegurar o uso racional dos recursos de tecnologia da informação colocados à sua disposição, priorizando o interesse público e institucional;

III. Comunicar ao Grupo de Resposta a Incidentes de Segurança em Computadores (GSIRT) quaisquer riscos ou incidentes de segurança sobre os quais tomem conhecimento;

IV. Assegurar-se de que as senhas e credenciais para acesso aos ativos de processamento e de informações estejam de acordo com os procedimentos estabelecidos e que as mesmas sejam protegidas e confidenciais, não devendo ser compartilhada;

V. Manter, obrigatoriamente, os dados críticos da Secretaria nos compartilhamentos de rede, disponibilizados pela DITEC e a SEGAD para todas as unidades administrativas do Governo do Distrito Federal.

17. UNIDADE ADMINISTRATIVA DA SEDHS RESPONSÁVEL PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

São obrigações da unidade administrativa da SEDHS responsável pela área de tecnologia da informação, atualmente a Diretoria de Tecnologia da Informação da Subsecretaria de Administração Geral – DITEC/SUAG:

I. Realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;

II. Assegurar o pleno e efetivo funcionamento dos recursos de tecnologia da informação disponibilizados pela SEDHS;

III. Assegurar a integridade e disponibilidade dos ativos que se encontram no ambiente computacional da SEDHS;

IV. Dar assistência ao CSIC na elaboração de normas e procedimentos de Segurança da Informação, no tocante às informações, comunicações e processos relativos presentes no ambiente computacional da SEDHS;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

V. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente SEDHS;

VI. Requisitar informações às demais áreas da SEDHS e realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das normas de Segurança da Informação e Comunicação no tocante aos ativos informatizados;

VII. Elaborar Plano de Resposta a Incidentes de Segurança da Informação e Comunicação, que inclua: ação imediata para interromper ou minimizar o incidente, investigação do incidente e restauração dos recursos afetados, e comunicação do incidente aos canais apropriados;

VIII. Utilizar servidores públicos do órgão, na gestão de processos de Tecnologia da Informação.

18. PROPRIETÁRIO

São obrigações do proprietário:

I. Identificar e definir as informações críticas e os requisitos de confidencialidade, integridade, disponibilidade e autenticidade dos seus ativos;

II. Classificar e rever periodicamente a classificação dos ativos sob sua propriedade, que requerem algum grau de sigilo, observando a legislação em vigor;

III. Participar do processo de avaliação e aceitação de risco;

IV. Participar das decisões relacionadas a qualquer violação de segurança dos ativos sob sua propriedade;

V. Autorizar a liberação de acesso à informação sob sua responsabilidade;

VI. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

VII. Participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

19. CUSTODIANTE

São obrigações do Custodiante:

I. Prestar assistência ao Proprietário na definição dos procedimentos operacionais e de controle, referentes a manuseio, armazenamento e disposição final dos ativos;

II. Controlar e proteger os ativos sob sua custódia;

III. Realizar, verificar e manter cópias de segurança (*backups*) dos ativos de informação sob sua custódia;

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511

IV. Comunicar ao GSIRT e ao proprietário qualquer incidente de segurança que afete os ativos sob sua custódia;

V. Implementar os controles de segurança contratando, se necessário, bens e serviços em Segurança da Informação e Comunicação.

20. GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA EM COMPUTADORES (GSIRT)

O GSIRT será responsável por:

I. Suspender, a qualquer tempo, o acesso de usuário ou processo a informações ou recursos de tecnologia da informação e comunicação, quando evidenciados riscos à segurança da informação, notificando, de imediato, o Gestor de Segurança da Informação;

II. Dar tratamento e encaminhamento aos incidentes de redes, tomando as medidas necessárias para conter as ameaças, minimizar os impactos e evitar futuras ocorrências, restabelecendo juntamente com o setor responsável, a integridade, confidencialidade e disponibilidade dos ativos;

III. Registrar, classificar e filtrar as notificações de Incidentes de Segurança;

IV. Executar o Plano de Resposta a Incidentes;

V. Recolher e preservar as evidências para subsidiar a forense computacional;

VI. Investigar as causas dos incidentes no ambiente computacional.

21. ATUALIZAÇÃO

A PoSIC/SEDHS, bem como as normas e procedimentos que dela se originem ou a ela se apliquem, devem ser atualizadas com periodicidade mínima anual ou quando ocorrerem mudanças significativas, que afetem a base de avaliação de risco original.

Secretaria de Estado de Desenvolvimento Humano e Social – SEDHS
SEPN 515, bloco A, 2º andar – CEP: 70.770-501
Fones: (61) 3348.3511