SERVIÇO DE LIMPEZA URBANA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC

1.OBJETIVO

1.1 A Política de Segurança da Informação e Comunicações – POSIC tem por objetivo prover a salvaguarda dos ativos formados por dados, informações e materiais sigilosos de propriedade ou de interesse do SLU-DF e do Governo do Distrito Federal, bem como dos sistemas computacionais e das áreas e instalações onde são produzidos, armazenados ou trafegam, além da preservação da inviolabilidade e da intimidade da vida privada, da honra e imagem das pessoas e da instituição.

1.2 As ações de segurança da informação e das comunicações a serem elaboradas no âmbito do SLU-DF, deverão observar sempre a garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, lembrando sempre que as informações classificadas em qualquer grau de sigilo devem estar disponíveis estritamente a quem estiver autorizado.

2. MARCO LEGAL

2.1 Lei Nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

2.2 Lei Nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador;

2.3 Lei Nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

2.4 Lei Nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

2.5 Decreto Nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

2.6 Decreto Nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de

dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

2.7 Instrução Normativa GSI-PR n. 01 de 13 de junho de 2008 que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal; e

2.8 NBR/ISO/IEC Nº 27.002, que institui o código de melhores práticas para gestão de segurança da informação.

3. ABRANGÊNCIA

3.1 A Política de Segurança da Informação e Comunicações aplica-se a todas as unidades administrativas, empregados, funcionários e colaboradores externos que prestam serviço em razão de contratos administrativos firmados na forma da Lei e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres.

4. VIGÊNCIA E REVISÕES

4.1 A Política de Segurança da Informação e Comunicações tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

4.2 A atualização da Política de Segurança da Informação e Comunicações será realizada pelo Comitê Gestor da Tecnologia da Informação e das Comunicações, na forma do Regimento Interno do Comitê (Resolução CGTIC n. 01/2015).

5. CONCEITOS E DEFINIÇÕES

5.1 Os conceitos e definições constantes deste item se aplicam de forma a auxiliar a interpretação da Política de Segurança da Informação e das Comunicações do SLU-DF e também no estabelecimento de futuras normas complementares.

5.1.1 Ativo: além da própria informação, todo o recurso utilizado para a sua produção, o seu tratamento, tráfego e armazenamento;

5.1.2 Autenticidade: propriedade de que a informação foi produzida, expedida,

modificada ou destruída por determinada pessoa física, ou por determinado sistema, órgão ou entidade;

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

5.1.4 Classificação: atribuição de grau de sigilo a dado, informação, documento, material, área física ou instalação, pela autoridade competente;

5.1.5 Códigos Maliciosos (agressivos) ou malware: qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico;

5.1.6 Análise de riscos: processo completo de análise e avaliação de riscos.[1]

5.1.7 Avaliação de riscos: processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco. [2]

5.1.8 Correio Eletrônico: meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;

5.1.9 Criptografia: ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

5.1.10 Criticidade: grau de importância da informação para a continuidade dos negócios do SLU-DF e suas entidades vinculadas, diretamente associada ao nível de disponibilidade e integridade da informação;

5.1.11 Chave de Acesso: código de acesso atribuído a cada Usuário. A cada Chave de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos disponíveis;

[1] ABNT ISO/IEC Guia 73:2005
[2] ABNT ISO/IEC Guia 73:2005

5.1.12 Disponibilidade: propriedade de que a informação esteja acessível e

utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

5.1.13 Diretrizes: são as instruções de alto nível que representam os princípios básicos que a Organização resolveu incorporar à sua gestão de acordo com a visão estratégica da alta Direção. Servem como base para que as normas e os procedimentos sejam criados e detalhados;

5.1.14 Download: ato de baixar um arquivo ou documento de outro computador, por meio da Internet.

5.1.15 FTP (File Transfer Protocol): protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

5.1.16 Gestor: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir ou alterar a sua classificação nos graus de sigilo, criticidade e perfil de acesso dos demais usuários e processos;

5.1.17 Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.[3]

5.1.18 Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento

5.1.19 Internet: associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação por meio de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc;

5.1.20 Informação confidencial: aquela cujo conhecimento e divulgação, por pessoa não autorizada, possa ser prejudicial ao interesse da instituição;

5.1.21 Informação reservada: dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos;

[3] ABNT ISO/IEC Guia 73:2005

5.1.22 Informação pública ou ostensiva: aquelas cujo acesso é irrestrito, disponível

para divulgação pública por meio de canais autorizados pela entidade gestora;

5.1.23 Instruções e Procedimentos – detalham no plano operacional configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas nas normas;

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

5.1.25 Intranet: rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os servidores e funcionários possam acessar as informações das suas instituições.

5.1.26 IMAP *(Internet Message Access Protocol):* protocolo de acesso a mensagens eletrônicas.

5.1.27 Login: identificador de usuário em um programa ou rede de computadores. Os logins são fornecidos em conjunto com a senha pessoal e intransferível para ingresso a redes, softwares e utilitários.

5.1.28 Normas: especificam no plano tático as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida pelas diretrizes;

5.1.29 Peer-to-Peer (P2P): é um tipo de programa que permite a distribuição de arquivos a outros usuários por meio da Internet.

5.1.30 POP (*Post Office Protocol*): protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

5.1.31 Segurança da informação: preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação.

5.1.32 Site: páginas contendo informações, imagens, fotos, vídeos, sons, etc, que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede;

5.1.33 Servidor de Correio Eletrônico: equipamento que provê o serviço de envio e recebimento de mensagens de correio eletrônico.

5.1.34 Software: programa de computador;

5.1.35 SMTP (*Simple Mail Transfer Protocol*): protocolo de comunicação usado para troca de mensagens na Internet via correio eletrônico.

5.1.36 Spam: qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.

5.1.37 Risco: combinação da probabilidade da ocorrência de um evento e de suas conseqüências;

5.1.38 Tratamento do risco: processo de seleção e implantação de medidas para modificar um risco.

5.1.39 Usuário: pessoa física formalmente autorizada a acessar o ambiente e as informações do SLU-DF e de suas estações;

5.1.40 Upload: envio de um arquivo de seu computador para outro, por meio da Internet.

5.1.41 URL: endereço utilizado para acessar a internet, intranet ou uma rede privada de computadores

5.1.42 Vírus Eletrônico: são pequenos programas que, a exemplo dos vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

6. DIRETRIZES DE SEGURANÇA:

6.1 A segurança é direcionada contra ameaças – naturais, acidentais ou intencionais -de destruição, modificação ou divulgação indevida das informações e para o impedimento de fraudes;

6.2 A informação deve ser tratada como um patrimônio a ser protegida no acesso, tráfego, uso e armazenamento, de acordo com sua classificação em graus de sigilo e criticidade;

6.3 A política de segurança deve ser conhecida e seguida por todos os usuários da instituição;

6.4 O Comitê Gestor da Tecnologia da Informação e das Comunicações – CGTIC- SLU-DF é responsável pela gestão de segurança e deve promover e disseminar a importância da segurança da informação e comunicações, por meio de programas de sensibilização e conscientização dos seus usuários;

6.5 A Diretoria de Modernização e Gestão Tecnológica – DIGET e responsável pelas ações de proteção da informação descritas no item 7.4 e o desenvolvimento de relatórios mensais para o Comitê Gestor de Tecnologia da Informação e Comunicação;

6.6 Registros e informações sigilosas devem ser protegidos contra perda, destruição e falsificação, sendo mantidos de forma segura para atender requisitos legais e regulamentares;

6.7 Os sistemas e equipamentos de informação e comunicações estão sujeitos a monitoração remota e eventual inspeção local, a fim de coibir a utilização indevida dos mesmos e danos resultantes desta utilização;

6.8 O monitoramento de que trata o item 7.7 será realizado pela Diretoria de Modernização e Gestão Tecnológica DIGET/SLU-DF. O resultado de qualquer monitoramento é considerado sigiloso e deverá tramitar como tal dentro de da empresa;

6.9 As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser precedidos de análise de custo/beneficio e balanceados de acordo com os danos potenciais de falhas de segurança;

6.10 Devem ser mantidos planos de contingência e recuperação de desastres, formais e

periodicamente testados, para garantir a continuidade das atividades críticas e o retorno à situação de normalidade, de acordo com os critérios definidos pelo Comitê Gestor da Tecnologia da Informação e das Comunicações – CGTIC/ SLU-DF;

6.11 O usuário deve ter acesso autorizado apenas às informações, instalações e recursos necessários e indispensáveis ao seu trabalho, de acordo com perfis definidos formalmente e:

a. Com o objetivo de resguardar a rede (internet) do Serviço de Limpeza Urbana do Distrito Federal serão bloqueados o uso de jogos, redes sociais, receitas, site de vídeos e músicas ou qualquer outro site que não seja compatível com as atribuições do setor;

b. É obrigatório o uso de conta email funcional para o exercício das atividades no SLU/DF; e

c. A autorização de acesso dos itens "a" deverá ser justificada e encaminha ao Comitê Gestor de Tecnologia e Comunicação.

6.12 O acesso a informações e sistemas de que trata o item 7.11 será concedido, ao usuário que tenha a necessidade de conhecer, mediante identificador pessoal (login) e senha, pessoal e intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento;

6.13 O usuário que tem acesso a informações confidenciais ou reservadas somente poderá fazer uso destas para os fins aprovados pelo respectivo gestor das informações, respeitando as regras de proteção estabelecidas;

6.14 Os usuários devem estar cientes das normas de segurança da informação vigentes no SLU-DF, bem como, dos procedimentos de segurança vigentes.

6.15 Deve ser disciplinado o uso correto da informação e de recursos computacionais de forma a minimizar possíveis riscos à segurança;

6.16 O acesso às informações que não sejam classificadas como públicas, dependerá da autorização do gestor da informação e deverá respeitar o grau de sigilo necessário, utilizando-a no estrito interesse da Administração em razão das suas atividades funcionais;

6.17 Quando do afastamento ou desligamento do usuário das suas atribuições faz-se necessário o cancelamento imediato dos direitos de acesso e uso da informação, além do preenchimento de termo de desligamento;

6.18 Os incidentes de segurança, tais como: indícios de fraude, sabotagem ou falha na segurança em processos, sistemas, instalações ou equipamentos devem ser prontamente notificados à chefia imediata e ao responsável pela gestão de segurança da informação do SLU-DF;

6.19 As condições e termos de licenciamento de software e os direitos de propriedade intelectual devem ser respeitados, estando vedada a instalação de programas de computador não homologados e licenciados pela DIGET do SLU-DF.

6.20 A instalação e o uso de sistemas e equipamentos para processamento de informação devem ser previamente homologados e autorizados pela DIGET, de acordo com os critérios definidos pelo CGTIC/SLU-DF;

6.21 Os recursos do SLU-DF e de suas entidades vinculadas não podem ser utilizados para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, nem veicular opiniões político-partidárias;

6.22 A entrada ou saída de equipamento computacional (patrimônio) das instalações da instituição deve ser informada pelo detentor do equipamento (responsável pelo bem patrimonial), sendo o trânsito permitido mediante a autorização da unidade competente;

7. DIRETRIZES PARA O CONTROLE E CLASSIFICAÇÃO DA INFORMAÇÃO

7.1 Classificação, os dados constantes nos bancos de dados dos sistemas de gestão das atividades metroviárias deverão ser classificados de acordo com o Decreto n. 4553, de 2002. Para tal a atribuição do grau de classificação será a seguinte:

7.1.1 **Ultra-secreto:** aqueles referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

7.1.2 **Secreto:** aqueles referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou

instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

7.1.3 **Confidencial:** aqueles que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

7.1.4 **Reservado**: aqueles cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

7.1.5 **Públicas ou Ostensivas**: todas as informações que não possuem grau de sigilo atribuído.

7.2 Competência de Classificação (gestores da informação), nos termos do Decreto 4.553/2002 as seguintes autoridades serão denominadas gestoras da informação e também responsáveis pela classificação, guarda, permissão de acesso as informações:

7.2.1 Atribuição do Grau de Sigilo **Ultra-secreto**: Ministros de Estado e Secretário Executivo: Poderão ser delegadas competências para outras autoridades.

7.2.2 Atribuição do Grau de Sigilo **Secreto, Confidencial e Reservado**: A autoridade com competência para a atribuição do grau ultra-secreto e as autoridades que exerçam funções de direção chefia ou assessoramento, de acordo com as atribuições regimentais definidas.

7.3 As autoridades descritas neste item serão as gestoras da informação e ficarão responsáveis pela classificação, guarda, concessão das permissões de acesso e por sua suspensão / cancelamento.

7.4 Gestores de Segurança, Nos termos do Decreto 4.553/2002 as seguintes autoridades serão responsáveis pela gestão da segurança da informação: Os membros do Comitê são responsáveis pela gestão da segurança da informação nas unidades que representam, bem como, deve resguardar a informação, comunicar a CGTIC sobre os incidentes de segurança.

8. RESPONSABILIDADES:

8.1 Relativamente à Política da Segurança da Informação e das Comunicações compete ao Comitê-Gestor de Tecnologia da Informação e das Comunicações do SLU-DF:

8.1.1 Propor e aprovar Normas Complementares que funcionarão em caráter acessório à Política de Segurança da Informação e das Comunicações – POSIC;

8.1.2 Apurar incidentes de segurança de caráter institucional, bem como propor às unidades competentes a investigação e a apuração de responsabilidade na eventual ocorrência destes;

8.1.3 Dispor sobre casos omissos e sobre a aplicação da Política de Segurança da Informação e das Comunicações – POSIC.

8.2 Compete aos Gestores da Informação:

8.2.1 Zelar pelo cumprimento da Política de Segurança da Informação e das Comunicações – POSIC;

8.2.2 Proceder à classificação dos dados e informações integrantes dos sistemas informatizados do SLU-DF;

8.2.3 Propor ao Comitê Gestor de Tecnologia da Informação e das Comunicações normas complementares para aplicação da Política de Segurança da Informação e das Comunicações – POSIC;

8.2.4 Comunicar à DIGET e ao Comitê de Tecnologia da Informação e das Comunicações quaisquer indícios de violação das normas de segurança da informação.

8.3 Compete a Diretoria de Modernização e Gestão Tecnológica - DIGET:

8.3.1 Zelar pelo cumprimento da Política de Segurança da Informação e das Comunicações – POSIC;

8.3.2 Adotar procedimentos operacionais com vistas a dar cumprimento às diretrizes da Política de Segurança da Informação e das Comunicações – POSIC e das Normas Complementares;

8.3.3 Instruir procedimentos técnicos de auditoria e investigação em casos de incidentes de segurança que vier a tomar conhecimento;

8.3.4 Propor ao Comitê Gestor de Tecnologia da Informação e das Comunicações normas complementares para aplicação Política de Segurança da Informação e das Comunicações – POSIC;

8.4 Compete aos usuários do SLU-DF e a todos os usuários externos que venham a usufruir de recursos tecnológicos e sistemas de informação do SLU-DF:

8.4.1 Zelar pelo cumprimento da Política de Segurança da Informação e das

Comunicações – POSIC;

8.4.2 Utilizar com probidade, responsabilidade e sigilo funcional as informações que tiver acesso ou conhecimento.

8.4.3 Não divulgar suas credenciais de segurança (logins e senhas).

8.4.4 Comunicar às autoridades competentes no SLU-DF sobre indícios de incidentes de segurança que venha a tomar conhecimento.

09. SANÇÕES

9.1 A violação das normas de segurança da informação e das comunicações constitui incidente de vulnerabilidade[6] e deverá ser apurado pela unidade competente no âmbito do SLU-DF;

9.2 O usuário que realizar ou colaborar para a realização de incidentes de segurança, comprovados pela área técnica competente, terá a suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais;

9.3 As penalidades e sansões serão impostas após a instauração do competente processo administrativo disciplinar.

Bruno Marques Presidente	André Pimenta Secretário Suplente
Everaldo Santos Membro	Victor Bruzzi Membro Suplente
Luiz Carlos Silva Membro Suplente	Avelange Duraes Membro Suplente

[6] São incidentes que ameaçam e fragilizam a rede interna do SLU-DF