06.181.6217.4031		MONITORAMENTO POR CÂMERA DE VÍDEO						
Ref. 004435	0001	MONITORAMENTO POR CÂMERA DE VÍDEO-SSP-DISTRITO FEDERAL						
			99	33.90.39	0	100	300.000	
								300.000
200101/00001	26101	SECRETARIA DE ESTADO DE TRANSPORTES DO DISTRITO FEDERAL						1.100.000
26.782.6216.3182		REFORMA DE TERMINAIS RODOVIÁRIOS						
Ref. 002206	0001	(***) REFORMA DE TERMINAIS RODOVIÁRIOS--DISTRITO FEDERAL						
		OBRA REALIZADA (M2) 0						
			99	44.90.51	2	100	1.100.000	
								1.100.000
200202/20202	26205	DEPARTAMENTO DE ESTRADAS DE RODAGEM - DER						601.246
26.451.6216.3197		CONSTRUÇÃO DE UNIDADES DO DER						
Ref. 002641	0001	CONSTRUÇÃO DE UNIDADES DO DER--DISTRITO FEDERAL						
		UNIDADE CONSTRUÍDA (UNIDADE) 0						
			99	44.90.51	0	100	601.246	
								601.246
310101/00001	27101	SECRETARIA DE ESTADO DE TURISMO DO DISTRITO FEDERAL						23.000
23.128.6001.4088		CAPACITAÇÃO DE SERVIDORES						
Ref. 002229	0022	CAPACITAÇÃO DE SERVIDORES-SECRETARIA DE TURISMO- PLANO PILOTO						
		SERVIDOR CAPACITADO (PESSOA) 0						

ANEXO II DESPESA R$ 1,00

CRÉDITO SUPLEMENTAR - ANULAÇÃO DE DOTAÇÕES ORÇAMENTO FISCAL

SUPLEMENTAÇÃO

RECURSOS DE TODAS AS FONTES

ESPECIFICAÇÃO			REG	NATUREZA	IDUSO	FONTE	DETALHADO	TOTAL
			1	33.90.39	0	120	23.000	
								23.000
340101/00001	34101	SECRETARIA DE ESTADO DE ESPORTE DO DISTRITO FEDERAL						70.000
27.812.6206.4170		MANUTENÇÃO DE ESPAÇOS ESPORTIVOS						
Ref. 002387	0001	(***) MANUTENÇÃO DE ESPAÇOS ESPORTIVOS--DISTRITO FEDERAL						
		UNIDADE MANTIDA (UNIDADE) 3						
			99	44.90.52	0	100	70.000	
								70.000
480101/00001	48101	DEFENSORIA PÚBLICA DO DISTRITO FEDERAL						300.000
28.846.0001.9050		RESSARCIMENTOS, INDENIZAÇÕES E RESTITUIÇÕES						
Ref. 001913	7028	RESSARCIMENTOS, INDENIZAÇÕES E RESTITUIÇÕES-CENTRO DE ASSISTÊNCIA JUDICIÁRIA DO DF-DISTRITO FEDERAL						
			99	33.90.93	0	100	300.000	
								300.000
2013AC00406							TOTAL	5.936.403

CONSELHO DE PARCERIAS PÚBLICO-PRIVADAS

RESOLUÇÃO N° 67, DE 07 DE OUTUBRO DE 2013.

Dispõe sobre aprovação de estudo e abertura de licitação de PPP na área de Mobilidade Urbana.

O CONSELHO GESTOR DE PARCERIAS PÚBLICO-PRIVADAS – CGP, no uso das atribuições que lhe conferem a Lei nº 3.792, de 2 de fevereiro de 2006, alterada pela Lei nº 4.828/2012, resolve:

Art. 1º aprovar, de acordo com a análise realizada pela Comissão Técnica instituída pela Portaria nº 09, de 11 de junho de 2013, os estudos técnicos, de viabilidade econômico-financeira e jurídico-institucional para a área de Mobilidade Urbana, em modelagem de Parceria-Público-Privada, realizados pelo Consórcio formado pelas empresas OAS S.A e JC Gontijo Engenharia S.A., conforme Chamada Pública nº 03/2012, de 03 de dezembro de 2012.

Art. 2º Fica autorizada a abertura do procedimento licitatório, nos termos do artigo 14, II, da Lei nº 3.792, de 2 de fevereiro de 2006, ressaltando-se que o Edital deverá ser elaborado com a participação da Procuradoria-Geral do Distrito Federal.

Brasília/DF, 07 de outubro de 2013

AGNELO QUEIROZ

Governador do Distrito Federal

Presidente do Conselho

ATA DE REUNIÃO DO CONSELHO GESTOR DE PARCERIAS PÚBLICO-PRIVADAS

Aos sete dias do mês de outubro do ano de 2013, no gabinete do governador do Distrito Federal, reuniu-se o Conselho Gestor de Parcerias Público-Privadas para deliberar sobre as matérias a seguir discriminadas, quando estiveram presentes o Senhor Governador do Distrito Federal e Presidente do Conselho Gestor de Parcerias Público-Privadas, AGNELO QUEIROZ, os senhores membros efetivos do Conselho, os Secretários de Estado GUSTAVO PONCE DE LEON SORIANO LAGO, ADONIAS DOS REIS SANTIAGO, SWEDENBERGER DO NASCIMENTO BARBOSA, LUIZ PAULO TELES FERREIRA BARRETO, a Procuradora-Geral do Distrito Federal, PAOLA AIRES CORRÊA LIMA e o membro eventual, o Secretário de Estado, DAVID JOSÉ DE MATOS. Havendo quórum legal, o presidente declarou abertos os trabalhos. Inicialmente, foi designado o Secretário Executivo deste Conselho, o Sr. MÁRCIO GALVÃO FONSECA para secretariar os trabalhos. Após discutidas as questões relativas às deliberações e votadas as matérias constantes da pauta, o Conselho, por unanimidade resolveu:

- aprovar, de acordo com a análise realizada pela Comissão Técnica instituída pela Portaria nº 09, de 11 de junho de 2013, os estudos técnicos, de viabilidade econômico-financeira e jurídico-institucional para a área de Mobilidade Urbana, em modelagem de Parceria-Público-Privada, realizados pelo Consórcio formado pelas empresas OAS S.A e JC Gontijo Engenharia S.A., conforme Chamada Pública nº 03/2012, de 03 de dezembro de 2012.
- autorizar a abertura do procedimento licitatório, nos termos do artigo 14, II, da Lei nº 3.792, de 2 de fevereiro de 2006, ressaltando-se que o Edital deverá ser elaborado com a participação da Procuradoria-Geral do Distrito Federal.

Nada mais havendo a tratar, foi encerrada a reunião. E, para constar, eu, Márcio Galvão Fonseca, Secretário Executivo do Conselho, designado, portanto, para conduzir a reunião, redigi, lavrei e datei a presente ata, que após lida, vai assinada por mim e pelos demais conselheiros.

AGNELO QUEIROZ

Presidente do Conselho Gestor de Parcerias Público-Privadas

Governador

MÁRCIO GALVÃO FONSECA, Secretário-Executivo do Conselho Gestor de Parcerias Público-Privadas; GUSTAVO PONCE DE LEON SORIANO LAGO, Conselheiro - Membro Efetivo; Secretário de Estado de Governo; ADONIAS DOS REIS SANTIAGO, Conselheiro - Membro Efetivo, Secretário de Estado de Fazenda; SWEDENBERGER DO NASCIMENTO BARBOSA, Conselheiro - Membro Efetivo, Secretário Chefe da Casa Civil da Governadoria; PAOLA AIRES CORRÊA LIMA, Conselheira - Membro Efetivo; Procuradora-Geral do Distrito Federal; LUIZ PAULO TELES FERREIRA BARRETO, Conselheiro - Membro Efetivo; DAVID JOSÉ DE MATOS, Membro Eventual, Secretário de Estado de Obras.

CASA CIVIL

COORDENADORIA DAS CIDADES

ORDEM DE SERVIÇO Nº 26, DE 17 DE OUTUBRO DE 2013.

O COORDENADOR-CHEFE DA COORDENADORIA DAS CIDADES, DA CASA CIVIL, DA GOVERNADORIA DO DISTRITO FEDERAL, no uso das atribuições regimentais e considerando o disposto no artigo 3º, do Decreto nº 23.536/2003, RESOLVE: TORNAR SEM EFEITO o extrato de cancelamento da Notificação de Sinal 1140/2012, referente ao processo 131.000.910/2012, publicado no DODF nº 91, em 06/05/2013, pág. 68.

FRANCISCO CHAGAS MACHADO FILHO

SECRETARIA DE ESTADO DE TRANSPARÊNCIA E CONTROLE

PORTARIA Nº 204, DE 16 DE OUTUBRO DE 2013.

Aprova a Política de Segurança da Informação - PSI e a Política de Uso de Correio Eletrônico - PUC da Secretaria de Estado de Transparência e Controle do Distrito Federal.

O SECRETÁRIO DE ESTADO DE TRANSPARÊNCIA E CONTROLE DO DISTRITO FEDERAL - substituto, no uso das atribuições que lhe confere o artigo 105, parágrafo único, incisos

I, III e V da Lei Orgânica do Distrito Federal, artigo 8, incisos II, VII e XIX da Lei nº 3.105, de 27 de dezembro de 2002, o Decreto Distrital nº 32.735, de 28 de janeiro de 2011, que modificou o art. 46 do Decreto nº 32.716, de 1º de janeiro de 2011, e com base no disposto no artigo 57, incisos II e VII do Regimento Interno da Corregedoria-Geral do Distrito Federal, anexo ao Decreto nº 24.582, de 11 de maio de 2004 e atendendo aos requisitos da legislação de regência a Lei nº 2.572, de 20 de julho de 2000, RESOLVE:

Art. 1º Ficam aprovadas, na forma dos Anexos I e II desta Portaria, a Política de Segurança da Informação e a Política de Uso de Correio Eletrônico da Secretaria de Estado de Transparência e Controle do Distrito Federal - PSI/STC.

Parágrafo único. A PSI/STC e a PUC/STC aplicam-se a todas as unidades da estrutura administrativa da Secretaria de Estado de Transparência e Controle do Distrito Federal e deverão ser fielmente observadas por todos os servidores, colaboradores, estagiários, consultores externos e prestadores de serviços, sob pena de responsabilidade, na forma da lei.

Art. 2º São objetivos da PSI/STC:

I - cumprir a Lei Distrital nº 2.572, de 20 de julho de 2000, que dispõe sobre a prevenção das entidades públicas do DF com relação aos procedimentos praticados na área de informática, e sua regulamentação, o Decreto nº 25.750, de 12 de abril de 2005;

II - cumprir o inciso II do art. 6º da Lei Federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - orientar os agentes públicos e prestadores de serviço acerca da importância da segurança da informação, com destaque à confiabilidade, integridade e disponibilidade;

IV - fomentar e disseminar a cultura da Segurança da Informação, sensibilizando todos os agentes públicos e prestadores de serviço da STC sobre a necessidade de protegê-la;

V - incrementar a segurança do ambiente da STC por meio da redução de riscos negativos.

Art. 3º É objetivo da PUC/STC:

I - estabelecer normas gerais de utilização do e-mail corporativo na STC, bem como, a definição de procedimentos específicos de uso e criação de contas de correio eletrônico.

Art. 4º Fica instituído o Comitê de Segurança da Informação da Secretaria de Estado de Transparência e Controle do Distrito Federal – CSI/STC.

Parágrafo Único. Compete ao CSI/STC:

I - estabelecer as regras de proteção dos ativos da STC, revisá-las e propor a sua atualização, pelo menos com periodicidade anual;

II - revisar os documentos do Sistema de Gestão de Segurança da Informação visando à melhoria contínua e aos avanços no nível de maturidade em Segurança da Informação;

III - analisar as infrações relativas à Segurança da Informação cometidas por servidores da STC, propondo as providências cabíveis; e

IV - executar outras atividades, em nível decisório, que impliquem a gestão eficiente da PSI/STC.

Art. 5º Os editais de licitação e os contratos administrativos elaborados no âmbito da Secretaria de Estado de Transparência e Controle do Distrito Federal deverão conter cláusula específica sobre a obrigatoriedade de atendimento às normas da PSI/STC.

§ 1º Os Agentes Públicos e Prestadores de Serviço na STC deverão assinar Termo de Responsabilidade, cujo modelo está contido no item 8, Anexo I desta portaria.

§ 2º As empresas contratadas também deverão demonstrar que possuem mecanismos formais de segurança que assegurem o sigilo das informações.

Art. 6º Revoga-se a Portaria nº 205, de 15 de dezembro de 2010.

Art. 7º Essa Portaria entra em vigor na data de sua publicação.

MAURO ALMEIDA NOLETO

ANEXO I

SECRETARIA DE ESTADO DE TRANSPARÊNCIA E CONTROLE DO DISTRITO FEDERAL

UNIDADE DE ADMINISTRAÇÃO TECNOLÓGICA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

1. INTRODUÇÃO

A Secretaria de Estado de Transparência e Controle do Distrito Federal – STC tem a missão institucional de "Orientar e controlar a correta aplicação dos recursos públicos, por meio de uma gestão transparente e com a participação da sociedade".

Neste contexto, a informação é a matéria-prima da atividade finalística da STC e deve ser protegida para garantir o fiel cumprimento de sua missão. A Política de Segurança da Informação – PSI é o instrumento destinado a orientar o uso e armazenamento adequados das informações da STC.

2. OBJETIVOS

• Cumprir a Lei Distrital nº 2.572, de 20 de julho de 2000, que dispõe sobre a prevenção das entidades públicas do DF com relação aos procedimentos praticados na área de informática, e sua regulamentação, o Decreto nº 25.750, de 12 de abril de 2005;

• Cumprir o inciso II do art. 6º da Lei Federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

• Orientar os agentes públicos e prestadores de serviços acerca da importância da Segurança da Informação, com destaque à confidencialidade, integridade e disponibilidade;

• Fomentar e disseminar a cultura da Segurança da Informação, sensibilizando todos os agentes públicos e prestadores de serviços da STC sobre a necessidade de protegê-la;

• Incrementar a segurança do ambiente da STC por meio da redução de riscos negativos.

3. PAPÉIS E RESPONSABILIDADES

Cabe aos agentes públicos e prestadores de serviços da STC:

• Conhecer as regras da PSI e cumpri-las;

• Tratar com zelo as informações sob sua responsabilidade.

Cabe aos gestores da STC e a seus substitutos formalmente designados, cumulativamente:

• Incentivar a participação dos servidores em eventos de Segurança da Informação - SI;

• Comunicar ao Comitê de Segurança da Informação – CSI, na figura de seu Presidente, ocorrências relativas à SI;

• Notificar tempestivamente à Diretoria de Gestão de Pessoas a movimentação de agentes públicos;

• Disseminar as regras da PSI e cobrar o efetivo cumprimento;

• Operacionalizar deliberações do CSI;

• Propor medidas referentes à SI.

Cabe à Unidade de Administração Tecnológica - UAT e à Subsecretaria de Administração Geral - SUAG:

• Propor o uso das melhores práticas e ferramentas voltadas para SI;

• Operacionalizar deliberações do CSI;

• Propor medidas visando à SI;

• Fornecer apoio técnico ao CSI.

Cabe ao CSI:

• Elaborar e revisar a PSI;

• Propor campanhas de conscientização, palestras e treinamentos;

• Participar da revisão da Matriz de Riscos;

• Participar da elaboração do Plano de Continuidade do Negócio – PCN;

• Deliberar sobre as questões relacionadas à Segurança da Informação não previstas nesta PSI.

4. CONCEITOS E DEFINIÇÕES

Agente Público - O agente público é todo aquele que presta qualquer tipo de serviço ao Estado, funções públicas, no sentido mais amplo possível dessa expressão, significando qualquer atividade pública. A Lei de Improbidade Administrativa (Lei nº 8.429/92), em seu art. 2º, conceitua agente público como "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 nas entidades mencionadas no artigo anterior". Trata-se, pois, de um gênero do qual são espécies o servidor público, o empregado público, o terceirizado e o contratado por tempo determinado.

Ativo - Qualquer coisa que tenha valor para a organização.

Ativos físicos - Computadores, equipamentos de comunicação, mídia removível e outros equipamentos.

Ativos lógicos - Bancos de dados, arquivos, documentação de sistemas, manuais do usuário, Planos de Continuidade do Negócio e programas de computador (software).

Ambiente - Entende-se por ambiente a estrutura física e lógica da Secretaria, contemplando todos os ativos – qualquer coisa que tenha valor para a organização.

Autenticação - Procedimento utilizado na identificação de usuários, dispositivos ou processos, e que é pré-requisito para o acesso aos recursos de um sistema.

Backup - Cópia de segurança de um arquivo em um dispositivo diferente daquele onde se encontra o arquivo original, por motivo de segurança, com a finalidade de restaurar o arquivo original, em caso de necessidade.

Comitê de Segurança da Informação (CSI) - Equipe com representantes de diversas áreas funcionais da organização que suporta as ações e decisões em Segurança da Informação.

Confidencialidade - Requisito que determina que uma informação não seja disponibilizada ou revelada para partes não autorizadas.

Controle de Acesso - Mecanismo utilizado para proteger os recursos de um sistema de acesso não autorizado. Deve permitir, de acordo com uma Política de Segurança da Informação, o acesso somente a entidades autorizadas, como usuários, processos, programas ou outros sistemas.

Corrente de e-mail - Evento que ocorre quando um e-mail é enviado para diversos conhecidos ao mesmo tempo e, eventualmente, repassado adiante podendo se espalhar em ritmo exponencial a milhares ou até milhões de pessoas.

Criptografia - Disciplina que trata dos princípios, meios e métodos para a transformação de dados, tornando-os ininteligíveis, de forma a possibilitar a detecção de modificações no conteúdo da informação e/ou prevenir seu uso não autorizado.

Custódia - Responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.

Disponibilidade - Requisito que determina que os recursos de um sistema estejam disponíveis para acesso, por entidades autorizadas, sempre que solicitados.

Drives públicos - Local para armazenamento de arquivos lógicos nos computadores (servidores) de rede da STC. É a unidade de rede identificada pela letra "G" no computador dos usuários, após autenticação na rede.

Estações de trabalho - São os computadores do tipo desktop e notebooks.

Gestor da Informação - Pessoa ou área funcional que autoriza ou nega o pedido de acesso a certa informação.

Gestor - Pessoa responsável pela gestão de alguma área, como gerente ou diretor.

Incidente de Segurança - Um incidente de segurança é caracterizado por qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas computacionais ou de redes de computadores. São exemplos: tentativas de obter acesso não autorizado a sistemas ou dados, uso ou acesso não autorizado a um sistema e desrespeito à Política de Segurança da Informação.

Integridade - Requisito que determina que uma informação não seja modificada ou destruída de maneira não autorizada ou acidental.

Logs - Arquivos de anotações ou listas sistemáticas de registro de eventos ocorridos.

Matriz de Risco - Tabela que contém um levantamento de riscos identificados na organização.

Mecanismos de Controle de Acesso - Mecanismos de hardware ou software, procedimentos operacionais ou gerenciais, usados para detectar e prevenir acessos não autorizados a sistemas computacionais.

Não repúdio - Garantia de segurança que impede uma entidade participante numa dada operação de negar essa participação.

Plano de Continuidade do Negócio - Coleção de procedimentos e informações que são desenvolvidos, compilados e mantidos prontos para uso em caso de um incidente de segurança, com a finalidade de possibilitar que a organização continue a conduzir suas atividades críticas em um nível aceitável.

Política de Segurança da Informação - Conjunto de diretrizes destinadas a definir a proteção

adequada dos ativos produzidos pelos Sistemas de Informação. Ela atribui direitos e responsabilidades aos indivíduos que lidam com os recursos computacionais de uma instituição e com as informações neles armazenadas. Define as atribuições de cada indivíduo em relação à segurança dos recursos com os quais trabalha. Qualquer evento que resulte no descumprimento da Política de Segurança da Informação é considerado um incidente de segurança.
Prestador de Serviço - Pessoa fisica ou jurídica contratada pela STC para prestação de serviços.
Proteção dos Ativos - Processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade.
Senha Fraca ou Óbvia - Senha na qual se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena tal como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado, dentre outras.
Sigilo - Classificação dada a informações às quais apenas entidades autorizadas e previamente autenticadas poderão ter acesso.
VPN – Virtual Private Network - Rede privada virtual. Forma de acessar a rede de dados da STC de maneira segura, quando em trabalho externo. Equivale ao acesso interno a rede de dados.
5. REGRAS GERAIS
São vedadas no âmbito da STC as atividades que atentem contra a legalidade, a moralidade, e contra a ética administrativa. Aquele que incorrer nas hipóteses deste item estará sujeito às penalidades previstas na legislação. Em consonância com a Lei Complementar nº 840/2011-DF estão previstas sanções nos artigos 199, 200 e 202 referentes às infrações relacionadas a Tecnologia da Informação. Em conformidade com a Lei nº 9.983/2000 estão previstas diversas sanções como multas e/ou detenção.
Os produtos desenvolvidos por agente público ou prestador de serviço são de propriedade exclusiva desta Secretaria. A reprodução destes programas requer prévia autorização.
Em conformidade com a Lei Federal nº 9.609, de 20 de fevereiro de 2002, a utilização dos recursos de TI deverá respeitar os direitos de propriedade intelectual de qualquer pessoa ou empresa.
Além das normas vigentes sobre a matéria, e das previstas no artigo 190, inciso XIV, artigo 192, incisos V e VI, e artigo 194, inciso II, da Lei Complementar nº 840/2011, são aplicáveis, no âmbito da STC, as seguintes regras:
5.1. REQUISITOS DE SEGURANÇA DO AMBIENTE HUMANO
Ambiente Humano é aquele composto por procedimentos a serem observados por agentes públicos e prestadores de serviços para a proteção dos ativos.
5.1.1. Do Ambiente Humano.
Nas instalações da STC e em cumprimento à Portaria nº 216/2010, de 28/12/2010, da SEPLAN, todos os agentes públicos ou prestadores de serviço deverão usar instrumento/meio de identificação.
5.1.1.1. Quanto à Admissão.
Antes da criação de uma identificação de usuário, solicitada formalmente pelo gestor, o agente público assinará o Termo de Responsabilidade perante a área de Gestão de Pessoas; o prestador de serviço assinará o Termo de Responsabilidade perante o Executor do Contrato, ou perante SUAG na ausência do Executor.
O termo de confidencialidade será incorporado aos contratos da STC.
5.1.1.2. Quanto ao Acompanhamento.
O gestor deverá estar atento a situações que possam representar ameaças à segurança da informação. Uma vez identificadas, as vulnerabilidades devem ser encaminhadas ao CSI, na figura de seu Presidente, para conhecimento e deliberação.
O agente público será estimulado a cumprir as regras dispostas nesta PSI por meio de programas de conscientização, palestras e treinamentos.
5.1.1.3. Quanto ao Desligamento.
A identificação fornecida e qualquer equipamento deverão ser devolvidos, bem como serão revogadas as permissões de uso de equipamentos, de mecanismos e de acessos físicos e lógicos da STC.
Quando um usuário encerrar suas atividades, seus arquivos armazenados na rede ou em estações de trabalho, assim como seus documentos em papel deverão ser revisados pela chefia imediata para determinar quem se tornará responsável pelas informações relacionadas e, se for o caso, identificar o método mais adequado para a eliminação dessas informações.
5.1.1.3.1 Quanto à Liberação.
O agente público ou prestador de serviço firmará, antes do desligamento e perante a área de Gestão de Pessoas, declaração de que não possui qualquer tipo de pendência junto às unidades que compõem a STC.
5.2. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO
Ambiente físico é aquele composto por todo o ativo permanente.
5.2.1. Regras gerais do Ambiente Físico.
A proteção física dos equipamentos de TI será efetuada mediante o acondicionamento em ambientes e controle de acesso adequado. Lei Distrital nº 2.572, de 20 de julho de 2000.
A SUAG e a UAT providenciarão as medidas necessárias para o alcance do nível de segurança física adequado, acionando as áreas correlatas.
5.3. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO
Ambiente lógico é composto por todo o ativo de informações.
5.3.1. Regras gerais do Ambiente Lógico.
A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, a Gerência de Documentação - GEDOC deve elaborar normas de classificação e tratamento de informações, bem como divulgá-las na STC.
Os dados, as informações e os sistemas de informação da organização e os sob sua guarda devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, confidencialidade e disponibilidade desses bens.
A divulgação de informação sigilosa, ou seja, aquela submetida temporariamente à restrição de acesso público, conforme disposto a norma nº 12.527/2011 - Lei de Acesso à Informação, não deve ser permitida, exceto quando autorizada por instância superior competente. Da mesma maneira, trechos, resumos, traduções ou qualquer material derivado de informações sigilosas ou resguardadas por direitos autorais devem seguir as regras de acordo com a sua classificação e grau de sigilo adotado.
Informações sigilosas armazenadas em mídia legível de computador (CDs, DVD, pen drive, etc.), deverão ser, quando possível, criptografadas quando enviadas por mensageiro, observando sempre o disposto na legislação vigente. Da mesma forma, quando uma informação sigilosa for enviada para redes externas, como a Internet, deve estar criptografada, salvo caso de impossibilidade técnica.
A informação sigilosa, armazenada em CDs, DVDs, fitas magnéticas, dispositivos de gravação ótica, pen drives, cartões de memória e assemelhados, ou em quaisquer outros meios magnéticos computacionais, deve ser apagada por meio de programas desenvolvidos para essa finalidade, uma vez que a simples reformatação não elimina totalmente a informação.
Dúvidas sobre criptografia ou sobre formas de formatação devem ser esclarecidas junto à UAT.
5.4. OUTRAS ORIENTAÇÕES
Utilizar somente estações de trabalho fornecidas pela UAT. O uso de notebooks particulares ou outros dispositivos de propriedade pessoal será autorizado após solicitação formal à UAT e avaliação dos impactos de segurança.
Não conectar computadores portáteis a redes não homologadas pela STC; utilizar, preferencialmente, o modem 3G e acessar aplicativos relacionados às atividades profissionais.
As estações de trabalho devem ser protegidas contra danos ou perdas, bem como contra acesso, uso ou exposição indevidos. Quando se distanciarem das estações de trabalho, os usuários devem bloqueá-las.
Deve-se evitar comer ou beber próximo aos equipamentos e dispositivos de TI.
Deve-se desligar equipamentos ao fim do expediente e guardar os dispositivos portáteis em local seguro.
Utilizar preferencialmente drive público para armazenamento de arquivos; no caso de trabalho remoto ou externo, arquivos gerados podem ser armazenados em drives locais, mas devem ser copiados para os drives públicos ao retorno às instalações do órgão ou via VPN – Virtual Private Network. Drives públicos são sujeitos a processos de cópia de segurança (backup), enquanto que drives locais e mídias (CDs, DVDs, pen drives, por exemplo) não são sujeitos a tais processos e, portanto, expostos a maiores riscos.
Armazenar nos drives públicos apenas conteúdos relacionados ao trabalho. Fotos, músicas, filmes e outros arquivos pessoais serão excluídos por meio de um processo periódico de limpeza de dados.
Utilizar correio eletrônico (“e-mail”) para as atividades profissionais e observar o limite de das caixas postais, conforme documento específico sobre uso de e-mail.
As senhas são de uso PESSOAL e INTRANSFERÍVEL.
Utilizar senhas que contenham no mínimo oito caracteres, compostas de caracteres de pelo menos 3 das 4 categorias a seguir: letras maiúsculas (A – Z), letras minúsculas (a – z), dígitos de base 10 (0 a 9), caracteres especiais (!, $, #, %). Deve-se evitar o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários (vide item 4 – Senha Fraca ou Óbvia).
Alterar periodicamente a senha. Será necessário alterar a senha a cada 180 (cento e oitenta) dias e não será permitida a repetição das últimas 2 (duas) senhas cadastradas. Caso uma senha seja digitada de modo errado por 3 (três) vezes consecutivas, o acesso à rede será bloqueado e restabelecido por meio de intervenção da UAT.
Manter o caráter sigiloso da senha de acesso aos recursos e sistemas; em sistema no qual é possível armazenar a senha na tela de entrada, tal opção nunca deve ser selecionada.
Ao realizar transações via web, certificar-se da procedência do sítio e da utilização de conexões seguras (criptografadas – HTTPS), além de buscar garantir que o endereço apresentado no navegador corresponda ao que se quer acessar, antes de realizar qualquer ação.
Todos os softwares e arquivos transferidos de fontes que não sejam da STC, via Internet ou qualquer outra rede pública, devem ser examinados com o software de detecção de vírus em uso. Esse exame deve acontecer antes que o arquivo seja executado ou aberto por outro programa, como, por exemplo, um editor de texto, e também antes e depois que o material tenha sido descompactado.
O usuário deve utilizar apenas softwares homologados pela UAT, a qual estabelecerá os aspectos de controle, distribuição e instalação de softwares, devendo ser consultada em caso de dúvidas.
6. REFERÊNCIAS NORMATIVAS
6.1. Lei Distrital nº 2.572, de 20 de julho de 2000.
Dispõe sobre a prevenção das entidades públicas do DF com relação aos procedimentos praticados na área de informática.
6.2. Decreto Distrital nº 25.750, de 12 de abril de 2005.
Regulamenta a Lei Nº 2.572.
6.3. Lei Federal nº 12.527, de 18 de novembro de 2011.
Regula o acesso a informações previsto na Constituição Federal.
6.4. Lei Complementar nº 840-DF, de 23 de dezembro de 2011.
Dispõe sobre o regime jurídico dos servidores públicos civis do Distrito Federal, das autarquias e das fundações públicas distritais.
6.5. Lei nº 9.609, de 19 de fevereiro de 1998.
Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
6.6. Lei nº 9.983, de 14 de julho de 2000.
Atualiza o Código Penal e dá outras providências.
6.7. Portaria DF nº 216, de 27 de dezembro de 2010.
Estabelece normas para uso e ocupação do Edifício Anexo do Palácio do Buriti.
6.8. Normas ABNT NBR ISO/IEC 27001 e 27002.
Instituem as melhores práticas para Gestão da Segurança da Informação.
6.9. Portaria nº 152, de 13 de julho de 2012.
Designa membros do Comitê de Segurança da Informação no âmbito da Secretaria de Estado de Transparência e Controle.

7. CONCLUSÃO (PSI)
A Secretaria de Transparência e Controle aprova a revisão da Política de Segurança da Informação, alinhada a sua missão institucional e plano estratégico, em consonância com a realização de atividades lícitas, éticas e administrativamente permitidas e observando os objetivos de confidencialidade, integridade e disponibilidade.
Fica determinado a todos seus agentes públicos ou prestadores de serviços o integral cumprimento das regras estabelecidas, devendo ser observados os requisitos de segurança do ambiente humano, físico e lógico, sob pena das responsabilizações penais, civis e administrativas de que tratam a Lei Complementar 840/2011.
8. ADENDO(S)
TERMO DE RESPONSABILIDADE
Em consonância com a Portaria nº 204, de 16 de outubro de 2013, que aprova a revisão da Política de Segurança da Informação da Secretaria de Estado de Transparência e Controle do Distrito Federal - STC, bem como com os artigos 190, inciso XIV, 192, incisos V e VI e 194, inciso II, da Lei Complementar nº 840/2011, declaro-me ciente de que o uso indevido ou fraudulento de quaisquer recursos disponibilizados poderá ensejar apuração de responsabilidade e aplicação de penalidades.
Declaro-me ainda ciente de que a Unidade de Administração Tecnológica e/ou o Comitê de Segurança da Informação resguardará(ão) o direito de rescindir o acesso a qualquer recurso de TI, a qualquer momento, e sem que seja previamente comunicado, desde que tal ato seja imprescindível para manter a segurança da informação na STC.
Nome:_____
Matrícula: _____ CPF:_____ Data: __/__/_____
Assinatura:_____

ANEXO II
SECRETARIA DE ESTADO DE TRANSPARÊNCIA E CONTROLE DO DISTRITO FEDERAL
UNIDADE DE ADMINISTRAÇÃO TECNOLÓGICA
POLÍTICA DE USO DE CORREIO ELETRÔNICO (E-MAIL)

1. OBJETIVO
O presente documento tem por finalidade o estabelecimento de normas gerais de utilização do e-mail corporativo na STC, bem como, a definição de procedimentos específicos de uso e criação de contas de correio eletrônico.
2. DEFINIÇÕES
E-mail corporativo: conta de correio eletrônico de uso corporativo, neste caso, de uso exclusivo para os trabalhos da Secretaria (ex.: nome.sobrenome@stc.df.gov.br);
Correio eletrônico: recurso de TI da STC que possibilita a troca de mensagens e arquivos, por meio de uma rede de comunicação de dados;
Recurso de TI: além da própria informação eletrônica, todo meio direto e indireto utilizado para sua transformação, tratamento, armazenamento, tráfego e segurança;
Usuário: qualquer agente público que utiliza os recursos de TI do ambiente STC;
Caixa de correio: local privado disponível na aplicação Microsoft Outlook.
3. DISPOSIÇÕES GERAIS
O usuário que utiliza o correio eletrônico corporativo da STC deve estar ciente que este possui recursos de armazenamento e disponibilidade de caixas de correio limitados.
A obtenção de acesso pelo usuário ao correio eletrônico está também condicionada ao aceite do Termo de Responsabilidade constante na Política de Segurança da Informação (PSI).
4. DEVERES DO USUÁRIO
O usuário é responsável pela utilização adequada de sua conta de e-mail de forma a não efetuar qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou da própria STC, em consonância com as determinações da Lei Complementar 840/2011, de 23 de dezembro de 2011, em especial os artigos 190 inciso XIV e 192 incisos V e VI. In Verbis:
Art. 190. São infrações leves: (...)
XIV - acessar, armazenar ou transferir, intencionalmente, com recursos eletrônicos da administração pública ou postos à sua disposição, informações de conteúdo pornográfico ou erótico, ou que incentivem a violência ou a discriminação em qualquer de suas formas.
Art. 192. São infrações médias do grupo II: (...)
V - usar recursos computacionais da administração pública para, intencionalmente:
a) violar sistemas ou exercer outras atividades prejudiciais a sites públicos ou privados; disseminar vírus, cavalos de tróia, spyware e outros males, pragas e programas indesejáveis;
b) disponibilizar, em sites do serviço público, propaganda ou publicidade de conteúdo privado, informações e outros conteúdos incompatíveis com os fundamentos e princípios da administração pública;
c) repassar dados cadastrais e informações de servidores públicos ou da repartição para terceiros, sem autorização.
VI - permitir ou facilitar o acesso de pessoa não autorizada, mediante atribuição, fornecimento ou empréstimo de senha ou qualquer outro meio:
a) a recursos computacionais, sistemas de informações ou banco de dados da administração pública;
b) a locais de acesso restrito.
5. PROCEDIMENTOS OPERACIONAIS
As contas de correio eletrônico só serão criadas para agentes públicos em atividade na STC, ressalvados casos de necessidade especial de serviço.
Estagiários em atividade na STC terão permissão apenas para enviar e receber e-mails internos, ressalvados casos de necessidade especial do serviço.
Atualmente, há um limite de envio de mensagens para 35 (trinta e cinco) destinatários. Alguns perfis estão autorizados a ultrapassar este limite, por exemplo: usuários do Gabinete da STC e usuários da Assessoria de Comunicação – ASCOM.
Os recursos de armazenamento para as caixas de correio corporativas serão definidos de acordo com as especificações do Anexo I. Os usuários devem gerenciar as suas caixas postais de modo a observar os limites de armazenamento previstos.
Cada mensagem de correio, incluindo anexos, tem o seu tamanho limitado a 12 MB (Mbytes) para envio e recebimento.
Será adotado como padrão de endereço de e-mail corporativo, o formato nome.sobrenome@stc.df.gov.br. No caso do nome e sobrenome já estar sendo utilizado por outro endereço de e-mail ou havendo justificativa fundamentada, será escolhido outro sobrenome do usuário para compor o endereço de e-mail.
Fica mantido o cadastro de contas de e-mail existente até a data deste normativo.
Fica facultado ao usuário que esteja com o endereço de e-mail em desacordo com esta norma solicitar a sua adequação. Esta adequação não influenciará no recebimento de mensagens pelo endereço antigo.
Para os grupos de usuários será adotado o padrão de nomenclatura composto pelo caracter '*' seguido da palavra Grupo e do nome da área. Exemplo: *Grupo UAT. Todos os servidores do setor UAT compõem esse grupo de distribuição. Isso significa que ao encaminhar uma mensagem para esse grupo, todos servidores da UAT receberão o e-mail. É possível criar o papel de moderador para os grupos com o objetivo de definir um ou mais usuários para autorizar a entrega das mensagens encaminhadas aos grupos.
Para as contas de serviço, o padrão de nomenclatura são os caracteres 'S_' seguindo do nome do serviço. Exemplo: S_Capacitacao. Para as contas de serviço, são definidos os usuários que terão permissão para gerenciar os e-mails que chegam para essas contas.
Todas as mensagens encaminhadas pelo servidor de e-mail da STC possuem o termo de isenção de responsabilidade (DISCLAIMER), com o seguinte texto padrão: A informação contida nesta mensagem de e-mail, incluindo quaisquer anexos, é de uso exclusivo do destinatário e pode conter informações confidenciais e/ou privilegiadas. Se você não é o destinatário designado, qualquer uso, cópia, divulgação, veiculação ou distribuição é estritamente proibido. Caso você tenha recebido esta mensagem por engano, por favor, notifique o remetente imediatamente, respondendo este e-mail, e apague esta mensagem de seu computador ou de qualquer outro banco de dados.
CONCLUSÃO
A Secretaria de Transparência e Controle aprova a Política de Uso de Correio Eletrônico (e-mail).
Fica determinado a todos seus agentes públicos ou prestadores de serviços o conhecimento desta Política para uso adequado do serviço de e-mail da STC.
Anexo I – Limites das Caixas de Correio da STC

Perfil do Usuário	Limite de Aviso	Proibição de Envio	Proibição de Envio e Recebimento
Secretário e Subsecretário	Não se aplica	Não se aplica	10 GB
Chefes, Diretores, Gerentes e Assessores	1,9 GB	2 GB	2 GB
Servidores	0,9 GB	1 GB	1,3 GB
Estagiários	33 MB	35 MB	40 MB
Serviços Corporativos	9 GB	10 GB	10 GB

Perfil do Usuário: Critério para a classificação de usuários ou grupo de usuários com características semelhantes.
Limite de Aviso: Alerta que indica quando a caixa de correio está próxima do seu limite.
Proibição de Envio: Situação que impede o envio de novas mensagens.
Proibição de Envio e Recebimento: Situação que impede tanto o envio quanto o recebimento de novas mensagens.
GB = Gigabytes
MB = Megabytes

RETIFICAÇÃO
Na Portaria nº 184, de 12 de setembro de 2013, publicado no DODF nº 199, de 25 de setembro de 2013, página 38, ONDE SE LÊ: "... e de 30 de dezembro de 2013 a 16 de janeiro de 2014...", LEIA-SE: "...e de 16 de dezembro de 2013 a 30 de janeiro de 2014...".

SECRETARIA DE ESTADO DE CULTURA

ORDEM DE SERVIÇO Nº 219, DE 15 DE OUTUBRO DE 2013.
O SECRETÁRIO-ADJUNTO DE ESTADO DE CULTURA DO DISTRITO FEDERAL, no uso de suas atribuições regimentais, constantes do Decreto nº. 33.178, de 1º de setembro de 2011 e tendo em vista: a) o planejamento e a realização de pautas dos eventos artísticos e musicais programados na programação da SeCult/DF em cada exercício: b) a necessidade de disciplinar os procedimentos de concessão de férias regulamentares de servidores lotados e em exercício em algumas Unidades Administrativas da Secretaria de Estado de Cultura do Distrito Federal - SeCult/DF; Geral; e c) o contido na informação nº 216/2007-DLDD/SRH, de 04 de outubro de 2007, da então Secretaria de Planejamento e Gestão do Distrito Federal, Parecer nº 1254/2009 – PROPES – PGDF e dos autos do processo nº 150.000905/2007, resolve:
Art.1º Determinar que os servidores do Quadro de Pessoal lotados e em exercício na Unidade Artística da Orquestra Sinfônica do Teatro Nacional Claudio Santoro- UAOSTNCS/SeCult/DF; Teatro Nacional Claudio Santoro-TNCS/ SeCult/DF e na Gerência de Venda e Arrecadação-GVA, da Diretoria de Planejamento e Finanças-DPF, da Subsecretaria de Administração Geral-SUAG/