DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA EXECUTIVA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES

DIRETRIZES E NORMAS

Sumário

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES DA ADVOCACIA GERAL DA UNIÃO

1.1. ESCOPO

A Política de Segurança da Informação e das Comunicações (POSIC) tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito da Advocacia-Geral da União (AGU).

O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, na AGU.

Essa Política aplica-se a todos os membros, servidores e estagiários da AGU e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da AGU.

1.2. CONCEITOS E DEFINIÇÕES

Para os fins dessa Política, considera-se:

- ✓ **Acesso Lógico** – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
- ✓ **Acesso Remoto –** ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
- ✓ **Agente responsável:** Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
- ✓ **ADSL (Asymmetric Digital Subscriber Line) – (Linha Digital Assimétrica para Assinante)** tecnologia de transmissão que possibilita o transporte de voz e dados a alta velocidade através da rede telefônica convencional, analógica ou digital**;**
- ✓ **Ameaça –** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- ✓ **Análise/avaliação de riscos –** processo completo de análise e avaliação de riscos;
- ✓ **Ativo -** qualquer bem, tangível ou intangível, que tenha valor para a organização;

- ✓ **Ativo da Informação –** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

- ✓ **Ativo Sigiloso –** qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;

- ✓ **Auditoria –** verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

- ✓ **Autenticação –** é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

- ✓ **Autenticidade –** propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

- ✓ **Banco de Dados (ou Base de Dados) –** é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações.

- ✓ **Biometria –** uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão;

- ✓ **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

- ✓ **Bluetooth -** tecnologia de transmissão de dados via sinais de rádio de alta frequência, entre dispositivos eletrônicos próximos;

- ✓ **Classificação da informação -** atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

- ✓ **Confidencialidade –** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

- ✓ **Contingência -** descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

- ✓ **Controle de Acesso -** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

- ✓ **Cópia de Segurança (Backup) –** copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

- ✓ **Correio Eletrônico -** é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

- ✓ **Credenciais ou contas de acesso -** permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

- ✓ **Criptografia –** é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

- ✓ **CTEC –** Comitê de Tecnologia da Informação da AGU;

- ✓ **CTIR GOV -** Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.

- ✓ **Dado –** representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

- ✓ **DTI –** Departamento de Tecnologia da Informação da AGU;

- ✓ **Diretriz -** descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

- ✓ **Disponibilidade -** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

- ✓ **Download - (Baixar)** copiar arquivos de um servidor (site) na internet para um computador pessoal;

- ✓ **Espelhamento –** Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.

- ✓ **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)** - grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

- ✓ **FTP (File Transfer Protocol) – (Protocolo de Transferência de Arquivo)** é um protocolo da Internet para transferência de arquivos;

- ✓ **Gestão de Continuidade de Negócios -** Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

- ✓ **Gestão de Risco –** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

- ✓ **Gestão de Segurança da Informação e Comunicações -** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

- ✓ **Gestor da Informação -** pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

- ✓ **Gestor de Segurança da Informação e das Comunicações** – é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF;

- ✓ **Hardware –** É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

- ✓ **HTTP (Hyper Text Transfer Protocol) - (Protocolo de Transferência de Hipertexto)** é uma linguagem para troca de informação entre servidores e clientes da rede;

- ✓ **HTTPS (HyperText Transfer Protocol Secure) –** (**Protocolo de Transferência de Hipertexto Seguro)** é uma linguagem para troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;

- ✓ **Incidente de Segurança -** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

- ✓ **Informação -** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

- ✓ **Informações Críticas -** são as informações de extrema importância para a sobrevivência da instituição;

- ✓ **Informação sigilosa** - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

- ✓ **Instant Messenger – (Mensageiro instantâneo)** é uma aplicação que permite o envio e o recebimento de mensagens em tempo real;

- ✓ **Integridade –** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

- ✓ **Internet –** rede mundial de computadores;

- ✓ **Internet Protocol – (Protocolo de Internet)** é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

- ✓ **Intranet –** rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

- ✓ **Log -** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

- ✓ **Logon -** Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível**;**

- ✓ **On line –** (**Estar disponível ao vivo**) no contexto da Internet significa estar disponível para acesso imediato, em tempo real;

- ✓ **Perfil de acesso -** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

- ✓ **Plano de Contingência -** Descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;

- ✓ **Plano de Continuidade de Negócios -** documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

- ✓ **Peer-to-peer (P2P) – (Ponto a ponto)** permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

- ✓ **Política de Segurança da Informação e das Comunicações (POSIC) -** documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

- ✓ **Protocolo -** convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

- ✓ **Proxy -** é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a

Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;

- ✓ **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- ✓ **Recursos Computacionais -** recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;
- ✓ **Rede Corporativa -** conjunto de todas as redes locais sob a gestão da instituição;
- ✓ **Rede Pública –** rede de acesso a todos;
- ✓ **Replicação -** é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento;
- ✓ **Roteador –** equipamento responsável pela troca de informações entre redes;
- ✓ **Sala Cofre –** é uma sala fortificada que pode ser instalada em uma instituição, provendo um local seguro de invasões e outras ameaças. São ambientes projetados para resistir a vários tipos de catástrofes. Suportam, por exemplo, temperaturas de até 1.200 graus Celsius, inundações, cortes bruscos de energia, gases corrosivos, explosões e até ataques nucleares;
- ✓ **Sala Segura -** sala que proporciona um ambiente seguro no Datacenter, oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente;
- ✓ **Segurança da Informação e Comunicações:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- ✓ **Servidor de Rede -** recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
- ✓ **Servidor -** pessoa legalmente investida em cargo público;
- ✓ **Sistemas de Informação –** conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;
- ✓ **Sistema de Segurança da Informação -** proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta

segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

- ✓ **Software -** são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

- ✓ **Site -** Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

- ✓ **Streaming -** transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

- ✓ **Switches –** Um switch de rede é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;

- ✓ **Termo de Responsabilidade -** termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

- ✓ **Tratamento da informação -** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

- ✓ **Tratamento de Incidentes de Segurança em Redes Computacionais** - serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

- ✓ **Trilhas de Auditoria -** são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

- ✓ **Usuário -** servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;

- ✓ **VLAN (Virtual Local Area Network ou Virtual LAN) – (**Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;

- ✓ **VPN (Virtual Private Network) – (Rede Privada Virtual)** é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

- ✓ **Vulnerabilidade -** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

- ✓ **Wireless (rede sem fio)** - rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

1.3. REFERÊNCIAS LEGAIS E NORMATIVAS

- ✓ Lei 12527, de 18 de novembro de 2011 – Lei de acesso a informação

- ✓ Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

- ✓ Lei n° 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

- ✓ Lei nº 8.159, de 08 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e alterações legais;

- ✓ Lei 10.683 de 28 de maio de 2003 – Art. 6º, competência do Gabinete de Segurança Institucional da Presidência da República;

- ✓ Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

- ✓ Decreto nº 6.931, de 11 de agosto de 2009 - art. 8º do Anexo I – competência do Departamento de Segurança da Informação e Comunicações;

- ✓ 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;

- ✓ 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;

- ✓ Decreto 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

- ✓ Portaria 257, de 09 de junho de 2011, que institui o Comitê Gestor do Sítio Eletrônico da AGU;

- ✓ Instrução Normativa GSI Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;
- ✓ Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização;
- ✓ Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações.
- ✓ Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
- ✓ Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;
- ✓ Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;
- ✓ Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- ✓ Norma Complementar nº 07/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- ✓ Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;
- ✓ Norma Complementar nº 09/IN01/DSIC/GSIPR, Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta;
- ✓ Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- ✓ Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

- ✓ Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

- ✓ Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

- ✓ Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

- ✓ Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

- ✓ Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta;

- ✓ NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão da Segurança da Informação;

- ✓ NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação;

- ✓ NBR/ISO/IEC 27001/2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação;

- ✓ ISO/IEC Guide 73:2002 - Gestão de Riscos / Vocabulário - Recomendações para uso em normas;

- ✓ Norma NBR/ISO/IEC 27005:2008 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI);

- ✓ Código Civil, Art. 1.016, que institui que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;

- ✓ Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/;

1.4. PRINCÍPIOS

São princípios da POSIC:

1.4.1 A garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais; e

1.4.2 A proteção dos dados, informações e conhecimentos produzidos na AGU classificados como sigilosos.

1.5. DIRETRIZES GERAIS

São diretrizes gerais da POSIC:

1.5.1 A preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da AGU;

1.5.2 Continuidade das atividades;

1.5.3 Economicidade da proteção dos ativos de informação;

1.5.4 Pessoalidade e utilidade do acesso aos ativos de informação; e

1.5.5 A responsabilização do usuário pelos atos que comprometam a segurança do sistema da informação.

1.5.6 Organização da Segurança da Informação

1.5.6.1 A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, disponibilidade, conformidade e confidencialidade;

1.5.6.2 Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio (regular exercício das funções institucionais);

1.5.6.3 O gerenciamento dos ativos de informação deverão observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

1.5.6.4 O cumprimento dessa Política, bem como das normas complementares e procedimentos de Segurança da Informação na AGU será auditado periodicamente, de acordo com os critérios definidos pelo CTEC, vinculado diretamente ao Gabinete do Advogado-Geral da União;

1.5.6.5 As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido;

1.5.6.6 O acesso às informações sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

1.5.6.7 A aquisição, contratação de serviços de desenvolvimento, instalação e uso de sistemas e equipamentos devem ser homologados e/ou autorizados pela administração;

1.5.6.8 Para garantir o cumprimento das normas, os responsáveis pelas unidades deverão auxiliar no controle do uso dos recursos computacionais;

1.5.6.9 Os requisitos de segurança da informação devem estar explicitamente citados em todos os termos de compromisso celebrados entre o órgão e terceiros;

1.5.6.10 Todos os membros, servidores e estagiários da AGU e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da AGU e sejam usuários dos ativos sigilosos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos da AGU.

1.5.7 Segurança em Recursos Humanos

1.5.7.1 As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da AGU;

1.5.7.2 Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

1.5.7.3 O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

1.5.7.4 Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização faz se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

1.5.7.5 Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;

1.5.7.6 Todo ativo produzido pelo usuário, desligado, deverá ser mantido pela AGU garantindo o reconhecimento e o esclarecimento da propriedade do acervo para Instituição;

1.6. COMPETÊNCIAS E RESPONSABILIDADES

1.6.1 Essa Política, as normas complementares e os procedimentos de segurança se aplicam a todos os membros, servidores e estagiários da AGU e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da AGU.

1.6.2 Compete ao Gabinete do Advogado-Geral da União

1.6.2.1 Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização; e

1.6.2.2 Assegurar os recursos necessários para a implementação e gestão da POSIC da AGU.

1.6.3 Compete ao Comitê de Tecnologia da Informação da AGU

1.6.3.1 Definir critérios para auditoria periódica destinada a aferir o cumprimento da POSIC da AGU, suas Normas Complementares e Procedimentos.

1.6.3.2 Manifestar-se sobre a POSIC, com posterior encaminhamento ao Advogado-Geral da União, para aprovação.

1.6.3.3 Designar o Comitê de Segurança da Informação, o Gestor de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

1.6.4 Compete ao Comitê de Segurança da Informação e Comunicações da AGU

1.6.4.1 Assessorar na implementação das ações de segurança da informação e comunicações;

1.6.4.2 Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

1.6.4.3 Propor alterações na POSIC; e

1.6.4.4 Propor normas relativas à segurança da informação e comunicações.

1.6.5 Compete ao Gestor de Segurança da Informação e Comunicações da AGU

1.6.5.1 Promover cultura de segurança da informação e comunicações;

1.6.5.2 Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

1.6.5.3 Propor recursos necessários às ações de segurança da informação e comunicações;

1.6.5.4 Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

1.6.5.5 Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

1.6.5.6 Manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

1.6.5.7 Propor normas relativas à segurança da informação e comunicações.

1.6.5.8 Propor modificações à POSIC;

1.6.5.9 Definir estratégias para a implantação da POSIC;

1.6.5.10 Editar Normas Complementares e Procedimentos de Segurança da Informação e das Comunicações, cabendo ao CTEC a recomendação de alteração normativa;

1.6.5.11 Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

1.6.5.12 Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;

1.6.5.13 Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

1.6.5.14 Manter a análise de risco atualizada, refletindo o estado corrente da organização;

1.6.5.15 Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

1.6.5.16 Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

1.6.5.17 Produzir relatórios síntese de incidentes de segurança da informação para o CTEC;

1.6.5.18 Planejar, coordenar, supervisionar e orientar a execução das atividades da Equipe de Tratamento de Incidentes de Rede (ETIR).

1.7. NORMAS COMPLEMENTARES

1.7.1 O regimento da POSIC no âmbito da AGU está estruturado nas seguintes Normas Complementares que tratam especificamente da gestão dos recursos de tecnologia da informação, e que, portanto, devem ser expressamente cumpridas:

1.7.1.1 **NC 01 - Acesso Físico e Lógico -** Estabelecer controle de acesso físico e lógico dentro da AGU;

1.7.1.2 **NC 02** – **Acesso Remoto Externo –** Critério para disponibilização de acesso remoto à rede corporativa;

1.7.1.3 **NC 03 - Tratamento da Informação -** Requisitos e regras para Tratamento da informação no ambiente da AGU;

1.7.1.4 **NC 04 - Contas de Acesso e Senhas -** Trata especificamente da Norma de uso das contas e senhas utilizadas para obter acesso à rede de dados da AGU;

1.7.1.5 **NC 05 - Correio Eletrônico -** Trata especificamente da Norma de uso dos recursos de correio eletrônico (e-mail) da AGU;

1.7.1.6 **NC 06 - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da AGU -** Regulamentar o funcionamento da Equipe de Tratamento e Resposta a incidentes em Redes Computacionais;

1.7.1.7 **NC 07 - Recursos Computacionais -** Trata especificamente da Norma da operação e manuseio dos recursos de informática disponíveis na AGU;

1.7.1.8 **NC 08 - Utilização da Internet e Intranet -** Trata especificamente da Norma de uso dos recursos de Internet e Intranet através da rede de dados da AGU.

1.7.1.9 **NC 09 – Avaliação de Conformidade** – Trata da apresentação de um conjunto de recomendações em conformidade que devem ser aplicadas conforme o contexto e as necessidades da AGU.

1.7.2 As Normas Complementares devem ser divulgadas em boletim interno da instituição e disponíveis na Internet e Intranet para todos os usuários dos recursos de tecnologia da informação da AGU (membros, servidores e estagiários da AGU e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da AGU);

1.7.3 Em nenhuma hipótese será permitido o descumprimento das Normas Complementares pela alegação de desconhecimento das mesmas por parte do usuário.

1.8. PENALIDADES

1.8.1 O não cumprimento das determinações da POSIC sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos da AGU;

1.8.2 O descumprimento das disposições constantes nessa Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

1.8.3 O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente;

1.8.4 Os casos omissos e as dúvidas surgidas na aplicação dessa política serão submetidos ao CTEC.

1.9. ATUALIZAÇÃO

1.9.1 Essa POSIC deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

1.10. VIGÊNCIA

1.10.1 Esse documento entra em vigor na data de sua publicação.

1.11. DISPOSIÇÕES FINAIS

1.11.1 Os casos omissos e as dúvidas com relação a essa POSIC serão submetidos ao Comitê de Segurança da Informação e das Comunicações.

1.12. ANEXO I - NORMAS COMPLEMENTARES

1.12.1. NC 01 - ACESSO FÍSICO E LÓGICO

1.12.1.1 Campo de Aplicação

Esta norma se aplica no âmbito da AGU.

1.12.1.2 Objetivo

Estabelecer controle de acesso físico dentro do Departamento de Tecnologia da Informação (DTI) e lógico no ambiente computacional da AGU.

1.12.1.3 Diretrizes Gerais

a) Acesso Físico

I. Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e suprimentos do DTI e à proteção dos recursos computacionais, permitido apenas às pessoas autorizadas;

II. Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado. No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los;

III. Todo o pessoal envolvido em trabalhos de apoio, tais como a manutenção das instalações físicas, deve ser orientado e capacitado para manter a adoção de medidas de proteção ao acesso;

IV. Todas as pessoas devem portar algum tipo de identificação visível que informe se é um servidor ou não, bem como o nível de autorização de acesso;

V. O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso destes às áreas de armazenamento ou processamento de informações sensíveis, salvo acompanhados e com autorização do responsável;

b) Acesso Lógico

I. Os controles de acesso lógico são um conjunto de procedimentos, recursos e meios utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes

corporativas, aplicações e sistemas de informação;

II. Os trechos que abrigam meios de comunicação devem ser protegidos para evitar a interceptação e/ou interferência de dados;

III. Os computadores e sistemas da AGU devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

IV. Os sistemas devem ser avaliados com relação aos aspectos de segurança antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas;

V. O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

VI. O Suporte Técnico da AGU poderá ter permissão de acesso remoto às estações de trabalho dos usuários de sua unidade quando necessário.

1.12.2. NC 02 - ACESSO REMOTO EXTERNO

1.12.2.1 Campo de Aplicação

Esta norma se aplica no âmbito da AGU.

1.12.2.2 Objetivo

Estabelecer critérios para a disponibilização do serviço de acesso remoto externo à rede da AGU, bem como as regras para a sua utilização, visando à prevenção do acesso não autorizado às informações da AGU.

1.12.2.3 Diretrizes Gerais

a) O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da AGU e que necessitam deste serviço para execução de suas atividades institucionais, desde que autorizados;

b) Os administradores da rede da AGU lotados no DTI, para o desempenho de suas atribuições, poderão ter permissão de acesso remoto a todos os recursos computacionais da AGU quando necessário;

c) Os Representantes de Informática, quando administradores de rede das unidades da AGU, poderão ter permissão de acesso aos servidores de rede e estações de trabalho de sua circunscrição quando necessário;

d) A liberação de acesso remoto, só será efetivada após avaliação e aprovação pelo DTI, para que se evitem ameaças à integridade e sigilo das informações contidas na rede AGU. Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança da rede da AGU;

e) A solicitação do acesso remoto deve conter, no mínimo, as seguintes informações:

I. Data da solicitação;

II. Tipo de solicitação;

III. Tempo de validade do acesso remoto;

IV. Justificativa;

V. Dados do solicitante;

VI. Dados do usuário.

f) A disponibilização de acesso remoto à rede da AGU para outras organizações deve obedecer às seguintes regras:

I. Direitos de acesso definidos por contrato formal entre as partes;

II. Acesso temporário e limitado às necessidades de negócio;

III. Revisão periódica dos direitos de acesso;

IV. Utilização de solução que permita a implementação e controle de regras de acesso.

g) O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

I. Finalização do período especificado na solicitação ou contrato;

II. Perda da necessidade de utilização do serviço;

III. Transferência do usuário para outras unidades;

IV. Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

h) As conexões remotas à rede da AGU devem ocorrer da seguinte maneira:

I. Utilização de autenticação;

II. As senhas e as informações que trafegam entre a estação remota e a rede da AGU devem estar criptografadas;

i) Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não fornecê-lo a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas;

j) É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.

1.12.3. NC 03 - TRATAMENTO DA INFORMAÇÃO

1.12.3.1 Campo de Aplicação

Essa norma se aplica no âmbito da AGU.

1.12.3.2 Objetivo

Definir os requisitos e regras para classificação e tratamento da informação no ambiente de tecnologia da AGU.

1.12.3.3 Diretrizes Gerais

a) A informação utilizada pela AGU é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, autenticidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado;

b) Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação dessa Norma;

c) O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece através da identificação e autenticação do usuário;

d) O ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não devem ser utilizado para testes. Os testes devem ser feitos em ambiente apropriado e gerenciado;

e) A passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse ambiente para sua execução;

f) Todos os procedimentos que possibilitam a proteção da informação e a continuidade de seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos;

g) Devem ser estabelecidos critérios para deleções segura de informações armazenadas em estações de trabalho e/ou outros dispositivos de armazenamento, como formatação de máquinas ou desmagnetização de discos, quando o equipamento for transferido para outro usuário ou descartado pela AGU para algum outro destino.

h) O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação;

i) O Gestor da Informação classificará o nível de confidencialidade e proteção da informação conforme Decretos Nºs 4553 de 27/12/2002 e 7.724 de 16/05/2012;

j) A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento;

k) Toda informação crítica para o funcionamento da AGU deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada. O Gestor da Informação é responsável pela definição dessa criticidade.

1.12.4. NC 04 - CONTAS DE ACESSO E SENHAS

1.12.4.1 Campo de Aplicação

Esta norma se aplica no âmbito da AGU.

1.12.4.2 Objetivo

Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação da AGU, assim como estabelecer critérios relativos às senhas das respectivas contas.

1.12.4.3 Diretrizes Gerais

a) Criação de Contas de Acesso

I. Todo cadastramento de conta de acesso à rede da AGU deve ser efetuado mediante solicitação formal;

II. Contas de acesso de terceirizados da AGU devem ter prazo de validade no máximo igual ao período de vigência do contrato ou período de duração de suas atividades;

III. As solicitações relativas à criação de cada conta devem ser mantidas registradas e armazenadas de forma segura pelo DTI;

IV. Todos os usuários devem assinar um termo de responsabilidade pela utilização da conta de acesso. Este termo deve ser entregue junto com a solicitação de criação de conta de acesso;

V. A nomenclatura das contas de acesso de usuários deve seguir padrão definido pelo DTI;

VI. A chefia imediata da área a qual pertence o usuário deve ser informada formalmente, pelo DTI, a respeito de qualquer evento relacionado a falhas de segurança referentes à conta do usuário e senha;

VII. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada ao DTI.

b) Exclusão e Bloqueio de Contas de Acesso

I. Toda exclusão ou bloqueio de conta de acesso à rede da AGU deve ser

efetuado mediante solicitação formal;

II. A exclusão da conta de acesso do usuário deve ser solicitada caso haja:

   i. Falecimento;

   ii. Aposentadoria; e

   iii. Outros afastamentos que caracterizem encerramento do vínculo com a instituição;

III. Contas sem utilização por mais de 45 (quarenta e cinco) dias serão bloqueadas;

IV. As contas deverão permanecer bloqueadas até que haja nova solicitação formal para desbloqueio;

V. As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de logon/acesso;

VI. As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.

c) Senhas

I. Todas as senhas, de usuários comuns, para autenticação na rede da AGU devem seguir os seguintes critérios mínimos:

   i. Toda senha deve ser constituída de, no mínimo, 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letras e números);

   ii. A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "1221jose" ou "1212silv";

   iii. A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;

   iv. É obrigatória a troca de senha ao efetuar o primeiro logon;

   v. É proibida a repetição das 5 últimas senhas já utilizadas;

II. Todas as senhas, de administradores locais e administradores de domínio, para autenticação na rede da AGU devem seguir os seguintes critérios mínimos:

i. Toda senha deve ser constituída de, no mínimo, 10 caracteres sendo obrigatório o uso de caracteres alfanuméricos (com letras maiúsculas e minúsculas) e caracteres especiais;

ii. A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário chama-se Jose da Silva, sua senha não pode conter partes do nome como "12$@joseSI" ou "12$@JOsilv";

iii. A data de expiração da senha deve ser de no máximo 45 dias, caso não seja alterada, esta será bloqueada;

iv. É obrigatória a troca de senha ao efetuar o primeiro logon;

v. É proibida a repetição das 10 últimas senhas já utilizadas;

III. Os critérios definidos acima serão auditados pelo DTI, por meio de ferramentas adequadas;

IV. A base de dados de senhas deve ser armazenada com criptografia;

V. O usuário poderá solicitar alteração de sua senha, caso não se recorde da mesma, mediante solicitação formal;

d) Utilização de Contas de Acesso e Senhas

I. A conta de acesso é o instrumento para identificação do usuário na rede AGU e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese;

II. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas;

III. A Coordenação-Geral de Pessoas (CGEP) da AGU deve comunicar ao DTI, no prazo de dois dias úteis, os desligamentos, as aposentadorias, os afastamentos e as movimentações de usuários que impliquem mudanças de lotação;

IV. O acesso aos serviços de tecnologia de informação da AGU deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da AGU.

V. Para fins de auditoria, as contas de administradores locais das estações de trabalho ou de servidores de rede só devem ser utilizadas quando estritamente necessário.

1.12.5. NC 05 - CORREIO ELETRÔNICO

1.12.5.1 Campo de Aplicação

Esta Norma se aplica no âmbito da AGU.

1.12.5.2 Objetivo

A disponibilização do serviço de correio eletrônico corporativo da AGU - AGU aos usuários.

1.12.5.3 Diretrizes Gerais

a) O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais da AGU;

b) São usuários do serviço de correio eletrônico corporativo os membros e servidores da AGU, seus órgãos e unidades, os estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional da AGU;

c) A concessão de contas de correio eletrônico depende de pedido fundamentado da autoridade responsável pela respectiva área, demonstrando a necessidade, para a Instituição, da utilização do serviço pelo agente;

d) Os titulares de órgão ou unidade da AGU podem solicitar a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação;

e) Cada unidade da AGU manterá no mínimo uma conta de correio eletrônico, destinada a comunicações institucionais;

f) É vedado o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

g) O acesso indevido às informações tramitadas por meio do serviço de correio eletrônico corporativo da AGU, ou contidas em seus ambientes, será punido na forma da lei;

h) O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

i) É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I. Praticar crimes e infrações de qualquer natureza;

II. Executar ações nocivas contra outros recursos computacionais da AGU ou de redes externas;

III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da AGU;

V. Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

VI. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela AGU;

VII. Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

VIII. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

j) Compete ao DTI disponibilizar o serviço de correio eletrônico corporativo, diretamente ou mediante contrato, competindo-lhe, ainda, o seguinte:

I. Zelar pelo atendimento aos princípios da segurança, integridade, sigilo e disponibilidade dos serviços e dados transmitidos por meio do sistema de correio eletrônico;

II. Prover meios tecnológicos necessários à adequada utilização do serviço;

III. Definir os padrões e requisitos para cadastramento, concessão, utilização, suspensão ou exclusão das contas de correio eletrônico e listas de distribuição, definidas por essa Norma;

IV. Manter, em local seguro e restrito, dados de auditoria acerca da utilização do serviço, no sentido de garantir a recuperação de mensagens em caso de danos ao ambiente de rede, devidamente comunicado a todos os usuários do serviço;

V. Suspender motivadamente o acesso a conta de correio quando constatado o uso indevido dos recursos, dando imediata ciência ao respectivo titular e ao responsável pela apuração formal;

VI. Manter proteção contra vírus e mensagens não solicitadas (spam) nos servidores do correio eletrônico;

VII. Restringir a transmissão de arquivos que, em tese, possam significar comprometimento do serviço;

VIII. Monitorar o uso do ambiente virtual, por meio de ferramentas sistêmicas, a fim

de preservar a integridade das informações e identificar possíveis violações ao disposto nessa Norma;

IX. Providenciar, sempre que necessária, a capacitação dos usuários no uso da ferramenta de correio eletrônico;

k) Cabe à SGA/CGEP (Coordenação de Gestão de Pessoas) informar ao DTI, em até dois dias úteis, as ocorrências de afastamentos ou desligamentos de usuários do serviço, que importem a necessidade de suspensão ou exclusão de contas de correio eletrônico.

1.12.6. NC 06 - EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS DA AGU

1.12.6.1 Campo de Aplicação

Esta norma se aplica no âmbito da AGU.

1.12.6.2 Objetivo

Regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes computacionais (ETIR), no âmbito da AGU, e ainda estabelecer diretrizes, critérios e procedimentos acerca do tratamento de incidentes na Rede da AGU

1.12.6.3 Diretrizes Gerais

a) Modelo de Implementação

I. O modelo de implementação a ser utilizado, inicialmente, pela ETIR será o modelo Centralizado. Neste modelo existirá uma ETIR central composta por servidores públicos ou militares com dedicação exclusiva às atividades de tratamento e resposta aos incidentes no ambiente computacional da AGU;

II. O Gestor de Segurança da Informação e das Comunicações será responsável por criar as estratégias, gerenciar as atividades e executar as tarefas, além de ser o responsável, perante a Advocacia Geral da União pela comunicação com o CTIR GOV;

III. A atuação da ETIR se dará por ações reativas e proativas;

IV. As ações reativas incluem recebimento de notificações de incidentes, orientação no reparo a danos, e analise de sistemas comprometidos buscando causas, danos e responsáveis;

b) Estrutura Organizacional

I. Deverá ser criada ETIR, unidade organizacional diretamente subordinada ao DTI, com no mínimo 2 (dois) integrantes, com a competência de coordenar as atividades de tratamento e resposta a incidentes em redes computacionais em conformidade com a POSIC;

II. A ETIR terá como competências:

i. Coordenar, executar e acompanhar as atividades de tratamento e resposta a incidentes na rede corporativa da AGU;

ii. Coordenar, executar e acompanhar a análise dos sistemas comprometidos buscando, causas, danos e responsáveis;

iii. Gerenciar contratos de prestação de serviços específicos, controlando a qualidade dos resultados de acordo com os critérios de aceitação do produto e dos serviços prestados;

iv. Coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa da AGU;

v. Coordenar, executar e acompanhar a análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes na AGU;

vi. Assistir o CTIR GOV com as informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal;

vii. Desenvolver um Plano de Conscientização em segurança da informação e comunicações afim de que todos os servidores da AGU tenham ciência do assunto;

viii. Participar na proposição de recursos necessários às ações de segurança da informação e comunicações;

ix. Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes da rede corporativa da AGU;

x. Participar da definição e acompanhar os indicadores de incidentes na rede corporativa da AGU;

xi. Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicações;

xii. Participar na proposição de recursos necessários às ações de segurança da informação e comunicações; e

xiii. Executar outras atividades correlatas que lhe forem demandadas.

c) Tratamento de Incidentes

I. Todo e qualquer servidor deve estar ciente que o tratamento de incidentes visa minimizar os impactos de um incidente nos processos em curso na AGU, sendo assim voltado à redução e contenção dos efeitos causados por eventos técnicos indesejáveis e seu monitoramento;

II. Quaisquer falhas, anomalias, ameaças ou vulnerabilidades observadas devem ser notificadas o mais rápido possível através do e-mail: abuse@agu.gov.br ;

III. A ETIR deverá propor regras para ações disciplinatórias no caso de condutas que violem as políticas estabelecidas ou que comprometam a segurança das informações da organização;

IV. Cabe a ETIR obter informações quantitativas acerca dos incidentes ocorridos que descrevam: sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes. Tais informações servem como indicadores da eficácia das políticas e da relação custo-benefício dos controles de segurança;

V. Após o levantamento dos dados do incidente a ETIR deverá tratá-lo e documentá-lo, visando manter um histórico dos incidentes e ainda uma cultura acerca dos mesmos;

VI. Caso o incidente tenha como origem outro órgão da Administração Pública Federal ou outro país, o CTIR GOV deverá ser acionado para juntamente a ETIR, tratar o incidente.

1.12.7. NC 07 - RECURSOS COMPUTACIONAIS

1.12.7.1 Campo de Aplicação

Esta norma se aplica no âmbito da AGU.

1.12.7.2 Objetivo

Estabelecer critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da rede AGU, assim como o controle, administração e requisitos mínimos desses recursos.

1.12.7.3 Diretrizes Gerais

a) Recursos Computacionais em Geral

I. Os usuários devem ter acesso unicamente àqueles recursos computacionais que forem indispensáveis à realização de suas atividades na AGU;

II. A utilização dos recursos de tecnologia, com finalidade pessoal, é permitida, desde que seja em um nível mínimo e que não viole a Política, as Normas Complementares e o Código de Ética da Instituição;

III. Os usuários são responsáveis pelos recursos computacionais por eles utilizados, devendo preservar a sua integridade e continuidade;

IV. Os ambientes onde se encontram instalados ou guardados os recursos computacionais devem permanecer protegidos mesmo na ausência dos usuários;

V. É vedado aos usuários da AGU utilizar a identificação e/ou senha de outro usuário para acessar ou utilizar um recurso computacional;

VI. É vedado aos usuários fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um Recurso Computacional;

VII. Os usuários que estiverem em trânsito por outras unidades da AGU poderão utilizar os recursos computacionais das unidades em que estiverem trabalhando;

VIII. Todos os equipamentos (estações de trabalho, notebooks, servidores, impressoras e outros) devem ter identificação padrão especificados pelo DTI.

IX. O usuário de equipamento de propriedade da AGU deve assinar termo de responsabilidade;

X. Tendo em vista a preservação do ambiente computacional da AGU, é vedado aos usuários o fornecimento de informações a terceiros sobre características, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis, ressalvada a possibilidade de disposição de tais informações pelo DTI, quando o desempenho de atividades institucionais assim exigir.

b) Estações de Trabalho

I. Estações de trabalho somente devem ser utilizadas para execução de atividades de interesse da AGU;

II. O usuário deve zelar pela conservação dos equipamentos de informática sob sua responsabilidade, não podendo fumar ou alimentar-se próximo a eles.

III. É vedado ao usuário abrir as estações de trabalho ou modificar a configuração do hardware;

IV. O usuário, sempre que se ausentar da estação de trabalho deve bloqueá-la para impedir o acesso não autorizado;

V. O usuário deve informar imediatamente ao DTI, quando identificada violação da integridade do equipamento por ele utilizado;

VI. A configuração do ambiente operacional da estação de trabalho somente poderá ser alterada por técnico autorizado pelo DTI;

VII. O usuário deve ligar/desligar de forma adequada e segura o equipamento;

VIII. As atualizações ocorrerão automaticamente mediante procedimentos realizados pelo DTI;

IX. Caso o usuário identifique a necessidade de alguma atualização deverá comunicar ao DTI;

X. Todas as estações de trabalho deverão possuir o programa de antivírus homologado pelo DTI;

XI. O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;

XII. O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho;

XIII. O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho;

XIV. Não é permitida a conexão de estações de trabalho particulares, portáteis ou não, à rede da AGU, exceto em casos de comprovada necessidade, situações nas quais deverá ser assegurada a devida adoção de padrões de segurança compatíveis com o disposto nessa norma, devendo a estação de trabalho ser

objeto de verificação de conformidade pelo DTI;

XV. Arquivos salvos na unidade de disco local não terão garantia de recuperação.

XVI. As credenciais de administrador do equipamento deverão ficar sob a guarda e responsabilidade do DTI, restando ao usuário, ao qual se destina o equipamento, utilizá-lo mediante credenciais de "usuário comum". Ressalva-se o caso de usuários da área técnica, devidamente autorizados, pelo DTI, que por força de suas funções e conhecimento técnico, se reservam ao direito de efetuar suas próprias instalações, bem como, a guarda e o uso oportuno das credenciais de administrador;

XVII. O compartilhamento de diretórios e arquivos em estações de trabalho somente deve ser realizado quando estritamente necessário para execução das atividades do usuário mediante solicitação formal ao DTI, devidamente justificada.

c) Equipamentos Portáteis

I. Os equipamentos portáteis devem respeitar as mesmas regras estabelecidas para estações de trabalho;

II. Equipamentos portáteis de propriedade da AGU devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade;

III. O usuário, ao solicitar o empréstimo de equipamentos portáteis da AGU, deve assinar o Termo de Responsabilidade;

IV. Somente técnicos autorizados pelo DTI devem configurar os equipamentos portáteis para acesso à rede da AGU;

V. O usuário deve evitar armazenar informações confidenciais em equipamentos portáteis da AGU.

d) Servidores

I. Todo equipamento servidor de rede deve estar instalado em salas apropriadas e construídas para este fim;

II. Somente os técnicos autorizados do DTI deverão ter acesso aos servidores;

III. O usuário somente terá acesso ao servidor de rede se atender aos seguintes requisitos:

i. Solicitação formal ao DTI com a justificativa e finalidade do acesso pretendido;

ii. Avaliação e aprovação do DTI;

IV. Todos os servidores de rede devem utilizar os sistemas operacionais atualizados;

V. A atualização dos servidores de rede deverá ser realizada pelos técnicos autorizados do DTI;

VI. O controle de acesso aos servidores de rede deverá ser realizado por técnicos autorizados pelo DTI.

e) Servidores de Arquivo

I. Nos servidores de arquivos locais devem ser gravados:

   a. Documentos relacionados ao trabalho cotidiano e à produção jurídica e administrativa local, que demande compartilhamento ou resguardo institucional;

   b. Pastas particulares de correio eletrônico, exclusivamente das contas corporativas da unidade.

II. As permissões de acesso deverão ser concedidas em nível de grupos;

III. Só será permitido o acesso a qualquer pasta ou arquivo no servidor mediante solicitação formal, pelo responsável do setor;

IV. É proibida a exposição de material de natureza pornográfica e racista, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;

V. Não é permitido criar ou remover arquivos fora da área alocada ao usuário ou que venham a comprometer o desempenho e funcionamento dos sistemas;

VI. É vedada a gravação de dados e informações de natureza particular;

VII. É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas para garantir o backup dos mesmos;

VIII. Deverão ser gravados no servidor apenas documentos de interesse da instituição;

IX. Documentos de interesse dos departamentos deverão ser criados ou compartilhados na estrutura departamental;

X. Identificada ocorrência em desacordo com o disposto nos artigos antecedentes, o DTI poderá, após notificar o responsável e resguardar as evidências necessárias, excluir ou isolar arquivos, revogar acessos ou requisitar o equipamento, relatando o fato imediatamente à autoridade responsável pela apuração da infração;

XI. O compartilhamento deve ser restrito aos diretórios necessários, nunca compartilhando o diretório raiz.

f) Ativos de Rede

I. As portas dos switches somente devem estar ativas se utilizadas e inventariadas;

II. Os switches e access points devem possuir controle de acesso;

III. Todo roteador utilizado na rede da AGU deve prover, no mínimo, o uso de ACLs (Access lists) e o filtro de pacotes;

IV. Todo ativo de rede deve estar em local seguro. Os switches departamentais devem estar instalados em racks devidamente fechados e seguros;

V. Os ativos de rede só podem ser instalados na rede da AGU após a sua adequação aos padrões de segurança definidos pelo DTI;

VI. Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado;

VII. As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos técnicos autorizados pelo DTI;

VIII. Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta;

IX. Profissionais técnicos no exercício de suas funções, não devem utilizar a rede de dados da AGU para testes, devendo para isto a AGU, prover segmento de rede independente;

X. À AGU reserva o direito de realizar investigações em qualquer dos equipamentos que integrem a sua rede local.

g) Rede Sem Fio

I. A utilização da rede sem fio para acesso à rede da AGU somente será efetuada com autenticação utilizando mecanismos de protocolo seguro;

II. Qualquer equipamento que utilize a rede sem fio da AGU deve respeitar as regras estabelecidas para Estações de Trabalho e Notebooks, inclusive, quando justificados, os equipamentos particulares;

III. Somente os técnicos autorizados do DTI devem estabelecer os procedimentos e configurações de segurança de rede sem fio;

IV. O DTI deve verificar a adequação das Estações de Trabalho e instruir os

usuários sobre os procedimentos para acesso à rede sem fio de acordo com os requisitos estabelecidos.

h) Impressoras

I. Somente os usuários previamente autorizados poderão ter acesso aos recursos de impressão;

II. A configuração da impressora na estação de trabalho do usuário somente deverá ser realizada pelos técnicos autorizados pelo DTI;

III. Os usuários não devem deixar informações críticas, sigilosas ou sensíveis da instituição em equipamentos de impressão, de tal forma que pessoas não autorizadas possam obter acesso a elas.

i) Utilização de Software

I. Na AGU, só será permitida a utilização de softwares homologados pelo DTI, respeitando os direitos autorais e contratuais dos fabricantes, e que sejam necessários para a execução das atividades dos usuários;

II. O registro dos softwares homologados, do número de licenças disponíveis e dos softwares instalados nas estações de trabalho deve ser mantido atualizado pelo DTI;

III. Perante a necessidade de utilização de software não homologado, a chefia imediata deverá solicitar formalmente ao DTI a homologação do mesmo contendo os seguintes itens:

   i. Especificações detalhadas do software solicitado;

   ii. Quantidade de licenças;

   iii. Suporte ao software (necessidade de suporte);

   iv. Justificativa.

IV. Compete ao Comitê de Tecnologia da Informação – CTEC deliberar sobre a aquisição de licenças e a distribuição nos diversos órgãos da AGU, de acordo com proposta apresentada pelo DTI;

V. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação da AGU e o suporte para o mesmo;

VI. A instalação e a utilização de software estão sujeitas ao cumprimento dos seguintes requisitos:

   i. Quantidades de licenças de uso adquiridos;

ii. Conformidade com a área de atuação do setor interessado;

iii. Compatibilidade com os softwares utilizados;

iv. Desempenho do ambiente computacional; e

v. Impacto entre a necessidade de instalação e a demanda de outros setores.

VII. É vedado:

i. Efetuar réplicas dos softwares adquiridos pela AGU, bem como promover esta prática com outros programas; e

ii. Utilizar softwares que, por algum motivo, descaracterizem os propósitos da instituição ou danifique de alguma forma o ambiente instalado, tais como jogos eletrônicos e outros.

VIII. A instalação de software de outras categorias, tais como freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida ao DTI;

IX. O DTI poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma;

X. Os usuários com credenciais de administrador somente poderão instalar softwares, necessários ao desempenho de suas atribuições excepcionais, mediante prévia e indispensável autorização do DTI.

j) Manutenção e Configuração

I. Toda solicitação de atendimento para instalação, suporte e configuração dos recursos computacionais deve ser efetuada mediante solicitação formal ao DTI;

II. A equipe de atendimento deve estar devidamente identificada para a execução dos serviços de suporte técnico;

III. Nas dependências físicas da AGU somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da instituição ou cedidos formalmente, sendo proibida a assistência técnica em equipamentos particulares;

IV. O usuário deve acompanhar o técnico durante a manutenção da sua estação de trabalho;

V. Todo equipamento que tiver a necessidade de ser deslocado para manutenção ou configuração, deverá estar devidamente identificado e embalado;

VI. O usuário deve estar ciente da saída do equipamento de seu local de trabalho caso seja necessária a retirada do mesmo para manutenção;

VII. Todo recurso computacional que sair das dependências físicas da AGU por motivo de manutenção deverá ser registrado pelo responsável da unidade e deverá ter suas informações institucionais críticas previamente excluídas;

VIII. A saída do equipamento deverá ser autorizada pelo DTI;

IX. O usuário deve manter o número, do registro do chamado ou número do documento de solicitação formal, do pedido de suporte por ele realizado para controle e acompanhamento do respectivo chamado.

k) Controle e Administração de Recursos Computacionais

I. Todo recurso computacional deve ser identificado e inventariado;

II. Os recursos computacionais que não são de propriedade da AGU devem ser devidamente identificados;

III. O DTI deve garantir a qualidade e disponibilidade dos serviços, identificando e informando a necessidade de aquisição de novos recursos de informática;

IV. Novas implementações, alterações e atualizações de recursos computacionais devem ser homologadas antecipadamente pelo DTI;

V. Os recursos computacionais devem ser monitorados e administrados pelo DTI;

l) Inclusão de Equipamentos na Rede

I. Não é permitida a conexão de dispositivos não autorizados na rede local, principalmente, equipamentos de rede sem fio ou qualquer outra solução que estabeleça conexão simultânea com a rede de dados da AGU e outras redes. Em casos justificados para o uso destes equipamentos, a AGU deve prover segmento de rede independente, de forma a permitir o compartilhamento de sua infraestrutura de TI sem o comprometimento do desempenho e da segurança da rede local;

VI. A instalação de novas redes no domínio da AGU deverá ter links próprios. Para tanto, a AGU deverá prover ambiente de segmentação de redes por VLANs de forma a permitir o compartilhamento de sua infraestrutura de TI sem o comprometimento do desempenho e da segurança.

1.12.8. NC 08 – UTILIZAÇÃO DA INTERNET E INTRANET

1.12.8.1 Campo de Aplicação

Esta norma se aplica no âmbito da AGU.

1.12.8.2 Objetivo

Estabelecer critérios para administração e utilização de acesso aos serviços de Internet e Intranet no âmbito da AGU.

1.12.8.3 Diretrizes Gerais

a) Internet

I. São usuários da Internet da AGU os membros, servidores, estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional da AGU;

II. O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

III. As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pelo DTI;

IV. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

V. Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada;

VI. É vedado o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente da AGU;

VII. O DTI deverá prover o serviço de conexão à Internet implementando mecanismos de segurança adequados;

VIII. O DTI deverá estabelecer níveis de acesso à Internet;

IX. Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pelo DTI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede da AGU;

X. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:

a. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;

b. Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da AGU;

c. Uso de IM (Instant Messenger) não homologado ou autorizado;

d. Uso recreativo da internet em horário de expediente;

e. Uso de proxy anônimo;

f. Acesso a salas de bate-papo (chats), exceto aqueles definidos como ferramenta de trabalho homologada pelo DTI;

g. Acesso a rádio e TV em tempo real, exceto os canais corporativos como, por exemplo, a TV Escola;

h. Acesso a jogos;

i. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;

j. Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;

k. Envio a destino externo de qualquer software licenciado à AGU ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;

l. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas da AGU;

m. Utilização de softwares de compartilhamento de conteúdos na modalidade peer-to-peer (P2P);

n. Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação da AGU, na forma definida pelo DTI.

XI. O usuário poderá solicitar liberação de determinada página, com a devida justificada, mediante solicitação formal ao DTI;

XII. Somente serão liberadas as páginas analisadas e autorizadas pelo DTI;

XIII. A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato ao DTI;

XIV. Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pelo DTI, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

b) Intranet

I. São usuários da Intranet da AGU os membros, servidores, estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional da AGU;

II. A Intranet deverá ser utilizada como mecanismo de divulgação de notícias e disponibilização de serviços de caráter institucional;

III. O acesso à Intranet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

IV. O acesso aos serviços de Intranet deve ser realizado mediante autenticação da conta do usuário, sendo que todos os acessos realizados serão auditados, constituindo um histórico de acessos, podendo ser consultado ou publicado a critério da instituição;

V. As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pelo Chefe da unidade;

VI. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

VII. Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada;

VIII. É vedado o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente da AGU;

IX. As aplicações a serem disponibilizadas na Intranet devem ser previamente analisadas, homologadas e aprovadas pelo DTI;

X. As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual através de logon / acesso.

XI. As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos. As variáveis necessárias para acesso e administração

devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva.

c) Navegação e Administração

I. Os navegadores de Internet e Intranet utilizados no âmbito da AGU deverão ser homologados pelo DTI;

II. As paralisações dos serviços de Internet e Intranet, para manutenção preventiva, devem ser previamente comunicadas pelo DTI a todos os usuários;

III. No caso de indisponibilidade repentina dos serviços de Internet ou Intranet por alguma falha, a paralisação deve ser comunicada pelo DTI;

IV. Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados ao DTI para que sejam solucionados.

1.12.9. NC 09 - AVALIAÇÃO DE CONFORMIDADE

1.12.9.1 CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito da Advocacia-Geral da União.

1.12.9.2 OBJETIVO

Apresentar um conjunto de recomendações em conformidade que devem ser aplicadas conforme o contexto e as necessidades da AGU.

1.12.9.3 DIRETRIZES GERAIS

a) A AGU está inserida em um contexto de regulamentos derivados de leis, contratos e acordos que deve respeitar e observar, para que não seja alvo de ações e também para que possa proteger-se contra terceiros. As políticas e procedimentos adotados devem refletir esses requisitos, atuando na prevenção de tais eventos;

b) Devem ser levantados os aspectos legais de segurança aos quais as atividades da AGU estão submetidas de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão;

c) Ameaças e riscos devem ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida. Tanto no surgimento de novas ameaças ou na extinção de outras, as políticas são atualizadas para refletir a realidade presente;

d) A avaliação de conformidade em SIC deve ser contínua e aplicada visando contribuir com a Gestão de Segurança da Informação;

e) As não-conformidades relativas ao descumprimento de legislações, normas e procedimentos serão consideradas riscos de SIC e devem ser tratadas;

f) Os responsáveis pela verificação de conformidade devem considerar os requisitos mínimos que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações, observando, dentre outros, as legislações vigentes a respeito de SIC para a Administração Pública Federal e normativos internos do órgão;

g) O Gestor de Segurança da Informação e das Comunicações deve estabelecer responsabilidades para o monitoramento e avaliação quanto a real adoção das políticas pelos indivíduos que o compõem;

h) Material obtido da Internet; material proveniente de artigos, livros e demais fontes em papel ou mídia eletrônica; ou de outras fontes públicas devem ser verificados quanto à existência de restrições legais para seu uso e reprodução;

i) O DTI deve adotar mecanismos para garantir o uso de licenças de software no limite estabelecido nos contratos de aquisição e utilização.