

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

O MINISTRO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL, no uso de suas atribuições;

CONSIDERANDO:

o disposto no artigo 6º e parágrafo único do art. 16 da Lei nº 10.683, de 28 de maio de 2003;

o disposto no inciso IV do *caput* e inciso III do §1º do art. 1º e art. 8º do Anexo I do Decreto nº 5.772, de 08 de maio de 2006;

o disposto nos incisos I, VI, VII e XIII do artigo 4º do Decreto nº 3.505, de 13 de junho de 2000;

as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos;

o interesse do cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

o dever do Estado de proteção das informações pessoais dos cidadãos;

a necessidade de incrementar a segurança das redes e bancos de dados governamentais; e

a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

RESOLVE:

Art. 1º Aprovar orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

Art. 2º Para fins desta Instrução Normativa, entende-se por:

I - Política de Segurança da Informação e Comunicações: 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;

II - Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI - 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;

VII - Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

VIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IX - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Art. 3º Ao Gabinete de Segurança Institucional da Presidência da República - GSI, por intermédio do Departamento de Segurança da Informação e Comunicações - DSIC, compete:

I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;

II - estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;

IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;

V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

VI - receber e consolidar os resultados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

VII - propor programa orçamentário específico para as ações de segurança da informação e comunicações.

Art. 4º Ao Comitê Gestor de Segurança da Informação compete:

I - assessorar o GSI no aperfeiçoamento da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta;

II - instituir grupos de trabalho para tratar de temas específicos relacionados à segurança da informação e comunicações.

Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de segurança da informação e comunicações; II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;

VIII - remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações para o GSI.

Parágrafo único. Para fins do disposto no *caput*, deverá ser observado o disposto no inciso II do art. 3º desta Instrução Normativa.

Art. 6º Ao Comitê de Segurança da Informação e Comunicações, de que trata o inciso VI do art. 5º, em seu âmbito de atuação, compete:

I - assessorar na implementação das ações de segurança da informação e comunicações;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; III - propor alterações na Política de Segurança da Informação e Comunicações; e

IV - propor normas relativas à segurança da informação e comunicações.

Art. 7º Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

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

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

VII - propor normas relativas à segurança da informação e comunicações.

Art. 8º O cidadão, como principal cliente da Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, poderá apresentar sugestões de melhorias ou denúncias de quebra de segurança que deverão ser averiguadas pelas autoridades.

Art. 9º Esta Instrução Normativa entra em vigor sessenta dias após sua publicação.

JORGE ARMANDO FELIX