PORTARIA Nº. 779/2009-DG/DPF, DE 18 DE JANEIRO DE 2010

Institui a Política de Segurança da Informação do Departamento de Polícia Federal – DPF e dá outras providências.

O DIRETOR-GERAL DO DEPARTAMENTO DE POLÍCIA FEDERAL, no uso da atribuição que lhe confere o inciso IV do artigo 28 do Regimento Interno do DPF, aprovado pela Portaria nº. 3.961, de 24 de novembro de 2009, do Excelentíssimo Senhor Ministro de Estado da Justiça, publicada na Seção 1 do DOU nº. 225, de 25 de novembro de 2009,

CONSIDERANDO o Decreto nº. 3.505/2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Instrução Normativa nº. 1/2008-GSI/PR, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

CONSIDERANDO a Portaria nº. 279/2006-MJ, que instituiu a Política de Segurança da Informação do Ministério da Justiça;

CONSIDERANDO a Portaria nº. 462/2000-GAB/DPF, que instituiu a Política de Segurança da Informação do DPF e a Portaria nº. 156/2009-GAB/DPF, que alterou a constituição e as atribuições da Comissão de Segurança Institucional – CSI;

CONSIDERANDO a NBR ISO/IEC 17799, que dispões sobre práticas internacionais para a gestão da segurança da informação; e

CONSIDERANDO a necessidade de formalizar as práticas de Segurança da Informação adotadas no âmbito do DPF,

R E S O L V E :

Art. 1º. Aprovar, na forma do Anexo, a Política de Segurança da Informação do DPF.

Parágrafo único. A presente Política de Segurança da Informação visa prover o DPF de norma para segurança da informação estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra indisponibilidade, divulgação, acesso e modificação não autorizados de informações e dados nos termos dos Decretos nº. 3.505/2000, 4.073/2002, 4.553/2002 e 5.301/2004, observadas as normas NBR ISO/IEC 27001:2005, NBR ISO/IEC 27002:2007 e NBR ISO/IEC 27005:2008.

Art. 2º. Esta política se aplica, no que couber, às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito do DPF ou quem quer que venha a ter acesso a dados ou informações protegidos por esse regulamento.

Art. 3º. Esta Portaria entra em vigor na data de sua publicação em Boletim de Serviço.

ANEXO

1. CONCEITOS E DEFINIÇÕES

1.1. Segurança da Informação:

"Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento". (08)

1.2. Confidencialidade:

"Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas". (01)

1.3. Integridade:

"Salvaguarda da exatidão e completeza da informação e dos métodos de processamento". (01)

1.4. Disponibilidade:

"Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário." (01)

1.5. Dado:

Qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação.

1.6. Informação:

Dados organizados e inseridos em um contexto, de maneira a propiciar determinado retorno ao manipulador, permitindo a escolha entre os vários caminhos que possam levar a um resultado.

1.7. Sistema 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.

1.8. Sistema de Segurança da Informação:

Sistema destinado à proteção contra a quebra de confidencialidade, de integridade ou de disponibilidade de dados ou informações armazenados, em processamento ou em trânsito, podendo abranger a segurança dos recursos humanos, da documentação e do material das áreas e instalações de comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (08)

1.9. Ativo de Informação:

É o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos. (01)

São exemplos de ativos associados com sistemas de informação:

a) bases de informação: base de dados e arquivos, documentação de sistema, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação e informações armazenadas;

b) ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) ativos físicos: equipamentos computacionais (processador, monitor, computador), equipamentos de comunicação (roteador, modem, PABX, fax, secretária eletrônica), mídia de armazenamento computacional (fitas e discos), outros equipamentos técnicos (nobreaks, ar-condicionado), mobília, acomodações, cofres, instalações; e

d) serviços: computação e serviços de comunicação, utilidades gerais, por exemplo iluminação, eletricidade e refrigeração.

1.10. Ativo de processamento:

Patrimônio formado por elementos físicos e lógicos essenciais à execução dos sistemas e processos do DPF, compreendendo tanto os produzidos internamente quanto os adquiridos.

1.11. Responsabilidade:

"Obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações". (06)

1.12. Usuário:

Indivíduo com acesso autorizado a dados e informações de acordo com as restrições e permissões definidas.

1.13. Servidor:

"Pessoa legalmente investida em cargo público". (05)

1.14. Colaborador:

Todas as pessoas envolvidas com o desenvolvimento de atividades na organização, de caráter permanente, continuado ou eventual, incluindo prestadores de serviço, consultores e estagiários.

1.15. Plano de Continuidade:

Abrange ações que envolvam respostas a eventos extraordinários, ações relativas à garantia da continuidade de processos e ações de recuperação ou de reposição de sistemas. Tem por objetivo manter em funcionamento os serviços e processos críticos na eventualidade da ocorrência de desastres, atentados e falhas.

1.16. Incidente de segurança de informação:

Conjunto de atividades ou eventos correlacionados entre si, vinculados à confidencialidade, integridade ou disponibilidade que resulta no comprometimento da segurança da informação.

1.17. Direito de acesso:

Faculdade de adentrar em um sistema de informação, respeitada a necessidade de conhecer.

1.18. Necessidade de Conhecer:

"Condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosas." (04)

1.19. Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação – GATI:

Grupo de pessoas com a responsabilidade de implantar e operacionalizar o tratamento da Segurança da Informação, no âmbito do Departamento de Polícia Federal, para prevenção, tratamento e resposta a incidentes de segurança da informação;

1.20. Comissão de Segurança Institucional – CSI:

Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do DPF;

1.21. Freqüência de Revisão:

Os instrumentos normativos gerados a partir desta política, incluindo a própria política, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de seis meses.

2. PRINCÍPIOS DE SEGURANÇA

A Política de Segurança da Informação no DPF é guiada pelos seguintes princípios: (03)

2.1. Responsabilidade:

As responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.

2.2. Conhecimento:

Para garantir a confiança no sistema, os administradores, os fornecedores e os usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários.

2.3. Ética:

Todos os direitos e interesses legítimos de usuários, intervenientes e colaboradores devem ser respeitados ao prover um sistema de informação e ao estabelecer um sistema de segurança.

2.4. Legalidade:

Processos de segurança devem levar em consideração os objetivos e a Missão do Departamento de Polícia Federal; bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais;

2.5. Proporcionalidade:

O nível, a complexidade e os custos dos processos de segurança devem ser apropriados e proporcionais ao valor e à necessidade de confiança nos sistemas de informação considerando a severidade, a probabilidade e a extensão de um dano potencial ou atual.

2.6. Integração:

Os processos de segurança devem ser coordenados e integrados entre si e com os demais processos e práticas da organização a fim de criar um sistema de segurança da informação coerente.

2.7. Celeridade:

As ações de resposta a incidentes e de correções de falhas de segurança devem ser tomadas o mais rápido possível.

2.8. Revisão:

Os sistemas de segurança devem ser reavaliados periodicamente, uma vez que os sistemas de informação e os requisitos de segurança variam com o tempo.

2.9. Liberdade:

Um sistema de segurança da informação deve ser compatível com o legítimo uso e fluxo de informações/dados devendo ser observadas as normas de privacidade e de direito de realização de auditorias.

3. COMPETÊNCIAS E RESPONSABILIDADES

3.1. Gerenciamento da Segurança da Informação:

O controle, a implementação e a manutenção da Segurança da Informação são de responsabilidade da seguinte infra-estrutura de gerenciamento: (01) (07)

a) Diretor-Geral: é responsável pela aprovação da Política de Segurança da Informação;

b) Comissão de Segurança Institucional: atribuições e composição são definidas em ato normativo próprio;

c) Gerente de Segurança: é o responsável por todas as atividades relacionadas com a Segurança da Informação, o qual, além de possuir formação profissional e experiência compatíveis com o grau de responsabilidade da função, deverá:

I – dispor de autoridade suficiente para que suas determinações referentes à Segurança da Informação sejam acatadas em todo o DPF;

II – ser membro integrante da Comissão de Segurança Institucional;

III – reportar-se diretamente a Comissão de Segurança Institucional de modo a evitar que as recomendações sobre questões de segurança da informação sejam diluídas ou ignoradas pela gerência intermediária no interesse da eficiência operacional;

IV – ser responsável pela gestão do conhecimento e pelas experiências internas para garantir consistência e fornecer auxílio nas tomadas de decisão sobre segurança da informação;

V – orientar e propor a oferta de recursos necessários em processos de investigação decorrentes de suspeitas de incidente ou violação de segurança da informação;

VI – difundir e promover o cumprimento da Política de Segurança da Informação pelas diversas áreas, enfatizando a responsabilidade de cada uma no tratamento da informação e dirimindo dúvidas quando necessário;

VII – promover cultura de segurança da informação e comunicações;

VIII – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

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

X – manter contato com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações.

d) GATI: atribuições e composição serão definidas em ato normativo próprio;

e) Gestor da Informação: é o dirigente da área a ser mais afetada por uma eventual falha no sistema de informação. O Gestor da Informação tem a responsabilidade primária pela segurança do sistema, além de:

I – determinar os requisitos de segurança da informação e autoridade para alocar os recursos necessários para alcançá-los;

II – definir as regras de liberação, bloqueio e autorização de acesso às informações pelas quais é responsável;

III – contabilizar e classificar a informação de acordo com o item 7, renovando ou alterando o seu tempo de vida pré-determinado;

IV – participar da definição e implantação dos mecanismos de proteção das informações sob sua gestão; e

V – conduzir processos formais de análise dos direitos de acesso dos usuários, de forma que tais direitos sejam analisados criticamente em intervalos regulares, não excedendo o período máximo de 6 (seis) meses, e que as autorizações para direitos de acesso privilegiado sejam analisadas em intervalos mais freqüentes, não excedendo o período máximo de 3 (três) meses.

f) Proprietário dos Ativos de Informação: é a pessoa responsável pela gerência da infra-estrutura do ativo, atendendo a especificação de qualidade de serviço e os requisitos de segurança da informação formulados pelo Gestor da Informação, e que poderá delegar formalmente atribuições relativas à Segurança da Informação.

3.2. Atribuição das responsabilidades em Segurança da Informação:

As responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação devem ser claramente definidas por normas específicas contendo orientações mais detalhadas para cada ativo e processo de segurança da informação:

a) Os vários ativos e processos de segurança da informação associados com o sistema devem ser identificados e claramente definidos; e

b) O gestor responsável por cada ativo ou processo de segurança da informação deve estar de acordo com as responsabilidades a ele atribuídas mediante o Regimento Interno. As áreas pelas quais cada gestor é responsável devem ser claramente definidas.

3.3. Processo de autorização para as instalações de processamento da informação:

A instalação de recursos para processamento de informações deve seguir as seguintes diretrizes:

a) Novos recursos devem ser formalmente aprovados:

I – pela administração dos usuários destes recursos; e

II – pelo gestor responsável pela manutenção do sistema de segurança da informação. (Este gestor deve garantir que todas as políticas e requisitos de segurança da informação relevantes sejam atendidos);

b) Novos aplicativos ou equipamentos, onde necessário, devem ser testados a fim de garantir que são compatíveis com outros componentes do sistema.

3.4. Cooperação entre organizações:

Devem ser mantidos contatos apropriados com autoridades legais, organismos reguladores, e provedores de serviço de informação, de forma a garantir que ações adequadas e

apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança da informação. Também deve ser providenciada a filiação a grupos de segurança da informação e a fóruns setoriais.

As trocas de informações de segurança devem ser restritas para garantir que informações confidenciais não sejam passadas para pessoas não autorizadas.

3.5. Segurança no acesso de prestadores de serviços:

Onde existir a necessidade de acesso de prestadores de serviços aos recursos de processamento da informação, uma avaliação dos riscos envolvidos deve ser feita para determinar as possíveis implicações na segurança e os controles necessários. Estes devem ser acordados e definidos através de contrato assinado com os prestadores de serviços.

O acesso de prestadores de serviços à informação e aos recursos de processamento da informação não deve ser permitido até que os controles apropriados sejam implementados e um contrato definindo os termos para a conexão ou acesso seja assinado.

Esta política deve ser observada no que concerne à assinatura de tais contratos e na contratação externa para processamento da informação.

4. CONTROLE E CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO:

4.1. Contabilização dos ativos:

O conjunto de informações acumuladas e o potencial de criação são considerados inteligência da instituição e devem ser preservados para que a instituição detenha sempre o controle da informação e da tecnologia desenvolvida por ela ou por terceiros. Toda e qualquer informação gerada dentro da instituição é de sua propriedade e só poderá ser divulgada mediante prévia autorização da autoridade competente.

Os principais ativos de informação devem ser inventariados sempre que se fizer necessário, não excedendo o período máximo de 6 (seis) meses.

No inventário devem constar pelo menos os seguintes itens:

a) Gestor;

b) Proprietário;

c) Classificação da informação;

d) Localização atual;

e) Normas e procedimentos relacionados;

f) Contratos relacionados;

g) Controles de segurança da informação implementados; e

h) Outros ativos relacionados.

4.2 Classificação da informação:

Os dados ou informações devem ser classificados segundo a necessidade de sigilo em: (04) (11)

a) Ultra-secreto: aqueles referentes à soberania e à integridade territorial nacionais, à planos e operações militares, às relações internacionais do País, à projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e à programas econômicos,

cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado. Competência para essa classificação: Presidente da República; Vice-Presidente da República; Ministros de Estado e autoridades com as mesmas prerrogativas; Comandantes da Marinha, do Exército e da Aeronáutica; e Chefes de Missões Diplomáticas e Consulares permanentes no exterior;

b) Secreto: aqueles referentes à sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, à assuntos diplomáticos e de inteligência e à planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado. Competência para essa classificação: as autoridades que exerçam funções de direção, comando, chefia ou assessoramento, de acordo com regulamentação específica de cada órgão ou entidade da Administração Pública Federal;

c) Confidencial: aqueles que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado. Competência para essa classificação: os servidores civis e militares, de acordo com regulamentação específica de cada órgão ou entidade da Administração Pública Federal;

d) Reservado: aqueles cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos. Competência para essa classificação: as autoridades estabelecidas acima; e

e) Excepcionalmente, a competência prevista pode ser delegada pela autoridade responsável a agente público em missão no exterior. Dados ou informações não classificados segundo os critérios acima, cuja revelação não compromete planos, operações ou objetivos neles previstos ou referidos, são considerados de caráter ostensivo.

4.3 Níveis de proteção:

Os dados ou informações classificados devem receber um nível adequado de proteção, que considere também o potencial de impacto causado pela perda de integridade ou disponibilidade. Devem ser considerados os seguintes níveis de proteção: (02) (03) (10)

a) Extremamente Alto:

1) as informações ou dados são de caráter ultra-secreto, ou seja, a revelação de um dado ou informação não autorizada pode causar danos muito graves à sociedade ou à administração;

2) as informações devem ser corretas o tempo todo;

3) não é permitida a interrupção dos serviços; e

4) como regra geral, a conseqüência da exploração de uma vulnerabilidade do ativo causaria danos catastróficos ou injúrias a indivíduos, envolvendo perda de vidas humanas.

b) Alto:

1) as informações ou dados são de caráter secreto, ou seja, a revelação de um dado ou informação não autorizada pode causar danos graves à instituição ou à sociedade;

2) erros que afetariam a Missão, a reputação ou o interesse da instituição devem ser detectados e corrigidos imediatamente;

3) não são admitidas interrupções nos serviços; e

4) como regra geral, a conseqüência da exploração de uma vulnerabilidade do ativo causaria danos graves ou injúrias a indivíduos, sem envolver perda de vidas.

c) Médio:

1) as informações ou dados são de caráter confidencial, ou seja, a revelação de um dado ou informação não autorizada pode fazer com que os planos, as operações ou os objetivos neles previstos ou referidos não sejam alcançados;

2) erros que afetariam a Missão, a reputação ou o interesse da instituição devem ser detectados e corrigidos. Pequenos erros podem ser tolerados;

3) pequenos períodos de interrupção dos serviços oferecidos podem ser admitidos; e

4) como regra geral, a conseqüência da exploração de uma vulnerabilidade do ativo causaria danos significantes a indivíduos, sem envolver perda de vidas ou sérias injúrias.

d) Baixo:

1) as informações ou dados são de caráter reservado, ou seja, a revelação de um dado ou informação não autorizada pode comprometer operações internas;

2) se não afetarem a Missão, a reputação ou o interesse da instituição, pequenos erros podem ser tolerados;

3) a interrupção dos serviços oferecidos pelo ativo causaria baixo impacto nas atividades internas da instituição; e

4) como regra geral, a conseqüência da exploração de uma vulnerabilidade do ativo causaria pequenos danos a indivíduos.

e) Extremamente Baixo:

1) o ativo é de caráter ostensivo, ou seja, pode ser do conhecimento de todos;

2) erros podem ser tolerados e não farão com que a Missão da organização seja afetada;

3) a interrupção dos serviços oferecidos pelo ativo não causa impacto nas atividades desenvolvidas pela instituição; e

4) como regra geral, a conseqüência da exploração de uma vulnerabilidade do ativo causaria danos mínimos que afetariam operações internas.

4.4. Marcação e tratamento da informação:

Deve ser estabelecido um conjunto apropriado de procedimentos para rotular e tratar a informação, os quais devem abranger qualquer tipo de ativo de informação.

5. SEGURANÇA EM PESSOAS:

5.1. Novos servidores e prestadores de serviço:

As responsabilidades de segurança da informação devem ser atribuídas por ocasião da posse do servidor e incluídas em contratos dos prestadores de serviço e monitoradas durante a vigência de cada contrato de trabalho.

As ações que podem ser tomadas nos casos de desrespeito ao acordo devem ser incluídas no termo de posse ou em contrato de trabalho.

Todos os servidores e prestadores de serviço que utilizam as instalações de processamento da informação devem obedecer ao normativo interno que regula a matéria.

5.2. Treinamento dos usuários:

Deve ser elaborada uma política de capacitação em segurança da informação para usuários com o objetivo de assegurar que estejam cientes das ameaças e preocupações de

segurança da informação e equipados para apoiar a política de segurança da instituição durante a execução normal do seu trabalho.

Os usuários devem ser treinados nos procedimentos de segurança da informação e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança.

5.3. Notificações de falhas e incidentes de segurança da informação e mau funcionamento:

Quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços devem ser registradas e imediatamente notificadas aos superiores para encaminhamento ao GATI. Os usuários, para sua própria proteção, não podem, sob nenhuma circunstância, tentar averiguar uma fragilidade suspeita. A investigação de uma fragilidade pode ser interpretada como potencial uso impróprio do sistema.

Os usuários não devem tentar remover um problema suspeito em um aplicativo ou equipamento a menos que sejam autorizados.

Devem ser estabelecidos procedimentos formais para notificação de falhas e incidentes de segurança da informação e mau funcionamento de equipamentos ou aplicativos, bem como procedimentos de resposta a incidentes a serem tratados exclusivamente no âmbito do GATI.

6. AUDITORIA E CONFORMIDADE:

6.1. Conformidade com os requisitos legais:

Os estatutos, regulamentações ou cláusulas contratuais relevantes devem ser explicitamente definidos e documentados para cada sistema de informação. Os controles e as responsabilidades específicos devem ser, de forma similar, definidos e documentados para atender a estes requisitos. Nesse sentido, será definido Plano de Controle de Acesso aos Recursos Computacionais do Departamento de Polícia Federal.

Devem ser adotados procedimentos apropriados para garantir a conformidade com as restrições legais no uso de materiais protegidos por leis de propriedade intelectual, direitos autorais, patentes ou marcas registradas.

Os sistemas de armazenamento de informações, além de disponibilizar os dados em prazos e formatos aceitáveis, devem proteger os registros contra perda, destruição e falsificação, visando a salvaguarda dos registros organizacionais.

6.2. Prevenção contra uso indevido de recursos de processamento da informação:

Os recursos de tecnologia da informação e comunicação são de propriedade do Departamento de Polícia Federal e são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração.

É considerada imprópria a utilização destes recursos para propósitos não profissionais ou não autorizados. Os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que tomarem conhecimento dessa prática devem levá-la ao conhecimento do superior imediato para que sejam aplicadas as ações disciplinares cabíveis.

6.3. Monitoração de uso, inspeção de arquivos e auditoria:

A área de tratamento e respostas de incidentes de segurança da informação pode, a qualquer tempo, monitorar e registrar dados como início e fim de conexões à rede, tempo de CPU, utilização de discos feita por cada usuário, registros de auditoria, carga de rede, dentre outros.

Se houver evidência de atividade que possa comprometer a segurança da rede ou dos computadores, a área de tratamento e respostas de incidentes de segurança da informação pode

monitorar as atividades de um determinado recurso, além de inspecionar arquivos, a bem do interesse da organização.

As ações de monitoração, auditoria e de inspeção com objetivo de apurar incidentes de segurança são restritas a área de tratamento e respostas de incidentes de segurança da informação.

Durante as auditorias de sistemas devem existir controles para salvaguardar a integridade e prevenir o mau uso dos sistemas operacionais e das ferramentas de auditoria.

Ao utilizar os recursos de informática, o usuário concorda com esta política e autoriza implicitamente as ações de auditoria, monitoração e inspeção eventualmente necessárias.

6.4. Análise crítica de segurança da informação e conformidade técnica:

A segurança dos sistemas de informação deve ser analisada criticamente a intervalos regulares. Tais análises devem ser executadas com base nas normas apropriadas. As plataformas técnicas e sistemas de informação devem ser auditados na conformidade com as normas de segurança da informação implementadas.

6.5. Cancelamento de acesso:

Ao se desligar do Departamento de Polícia Federal o servidor, colaborador, consultor externo, estagiário ou prestador de serviço deve ter sua autorização de acesso cancelada e não poderá fazer uso de benefícios, contas, senhas de acesso, direitos especiais ou informações.

6.6. Suspensão de privilégios individuais:

A gerência da rede pode suspender todos os privilégios de determinado usuário em relação ao uso de redes e computadores sob sua responsabilidade, por razões ligadas à segurança física e ao bem estar do usuário, ou por razões disciplinares ou relacionadas à Segurança da Informação e ao bem-estar dos outros membros da rede. O acesso será prontamente restabelecido quando a Segurança da Informação e o bem-estar puderem ser assegurados.

6.7. Processo disciplinar;

A violação das normas de segurança da informação resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais e em penas e sanções legais impostas através de um procedimento administrativo disciplinar. Os casos omissos a esta política serão tratados pela Comissão de Segurança Institucional ou pelo órgão competente.

7. USO DOS RECURSOS COMPUTACIONAIS

O uso dos recursos computacionais no DPF, incluindo o correio eletrônico institucional e os acessos à Internet deverão seguir as diretrizes pertencentes na Política de Uso Aceitável (PUA), publicada na Portaria nº. 330/2009-DG/DPF, de 9 de junho de 2009.

8. CONCLUSÃO

As diretrizes de segurança da informação estabelecidas neste documento são aplicáveis tanto às informações armazenadas, quanto em trânsito e devem ser seguidas por todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

9. REFERÊNCIAS

(01) ABNT (2001) "Tecnologia da Informação – Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799)". ABNT. 2001.

(02) Stonebumer, G.; Goguem, A. e Feringa, A. (2001) "Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology (Special Publication 800-30)". NIST. 2001.

(03) OICT (Office of Information and Communications Technology) (1997), Information Security Guideline for NSW Gevernment – Part 1 Information Segurity Risc Management, Department of Commerce Guidelines, NSW – Autrália. 2003, 84p.

(04) Decreto nº. 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Publicado em 30 de dezembro de 2002.

(05) Lei nº. 8.112, de 11 de novembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

(06) Resolução nº. 2, de 25 de setembro de 2001, Ministério do Planejamento. Aprova a Política de Segurança da ICP – Brasil.

(07) Beal, Adriana (2003) "Manual de Segurança de Sistemas de Informação". Vydia Tecnologia. Fevereiro de 2003.

(08) Decreto nº. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Publicado em 14 de junho de 2000.

(09) Decreto nº. 4.073, de 03 de janeiro de 2002. Regulamenta a Lei nº. 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. Publicado em 04 de Janeiro de 2002.

(10) Decreto nº. 5.301, de 9 de dezembro de 2004. Regulamenta o disposto na Medida Provisória nº. 228, de 9 de dezembro de 2004, que dispõe sobre a ressalva prevista na parte final do disposto no inciso XXXIII do art. 5º. da Constituição, e dá outras providências. Publicado em 10 de dezembro de 2004.

(11) 03/IN01/DSIC/GSIPR – Diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.