PORTARIA Nº 279, DE 10 DE MARÇO DE 2006

Institui a Política de Segurança da Informação do Ministério da Justiça, e dá outras providências.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais e na forma dos Decretos nº 3.505, de 13 de junho de 2000, 4.073, de 03 de janeiro de 2002, e 4.553, de 27 de dezembro de 2002,

Considerando a necessidade de formalizar as práticas de Segurança da Informação adotadas pelo Ministério da Justiça,

Considerando o teor do Aviso nº 89-GSIPR/CH/SAEI, do Gabinete de Segurança Institucional da Presidência da República,

Considerando que a tramitação de informações seguras no âmbito deste Ministério é essencial ao cumprimento de sua missão institucional, e

Considerando a importância que deve ser dada à garantia da integridade, disponibilidade e autenticidade dos dados e informações nos mais diversos suportes utilizados por este Ministério, resolve:

Art. 1° Aprovar, na forma do Anexo, a Política de Segurança da Informação do Ministério da Justiça - PSI/MJ.

Parágrafo único. A Política de que trata este artigo visa prover o Ministério da Justiça de norma para segurança da informação, estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizados de informações e dados.

Art. 2º As diretrizes de segurança da informação estabelecidas nesta Portaria 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.

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

MÁRCIO THOMAZ BASTOS

ANEXO

1. FINALIDADE

Prover o Ministério da Justiça 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 3.505/00 (08), 4.073/02 (09), 4.553/02 (04) e 5.301/04 (11), observada a norma NBR ISO/IEC 17799 (01).

2. ABRANGÊNCIA

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 Ministério da Justiça ou quem quer que venha a ter acesso a dados ou informações protegidos por esse regulamento.

3. FREQÜÊNCIA DE REVISÃO

Os instrumentos normativos gerados a partir desta política devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 6 (seis) meses.

4. TERMOS E DEFINIÇÕES

4.1 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)

4.2 Confidencialidade

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

4.3 Integridade

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

4.4 Disponibilidade

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

4.5 Dado

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

4.6 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.

4.7 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.

4.8 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)

4.9 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, 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;
d) serviços: computação e serviços de comunicação, utilidades gerais, por exemplo iluminação, eletricidade e refrigeração.

4.10 Ativo de processamento
Patrimônio formado por elementos físicos e lógicos essenciais à execução dos sistemas e processos do MJ, compreendendo tanto os produzidos internamente quanto os adquiridos.

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

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

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

4.14 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.

4.15 Plano de Continuidade
Abrange ações que envolvem 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.

4.16 Incidente de segurança de informação
Conjunto de atividades ou eventos correlacionados entre si, vinculados à confidencialidade, integridade ou disponibilidade da informação.

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

4.18 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 sigilosos." (04)

5. PRINCÍPIOS DE SEGURANÇA
A Política de Segurança da Informação no Ministério da Justiça é guiada pelos seguintes princípios: (03)

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

5.2 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.

5.3 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.

5.4 Legalidade
Processos de segurança devem levar em consideração os objetivos e a Missão do Ministério da Justiça; bem como as leis, normas e políticas organizacionais, administrativas, comerciais, técnicas e operacionais;

5.5 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.

5.6 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.

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

5.8 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.

5.9 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.

6. SEGURANÇA ORGANIZACIONAL
6. 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) (10)
a) Autoridade máxima: é responsável pela aprovação da Política de Segurança da Informação.
b) Comitê Gestor da Segurança da Informação, que deve:
i. ser composto por servidores públicos;
ii. garantir que a segurança seja parte do planejamento dos processos de tratamento da informação;
iii. garantir direcionamento claro e suporte de recursos e de gerência aos envolvidos nas atividades de segurança da informação;
iv. deliberar sobre as diretrizes, normas e procedimentos de segurança da informação propostas por iniciativa dos próprios membros ou do Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação - GATI, bem como sobre alterações na Política de Segurança da Informação; e
v. analisar criticamente os incidentes de segurança da informação encaminhando sugestões de mitigação.
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 sejam acatadas em todo Ministério da Justiça;
ii. ser membro integrante do Comitê Gestor da Segurança da Informação;
iii. reportar-se diretamente ao Comitê Gestor da Segurança da Informação 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. gerenciar o Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação;
v. ser responsável pela gestão do conhecimento e pelas experiências internas para garantir consistência e fornecer auxílio nas tomadas de decisão sobre segurança da informação;
vi. orientar e oferecer recursos necessários em processos de investigação decorrentes de suspeitas de incidente ou violação de segurança da informação;

vii. 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.
d) Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação - GATI, cujos membros devem dedicar-se exclusivamente às atividades relacionadas à Segurança da Informação, sendo responsável por:
i. participar da elaboração de planos de continuidade;
ii. realizar auditorias, monitoração de uso e inspeções para avaliação da conformidade com as normas de segurança da informação em vigor;
iii. revisar e manter atualizadas as normas, instruções e procedimentos para tornar efetiva as diretrizes da Política de Segurança da Informação;
iv. propor as regras e atribuir as responsabilidades específicas para a Segurança da Informação;
v. avaliar a adequação e coordenar a implementação de controles específicos de segurança da informação para sistemas (aplicativos e equipamentos) ou serviços;
vi. definir mecanismos e regras de controle que monitorem o cumprimento da Política de Segurança da Informação, implantando os que estiverem sob sua responsabilidade;
vii. propor as metodologias e processos específicos para a Segurança da Informação, tais como análise e avaliação de riscos e sistema de classificação da informação;
viii. dar suporte de segurança da informação às diversas áreas que manipulem informações;
ix. analisar tecnicamente e monitorar incidentes de segurança da informação;
x. auxiliar os Gestores da Informação no processo de classificação da informação; e
xi. implementar mecanismos que permitam a quantificação, a classificação e o levantamento de custos dos incidentes de segurança da informação e do mau funcionamento de sistemas.
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, em conjunto com o GATI;
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.

6.2 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;
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 serclaramente definidas.

6.3 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;
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;
O uso de recursos pessoais de processamento de informação no ambiente de trabalho pode causar novas vulnerabilidades e, por esta razão, deve ser avaliado e autorizado pelo GATI.

6.4 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.

6.5 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.

7. CONTROLE E CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO
7.1 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.

7.2 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.

7.3 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.

7.4 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.

8. SEGURANÇA EM PESSOAS
8.1 Novos servidores e prestadores de serviço
As responsabilidades de segurança da informação devem ser atribuídas na fase de recrutamento, incluídas em contratos 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 contrato de trabalho.
Todos os servidores e prestadores de serviço que utilizam as instalações de processamento da informação devem obedecer ao regimento interno.

8.2 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.

8.3 Notificação 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. 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.

9. CONFORMIDADE
9.1 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.
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.

9.2 Prevenção contra uso indevido de recursos de processamento da informação
Os recursos de tecnologia da informação e comunicação são de propriedade do Ministério da Justiça 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.

9.3 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 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.

9.4 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.

9.5 Cancelamento de acesso
Ao se desligar do Ministério da Justiça 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.

9.6 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 bemestar 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.

9.7 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 sansões legais impostas através de um procedimento administrativo disciplinar.

Os casos omissos a esta política serão tratados pelo Comitê

Gestor de Segurança da Informação ou pelo órgão competente.

10. 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.

11. 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 N° 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 N° 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 N° 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 N° 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 N° 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) Nascimento, Ronaldo Íon. (2003). Ferramenta para Análise de Riscos Baseada na Norma ISO/IEC 17799. Publicação UnB. LabRedes. PFG.030/2003, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF.

(11) Decreto N° 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.