

Parágrafo único. A captação e o fornecimento de bases de dados e informações que não estiverem em conformidade com a PGDS-MJSP devem ser encaminhados para encerramento.

## CAPÍTULO VI

### DISPOSIÇÕES FINAIS

Art. 37. Dentro de cento e oitenta dias contados da data de publicação desta Portaria, as unidades organizacionais do MJSP deverão encaminhar ao Comitê de Governança de Dados e Sistemas de Informação a relação detalhada dos sistemas de informação, bases de dados, tabelas e consultas sob sua gestão, contendo:

I - descrição dos sistemas sob sua gestão e respectiva finalidade;

II - descrição detalhada dos bancos de dados e respectivas tabelas;

III - descrição detalhada dos campos das tabelas do banco de dados;

IV - descrição detalhada das relações entre as tabelas do banco de dados, no caso de banco de dados relacional;

V - descrição detalhada dos itens de informação, no caso de bancos de dados não relacionais;

VI - descrição do sigilo relativo à tabela, ao campo ou ao item de informação, com a respectiva fundamentação legal; e

VII - descrição detalhada do processo de trabalho, serviço público ou política pública as quais as bases de dados, os sistemas de informação ou os demais itens de informação estão associados.

Art. 38. Os acordos de cooperação, acordos, ajustes e demais instrumentos de captação de bases de dados e outros ativos de informação atualmente vigentes serão revistos no prazo de trezentos e sessenta dias contados da data de publicação desta Portaria, de forma a atender os objetivos, os princípios e as demais diretrizes aqui previstas.

## ANEXO XIII

### DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO - POSIC

#### CAPÍTULO I

##### DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicação - POSIC, que passa a integrar o SG-MJSP.

#### CAPÍTULO II

##### DO ESCOPO

Art. 2º A Política de Segurança da Informação e Comunicação - POSIC tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, bem como orientar as atitudes adequadas no manuseio, no tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso contra ameaças e vulnerabilidades.

#### CAPÍTULO III

##### DOS PRINCÍPIOS

Art. 3º As ações relacionadas com a segurança da informação e comunicação devem obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da ética, de auditoria e do não repúdio.

Parágrafo único. Devem ser adotadas como estratégias fundamentais de proteção:

I - privilégio mínimo: o acesso deve ser apenas às informações e recursos necessários para sua finalidade legítima;

II - defesa em profundidade: utilizar várias camadas de controle de segurança complementares;

III - elo mais fraco: a segurança total do sistema é igual à segurança oferecida pela sua proteção mais frágil; e

IV - simplicidade: quanto mais simples for um sistema, mais fácil é torná-lo seguro.

## CAPÍTULO IV

### DO ÂMBITO DE APLICAÇÃO

Art. 4º As disposições desta POSIC e eventuais normas complementares aplicam-se:

I - aos órgãos de assistência direta e imediata do Ministro;

II - aos órgãos específicos singulares e colegiados;

III - às entidades vinculadas do MJSP; e

IV - aos servidores, colaboradores, estagiários, consultores e quem, de alguma forma, desempenhe atividades no Ministério.

§ 1º É permitido aos órgãos de assistência direta e imediata ao Ministro, aos órgãos específicos singulares e colegiados, bem como às entidades vinculadas do Ministério que não integram o CGDSIC adotarem uma Política de Segurança da Informação e Comunicação própria.

§ 2º Os órgãos de assistência direta e imediata ao Ministro, os órgãos específicos singulares e colegiados, bem como as entidades vinculadas do Ministério que não integram o CGDSIC e que decidirem adotar a POSIC do MJSP deverão definir o seu modelo próprio de Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR e instituir sua criação.

Art. 5º As disposições desta POSIC também se aplicam, no que couber, ao relacionamento do Ministério com outros órgãos e entidades públicas ou privadas.

Parágrafo único. Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Ministério devem:

I - atender, no que couber, a essa política e demais normas relacionadas;

II - conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem; e

III - prever a obrigação de divulgação dessa política e suas normas complementares aos empregados envolvidos em atividades do contrato, por meio da assinatura de termo de ciência, quando a natureza de seu objeto ou condições específicas assim o exigirem.

## CAPÍTULO V

### DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os efeitos do disposto neste Anexo, adota-se a terminologia definida no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI nº 93, de 26 de setembro de 2019, e revisões posteriores, considerando-se ainda as seguintes definições:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - alta administração: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo Direção e Assessoramento Superiores - DAS ou Função Comissionada do Poder Executivo - FCP e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

III - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

IV - ativo: qualquer coisa que tenha valor para a organização e para os seus negócios;

V - ativos de informação: um corpo de informações, definido e gerenciado como uma unidade única para que possa ser entendido, compartilhado, protegido e explorado de forma eficiente e cuja informação têm valor, risco, conteúdo e ciclos de vida reconhecíveis e gerenciáveis;

VI - auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

VII - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

VIII - colaborador: pessoa jurídica ou pessoa física que desempenhe atividade de interesse do Ministério, realize estágio ou preste serviço, em caráter permanente ou eventual;

IX - computação em nuvem: modelo computacional que permite acesso por demanda e, independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

X - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

XI - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais, que, via de regra, requer procedimentos de autenticação;

XII - custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante ou dos ativos de informação que compõem o sistema de informação;

XIII - dados: informação processada ou armazenada por um computador podendo estar na forma de textos, documentos, imagens, áudios, clips, softwares, entre outros;

XIV - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XV - dispositivos móveis: equipamentos portáteis dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre os quais se incluem notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos, cartões de memória, entre outros;

XVI - Equipe de Tratamento e Resposta a Incidentes Cibernéticos: grupo de pessoas com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, observando a política de segurança e os processos de gestão de riscos de segurança da informação e comunicação do órgão ou da entidade;

XVII - evento: qualquer mudança de estado que tenha significado para o gerenciamento de item de configuração ou serviço de TI;

XVIII - gestão de ativos de informação: atividade coordenada de uma organização para obter valor a partir dos ativos, o que envolve um equilíbrio entre custos, riscos e desempenho;

XIX - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem, além de fornecer uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XX - gestão de riscos de segurança da informação e comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXI - gestão de segurança da informação e comunicação: 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 comunicação;

XXII - gestor de segurança da informação e comunicação: é responsável pelas ações de segurança da informação e comunicação no âmbito do órgão ou entidade da Administração Pública Federal;

XXIII - grau de sigilo: gradação de segurança atribuída a dados e informações em decorrência de sua natureza ou conteúdo;

XXIV - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXV - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXVI - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVII - não repúdio: garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá posteriormente negar sua autoria;

XXVIII - rede corporativa: sistema de transmissão de dados que transfere informações entre diversos equipamentos de uma mesma corporação e entre alguns desses equipamentos e o mundo externo;

XXIX - sistemas de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações em forma integrada;

XXX - Termo de Responsabilidade, Confidencialidade e Sigilo de Informação: 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;

XXXI - usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade, Confidencialidade e Sigilo de Informação; e

XXXII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

## CAPÍTULO VI

### DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 7º As ações de segurança da informação e comunicação deverão observar as disposições legais e regulamentares vigentes sobre o assunto.

## CAPÍTULO VII

### DAS DIRETRIZES GERAIS

Art. 8º A segurança da informação e comunicação é de responsabilidade de todos.

Art. 9º As ações de segurança da informação e comunicação devem considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, os requisitos legais, a estrutura e a finalidade do órgão.

Art. 10. As diretrizes de segurança da informação e comunicação descritas nesta Política devem ser observadas e cumpridas por todos os usuários que executam atividades vinculadas a este órgão durante todas as etapas do tratamento da informação, a saber:

I - produção;

- II - recepção;
- III - classificação;
- IV - utilização;
- V - acesso;
- VI - reprodução;
- VII - transporte;
- VIII - transmissão;
- IX - distribuição;
- X - arquivamento;
- XI - armazenamento;
- XII - eliminação;
- XIII - avaliação;
- XIV - destinação; e
- XV - controle da informação.

Art. 11. É condição para acesso aos ativos de informação do órgão a adesão formal aos termos desta política, mediante aceite de Termo de Responsabilidade, Confidencialidade e Sigilo de Informação.

Parágrafo único. A área de Tecnologia da Informação e Comunicação definirá o modelo do Termo de Responsabilidade, Confidencialidade e Sigilo de Informação a ser utilizado.

Art. 12. Todos os agentes públicos do órgão são responsáveis pela segurança dos ativos de informação e comunicação que estejam sob a sua responsabilidade e por todos os atos executados com sua identificação, tais como:

- I - identificação de usuário da rede (Login);
- II - crachá; e
- III - endereço de correio eletrônico ou assinatura digital.

Art. 13. Os recursos de tecnologia da informação e comunicação disponibilizados pelo órgão devem ser utilizados dentro do seu propósito, observado o uso ético em conformidade com a legislação vigente.

Art. 14. Os contratos de prestação de serviços conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo, ainda, exigir da entidade contratada a assinatura de Termo de Responsabilidade, Confidencialidade e Sigilo de Informação quando a natureza de seu objeto ou condições específicas assim o exigirem.

Art. 15. As normas, os procedimentos, os manuais e as metodologias de segurança da informação e comunicação devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de segurança da informação e comunicação, e devem estipular mecanismos que objetivem a conformidade dos controles de segurança da informação e comunicação associados, inclusive a previsão de auditoria.

Art. 16. A integração e a sinergia entre as instâncias e estruturas de supervisão e apoio definidas nesta POSIC e aquelas definidas no sistema de governança do órgão devem ser asseguradas por meio de modelos de relacionamento que considerem e compartilhem, quando possível, as competências, responsabilidades, informações e as próprias estruturas.

## CAPÍTULO VIII

### DAS DIRETRIZES ESPECÍFICAS

Art. 17. Para cada uma das diretrizes constantes das seções deste Capítulo, deve ser avaliada a pertinência da elaboração de políticas, normas, procedimentos, orientações e/ou manuais complementares que disciplinem ou facilitem seu entendimento.

## Seção I

### Da Propriedade da Informação

Art. 18. As informações geradas, adquiridas ou custodiadas sob a responsabilidade do órgão são consideradas parte do seu patrimônio intelectual, não cabendo a seus criadores qualquer forma de propriedade, salvo aqueles direitos garantidos no âmbito da Lei nº 10.973, de 2 de dezembro de 2004, e em outras legislações, e devem ser protegidas segundo as diretrizes descritas nesta política, em seus documentos complementares e demais regulamentações em vigor.

Parágrafo único. Incluem-se como propriedade do órgão todos os dados produzidos por ferramentas de trabalho providas para o bom desempenho das atividades laborais, a exemplo de dados do correio eletrônico corporativo, dados compartilhados em ferramentas de colaboração institucionais, registros de uso da internet, dentre outros, respeitada a proteção dos dados pessoais, na forma da legislação vigente.

## Seção II

### Do Tratamento da informação

Art. 19. A informação custodiada que for manuseada, armazenada, transportada ou eliminada pelos agentes públicos deste órgão, no exercício de suas atividades, deve ser protegida segundo as diretrizes descritas nesta POSIC e nas demais regulamentações em vigor.

Art. 20. Toda informação criada, manuseada, armazenada, transportada ou eliminada pelo órgão deve ser avaliada e, quando cabível, classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada, conforme processo de classificação da informação implementado e mantido no órgão em conformidade com a legislação em vigor.

Art. 21. Toda informação criada, manuseada, armazenada, transportada, eliminada ou custodiada por este órgão é de sua responsabilidade e deve ser protegida adequadamente.

## Seção III

### Dos Controles de Acesso e do Acesso à Internet

Art. 22. Todos os eventos relevantes devem ser registrados para a segurança e o rastreamento de acesso às informações, conforme norma específica.

Parágrafo único. Devem ser criados mecanismos para assegurar a exatidão e a integridade dos registros de auditoria nos ativos de informação.

Art. 23. Todo agente público do órgão que utiliza os recursos de tecnologia da informação e comunicação deve ter uma conta de acesso própria, cuja concessão e revogação será regulamentada em norma específica.

§ 1º A identificação do usuário, por qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo o reconhecimento do usuário de maneira clara e irrefutável.

§ 2º O usuário é responsável por todos os atos praticados com o uso de sua identificação na rede de dados, no correio eletrônico, na utilização da assinatura digital e recursos criptográficos, dentre outros, ficando encarregado pela segurança dos ativos e processos que estejam sob sua responsabilidade.

§ 3º A autorização, o acesso, o uso da informação e dos recursos de tecnologia da informação e comunicação devem ser controlados e limitados ao que for necessário ao cumprimento das atribuições de cada agente público.

§ 4º Deve-se aplicar a segregação de funções para as atividades de controle de acesso, incluindo o pedido de acesso, a autorização de acesso e a administração de acesso.

Art. 24. O acesso à rede mundial de computadores - Internet, no ambiente de trabalho, será regulamentado em norma específica.

## Seção IV

### Da Gestão de Ativos

Art. 25. Os ativos associados à informação e aos recursos de processamento da informação devem ser identificados e associados a um proprietário e um inventário destes ativos deve ser estruturado e mantido, conforme norma específica.

§ 1º O uso aceitável das informações, dos ativos associados e dos recursos de processamento da informação deve ser identificado e documentado.

§ 2º Os ativos devem ser passíveis de monitoramento e ter seu uso investigado, quando necessário, por meio de mecanismos que permitam a rastreabilidade de seu uso.

Art. 26. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizado, deve ser condicionado à assinatura do Termo de Responsabilidade, Confidencialidade e Sigilo de Informação, observando a legislação em vigor.

## Seção V

### Da Gestão de Riscos

Art. 27. As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação e comunicação, em conformidade com a Política de Gestão de Riscos e Controles Internos.

Parágrafo único. A gestão de riscos de tecnologia da informação deve avaliar os riscos relativos à segurança dos ativos de tecnologia da informação e a conformidade com exigências regulatórias ou legais.

## Seção VI

### Da Gestão da Continuidade do Negócio

Art. 28. A Estrutura de Segurança da Informação e Comunicação, em conjunto com as áreas responsáveis pelos ativos de informação, deverão instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços.

§ 1º O plano de continuidade deve conter os requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

§ 2º Os controles de gestão de continuidade da segurança da informação estabelecidos e implementados devem ser verificados a intervalos regulares, para garantir que sejam válidos e eficazes em situações adversas.

## Seção VII

### Da Gestão de Incidentes de Rede

Art. 29. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados em tempo hábil, bem como registrados em relatório abrangendo desde sua identificação até o tratamento, de forma a possibilitar auditorias futuras pelas áreas responsáveis pelos respectivos ativos de informação impactados e garantir a continuidade das atividades.

Parágrafo único. As responsabilidades e procedimentos de gestão de incidentes de rede devem ser estabelecidos, respeitando-se a segregação de funções, para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

Art. 30. A gestão de incidentes de segurança da informação será regulamentada por norma específica.

## Seção VIII

### Da Auditoria e Conformidade

Art. 31. O uso dos recursos de tecnologia da informação e comunicação disponibilizados por este órgão é passível de monitoramento e de auditoria, devendo ser implementados e mantidos mecanismos que permitam sua rastreabilidade.

§ 1º As atividades dos administradores e operadores do sistema devem ser registradas e os registros protegidos e analisados criticamente, a intervalos regulares.



§ 2º Os registros de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares.

Art. 32. Os controles de segurança da informação e comunicação devem ser analisados criticamente e verificados em períodos regulares pela Estrutura de Segurança da Informação e Comunicação, tendo por base a conformidade com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes, de modo a assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

Art. 33. A privacidade, o sigilo e a proteção das informações de identificação ou de cunho pessoal devem ser asseguradas, observando a legislação vigente.

#### Seção IX

##### Do Uso e do E-mail

Art. 34. O serviço de correio eletrônico terá seu uso exclusivo por agentes públicos no exercício de suas funções.

Art. 35. As regras de acesso e utilização do e-mail corporativo deverão ser definidas por norma específica.

#### Seção X

##### Da Computação em Nuvem

Art. 36. Fica permitido o tratamento das informações em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de segurança da informação e comunicação.

§ 1º O tratamento das informações deve ser realizado em ambiente previamente homologado pela autoridade da área de Tecnologia da Informação e Comunicação.

§ 2º É vedado o tratamento, em ambiente de computação em nuvem, de informação classificada em grau de sigilo, conforme a legislação vigente.

Art. 37. Nas contratações de soluções de tecnologias da informação e comunicação que utilizem recursos de computação em nuvem, devem ser observados os regramentos e as legislações vigentes que tratam do armazenamento de dados, metadados, inclusive as cópias de segurança quanto à necessidade de permanência em território nacional.

Parágrafo único. A área de Tecnologia da Informação e Comunicação deve manter monitoramento visando garantir que o disposto no caput deste artigo seja cumprido.

#### Seção XI

##### Da Aquisição, do Desenvolvimento de Software Seguro e da Manutenção de Sistemas

Art. 38. A área de Tecnologia da Informação e Comunicação deve estabelecer critérios de segurança para o desenvolvimento, manutenção e aquisição de sistemas e aplicações.

§ 1º Os requisitos relacionados à segurança da informação devem ser incluídos nas especificações dos novos sistemas de informação ou melhorias dos sistemas de informação existentes.

§ 2º As metodologias e regras implantadas para o desenvolvimento de sistemas e software devem contemplar requisitos relacionados à segurança da informação e desenvolvimento seguro de software.

#### Seção XII

##### Dos Dispositivos Móveis

Art. 39. O uso dos dispositivos móveis portáteis providos aos agentes públicos deverá ser realizado exclusivamente no interesse do órgão.

Art. 40. Todo dispositivo móvel usado para acessar a rede corporativa estará submetido às normas de segurança da informação e comunicação estabelecidas.

#### Seção XIII

##### Da Segurança Física e do Ambiente



Art. 41. Deverão ser providos mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências, em resposta aos riscos.

Parágrafo único. Norma específica deverá ser editada para regulamentar o acesso a áreas seguras e proteção do perímetro.

#### Seção XIV

##### Da Segurança em Recursos Humanos

Art. 42. Os usuários devem ter ciência das ameaças e preocupações relativas à segurança da informação e comunicação e de suas responsabilidades e obrigações conforme estabelecidos nesta política.

Art. 43. Todos os usuários devem difundir e exigir o cumprimento desta política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 44. Todos os colaboradores do órgão e, quando pertinente, partes externas devem receber treinamento e atualizações regulares sobre as políticas e procedimentos organizacionais de segurança da informação e comunicação.

Art. 45. O gestor de Segurança da Informação e Comunicação disponibilizará canal de notificação, de forma anônima, para reportar violações dos procedimentos e políticas de segurança da informação, sendo dever dos usuários relatar qualquer desvio que possa comprometer a segurança da informação e comunicação.

Parágrafo único. Toda notificação deverá ser averiguada, registrada e tratada, devendo ser uma prática a divulgação desse canal no âmbito deste órgão.

#### Seção XV

##### Da Gestão de Operação e Comunicações

Art. 46. A área de Tecnologia da Informação e Comunicação deve estabelecer modelos e arquiteturas de referência que descrevam requisitos mínimos para a disponibilização de serviços, sistemas e infraestrutura, atendendo às necessidades operacionais e de segurança desta política.

Parágrafo único. Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que deles necessitem.

Art. 47. A utilização dos recursos deve ser monitorada e ajustada e projeções devem ser feitas para necessidade de capacitação futura que garanta o desempenho necessário do sistema.

### CAPÍTULO IX

#### DAS PENALIDADES

Art. 48. A não observância desta política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicação, acarretará, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Parágrafo único. A área de Tecnologia da Informação e Comunicação poderá adotar as providências emergenciais necessárias para cessar as ameaças à segurança da informação e comunicação.

### CAPÍTULO X

#### DA ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO E SUAS RESPONSABILIDADES

Art. 49. A segurança da informação e comunicação é disciplina fundamental da boa governança corporativa.

Art. 50. Fica instituída a Estrutura de Segurança da Informação e Comunicação com atribuições definidas nesta POSIC.

Art. 51. A Estrutura de Segurança da Informação e Comunicação deverá institucionalizar um modelo de gestão de segurança da informação e comunicação capaz de apoiar os diversos níveis hierárquicos do órgão com o objetivo de integrar os controles e processos de segurança da informação e comunicação aos processos organizacionais existentes.

Parágrafo único. A participação na referida estrutura e eventuais grupos de trabalho associados não enseja remuneração de qualquer espécie ou quaisquer criações de cargos além daqueles já existentes na estrutura regimental, sendo considerada serviço público relevante.

Art. 52. Em conformidade com a política de governança institucional, a Estrutura de Segurança da Informação e Comunicação é constituída por:

- I - Comitê de Governança Estratégica - CGE;
- II - Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC;
- III - Gestor de Segurança da Informação e Comunicação;
- IV - Comissão Permanente de Avaliação de Documentos - CPAD;
- V - Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS; e
- VI - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

Parágrafo único. Os responsáveis por presidir ou coordenar as instâncias que formam a referida Estrutura de Segurança da Informação e Comunicação deverão garantir, em consonância com suas atribuições específicas, o cumprimento do disposto no Capítulo VII deste Anexo e o efetivo desempenho das competências da respectiva instância.

Art. 53. O CGE é a instância colegiada constituída como último nível para discussão de questões relativas à segurança da informação e comunicação, com caráter deliberativo.

Art. 54. O CGDSIC é unidade de apoio do CGE para temas relacionados com gestão de segurança da informação e comunicação, dentre outros.

Art. 55. A CPAD tem a responsabilidade de, dentre outros, orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no seu âmbito de atuação, tendo em vista a identificação dos documentos para guarda permanente e a eliminação dos destituídos de valor.

Art. 56. A CPADS tem a atribuição de opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo, dentre outras.

Art. 57. A função de Gestor de Segurança da Informação e Comunicação é instituída pelo SG-MJSP.

Art. 58. A Estrutura de Segurança da Informação e Comunicação do Ministério deverá estipular e implementar mecanismos que apoiem e garantam o comprometimento dos recursos humanos na implementação das diretrizes desta POSIC.

#### Seção I

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR

Art. 59. Fica criada a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

§ 1º Compete ao Gestor de Segurança da Informação e Comunicação designar os integrantes da ETIR, suas atribuições, os serviços a serem prestados, modelo de implementação, público-alvo, autonomia, estrutura organizacional, escopo de atuação e demais exigências relacionadas ao desempenho de suas atividades, em cumprimento às disposições sobre a criação e o funcionamento de colegiados da administração pública federal.

§ 2º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe.

§ 3º A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos.

§ 4º O Gestor de Segurança da Informação e Comunicação deverá instituir, no âmbito da área de Tecnologia da Informação e Comunicação, áreas de monitoramento, prevenção, reação, análise e inteligência de SIC, dentre outras, visando prestar apoio à ETIR.

Art. 60. A ETIR tem por missão identificar, receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança da informação e comunicação em sistemas computacionais, atuando também de forma proativa, com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer a missão da instituição, em consonância com as atividades de resposta e tratamento a incidentes em redes, tais como recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais.

## CAPÍTULO XI

### DAS DISPOSIÇÕES FINAIS

Art. 61. A POSIC e os documentos dela derivados deverão ser revisados sempre que mudanças significativas na estrutura do órgão ocorrerem ou quando alterações em normas e outras políticas forem aprovadas, ou ainda periodicamente a cada três anos, conforme a legislação vigente.

Art. 62. A POSIC e as normas e os procedimentos de segurança da informação e comunicação a ela associados deverão ser amplamente divulgados a todos que atuem direta e indiretamente no Ministério.

Este conteúdo não substitui o publicado na versão certificada.