MINISTÉRIO DO DESENVOLVIMENTO REGIONAL – MDR
COMPANHIA DE DESENVOLVIMENTO DOS VALES
DO SÃO FRANCISCO E DO PARNAÍBA

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA CODEVASF

Deliberação. nº 12, de 22 de fevereiro de 2021

2021

# SUMÁRIO

## CAPÍTULO I
## DO ESCOPO

Art. 1º A Política de Segurança da Informação da Codevasf - Posin tem por finalidade estabelecer as diretrizes para a segurança no uso, tratamento e controle, proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação da Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba - Codevasf.

Parágrafo único. A Posin está alinhada ao planejamento estratégico da Empresa, de forma a garantir a autenticidade, confidencialidade, disponibilidade e integridade das informações.

Art. 2º Para a segurança da informação na Codevasf serão rigorosamente observados o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

## CAPÍTULO II
## DA ABRANGÊNCIA

Art. 3º O disposto neste instrumento aplicar-se-á a todos empregados, estagiários, prestadores de serviço e demais agentes públicos ou privados que, formalmente, executem atividades no âmbito da Codevasf.

§ 1º Os contratos, convênios, termos de fomento, termos de colaboração e instrumentos congêneres, bem como os respectivos termos aditivos, conterão cláusulas específicas que imponham aos contratados/convenentes e assemelhados a obrigação de observarem o disposto na Política de Segurança da Informação– Posin, para o exercício de suas atividades no âmbito da Codevasf.

§ 2º Os estagiários serão orientados pelos seus respectivos supervisores quanto ao disposto nesta Posin.

## CAPÍTULO III
## DOS CONCEITOS E DAS DEFINIÇÕES

Art. 4º Para efeito da Posin da Codevasf, considera-se:

I – **Agente Responsável:** empregado ocupante de cargo de titular da Unidade de Infraestrutura e Tecnologia da Gerência de Tecnologia da Informação da Área de Gestão Estratégica, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

II - **Ativos de informação:** meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

III - **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;

IV - **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidades não autorizadas ou não credenciadas;

V - **Criptografia**: conjunto de princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra não inteligível, de forma que possa ser conhecida apenas pelo destinatário detentor da chave criptográfica;

VI - **Cópia de Segurança:** trata-se de cópia de dados em um meio separado do original, de forma a permitir a recuperação, dentro de período definido, em caso de pane na fonte original;

VII - **Credencial ou conta de acesso:** permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso ao ambiente físico ou lógico. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha ou dispositivo digital (token);

VIII - **Disponibilidade:** propriedade que garante que informações e serviços estejam acessíveis e utilizáveis sob demanda por pessoas, sistemas, órgãos ou entidades, devidamente autorizados;

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

X - **Gestor de Segurança da Informação:** empregado responsável pelas ações de segurança da informação no âmbito da Codevasf;

XI - **Gestão de Riscos de Segurança da Informação:** conjunto de processos que permitem identificar, analisar, avaliar e implementar medidas de proteção necessárias para o tratamento de riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

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

XIII - **Incidente em segurança da informação:** qualquer evento indesejado ou inesperado, confirmado ou sob suspeita, que possa comprometer as operações do negócio ou ameaçar a segurança da informação em aspectos de confiabilidade, integridade, disponibilidade ou autenticidade;

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

XV - **Plano de Continuidade de Negócios:** documentação dos procedimentos e das informações requeridas para que a Codevasf mantenha disponíveis e operacionais seus ativos críticos de informação segundo abordagem e estratégia definida em casos de incidentes;

XVI - **Segurança da Informação:** ações de proteção contra o acesso não autorizado, o uso indevido, a divulgação ilegal, a interrupção, a modificação ou a destruição não programada da informação e dos sistemas de informação, a fim de garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações; e

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

## CAPÍTULO IV
## DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5º A Posin da Codevasf está fundamentada, sem prejuízo de outras legislações aplicáveis, nos seguintes normativos:

I - Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

II - Lei nº 9.983, de 14 de julho de 2000 que altera o Decreto Lei nº 2.848, de 07 de dezembro de 1941, que trata da tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

III - Lei nº 12.527, de 18 de novembro de 2011 - Lei de acesso a informação;

IV - Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), e altera a Lei nº 12.965, de 23 de abril de 2014 que dispõe sobre o Marco Civil da Internet;

V - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações;

VI - Decreto nº 7.845 de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VII – Decreto nº 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, **caput**, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

VIII – Decreto nº 9.832 de 12 de junho de 2019, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação;

IX - Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da Administração Pública Federal;

X - Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;

XI - Norma Complementar nº 06/IN01/DSIC/GSIPR que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XII - Norma Complementar nº 07/IN01/DSIC/GSIPR que estabelece diretrizes para implementação de controles de acesso relativos à Segurança e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

XIII - Norma Complementar nº 08/IN01/DSIC/GSIPR que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XIV - Norma Complementar nº 11/IN01/DSIC/GSIPR que estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

XV - Norma Complementar nº 14/IN01/DSIC/GSIPR, e seu anexo, que estabelece diretrizes relacionadas à Segurança da Informação e Comunicações para o uso de computação em nuvem nos órgãos e entidades da Administração Pública Federal;

XVI - Norma Complementar nº 15/IN01/DSIC/GSIPR que estabelece diretrizes para o uso das redes sociais na Administração Pública Federal, direta e indireta – APF;

XVII – Norma NBR/ISO/IEC 27002/2005, de 31 de agosto de 2005, que institui o código de melhores práticas para gestão de segurança da informação;

XVIII – Norma NBR/ISO/IEC 27001/2006, de 31 de março de 2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação;

XIX - Norma NBR/ISO/IEC 27005/2008 que estabelece diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI);

XX - Instrução Normativa GSI Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

XXI – Instrução Normativa Nº 1, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal; e

XXII – Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação.

## CAPÍTULO V
## DOS PRINCÍPIOS

Art. 6º As ações de Segurança da Informação e Comunicações, no âmbito da Codevasf, são norteadas pelos seguintes princípios:

I - **responsabilidade**: os usuários dos sistemas de informação e comunicação devem conhecer e respeitar a Posin da Codevasf e serem responsabilizados pelos atos que comprometam a segurança da informação;

II - **ética**: as regras e os preceitos de ordem valorativa e moral de um indivíduo devem ser preservados sem o comprometimento da segurança da informação e comunicações;

III - **celeridade**: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;

IV - **clareza**: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

V - **privacidade**: o direito do cidadão de não ter registros pessoais e da vida privada divulgados sem sua prévia autorização devem ser assegurados; e

VI - **publicidade**: a divulgação das informações deve observar os critérios legais aplicáveis.

## CAPÍTULO VI
## DOS PRECEITOS

Art. 7º Constituem preceitos da Posin da Codevasf:

I - **segregação de função**: funções de planejamento, execução e controle deverão ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

II - **auditabilidade**: eventos significantes de sistemas e processos deverão ser rastreáveis até o evento inicial;

III - **controles automáticos**: sempre que possível, controles de segurança automáticos deverão ser utilizados;

IV - **resiliência**: os sistemas e processos deverão ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

V - **defesa em profundidade**: controles deverão ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança;

VI - **exceção aprovada**: exceções à Política de Segurança da Informação - Posin deverão sempre ter aprovação superior; e

VII - **substituição da segurança em situações de emergência**: deverão existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

## CAPÍTULO VII
## DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º Fica instituído o **Comitê de Segurança da Informação - CSI da Codevasf**, órgão colegiado de natureza consultiva e deliberativa, de caráter permanente, com as seguintes competências:

I – assessorar na implementação das ações de segurança da informação no âmbito da Empresa;

II - constituir grupos de trabalho para tratar de temas ou soluções específicas aplicáveis à segurança da informação;

III - propor medidas de conscientização, sensibilização e treinamento dos usuários dos sistemas de informação;

IV - propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação, em conformidade com a legislação em vigência;

V - tomar conhecimento da execução do Plano de Segurança da Informação – PSI no âmbito da Codevasf**;**

VI – emitir orientações a respeito dos incidentes críticos de segurança da informação a ele reportados.

§ 1º O Comitê de Segurança da Informação - CSI da Codevasf será coordenado pelo Gestor de Segurança da Informação da Codevasf.

§ 2º A composição, a organização e o funcionamento do CSI serão disciplinados em regimento próprio, aprovado pela Diretoria Executiva – DEX.

Art. 9º Fica instituída a **Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR da Codevasf**, equipe técnica de caráter permanente com as seguintes competências:

I - receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação e comunicações na rede e em sistemas computacionais da Codevasf;

II – apurar tecnicamente os incidentes críticos de segurança da informação, originados pelo descumprimento desta política, consolidando informações e reportando ao Comitê Gestor de Segurança da Informação.

III - atuar de forma preventiva, sempre que possível, e reativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o negócio da organização, implementando controles de segurança aplicáveis;

IV – buscar atuar conforme os padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República - CTIR GOV; e

§ 1º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR da Codevasf será chefiada pelo agente responsável.

§ 2º A composição, a organização e o funcionamento da ETIR serão disciplinados em regimento próprio, aprovado pela Diretoria Executiva – DEX.

Art. 10. Ao **Gestor de Segurança da Informação da Codevasf** caberá as seguintes atribuições:

I - coordenar o Comitê de Segurança da Informação - CSI em suas atividades e deliberações;

II - promover a divulgação da política e das normas internas de segurança da informação vigentes na Codevasf;

III – acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

IV – submeter o regimento interno do Comitê de Segurança da Informação, e suas alterações, à apreciação do referido Colegiado

V – verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

VI – acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação de segurança da informação;

VII - propor ao diretor-presidente os recursos necessários às ações de segurança da informação no âmbito da Empresa quando do planejamento orçamentário;

VIII - manter contato direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPRP, em assuntos relativos à segurança da informação;

IX – estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

Parágrafo único. O Gestor de Segurança da Informação da Codevasf será designado pelo diretor-presidente da Empresa, dentre os empregados ocupantes de cargo efetivo na Empresa, com capacitação técnica compatível às suas atribuições.

Art. 11. Ao A**gente Responsável pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR** da Codevasf caberá:

I - propor a criação de procedimentos internos;

II - gerenciar as atividades e distribuir tarefas para os membros que compõem a Equipe; e

III – coordenar as atividades de tratamento e resposta a incidentes em redes computacionais.

Art. 12. Compete à **Gerência de Tecnologia da Informação - AE/GTI**, no que se refere à segurança da informação, sem prejuízo das competências regimentais:

I - conscientizar, sensibilizar e treinar os usuários dos sistemas de informação e comunicações em relação aos conceitos e às práticas de segurança da informação;

II - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários dos sistemas de informação;

III - monitorar, analisar e implementar mecanismos que permitam identificar, avaliar e mitigar os danos ocasionados por incidentes de segurança;

IV - providenciar cópias de segurança e procedimentos de recuperação das informações conforme prazos e padrões compatíveis com as normas públicas;

V - promover inspeções periódicas em sistemas de informação e recursos computacionais verificando a integridade do próprio ambiente informatizado, com vistas a garantir a integridade dos dados manipulados;

VI - propor, implantar e operacionalizar rotinas e procedimentos que visam garantir o cumprimento dos princípios e diretrizes estabelecidas na Política de Segurança da Informação e da Codevasf;

VII - estimular a adoção de práticas que promovam a segurança da informação de TI na Empresa;

VIII - propor normativos operacionais aplicáveis à segurança da informação de TI em observância às normas exaradas pelo Gabinete de Segurança Institucional da Presidência da República – GSIPR;

IX - supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas de informação e dispositivos de tecnologia da informação voltados para segurança da informação;

X - manter a análise de riscos cibernéticos, refletindo o estado corrente da organização; e

XI - elaborar os Planos de Gerenciamento de Incidentes, Continuidade de Negócios, e Recuperação de Negócios com vistas a garantia de continuidade na disponibilização de recursos e serviços afetos à Tecnologia da Informação.

## CAPÍTULO VIII
## DAS DIRETRIZES GERAIS

Art. 13. De forma a promover a gestão e fomentar os aspectos de segurança da informação , a Codevasf deverá instituir normativos operacionais que estabeleçam processos e procedimentos que garantam o controle de acesso às informações, instalações e sistemas de informação.

Art. 14. O gerenciamento dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

Art. 15. Os usuários deverão ser treinados e conscientizados nos procedimentos de segurança da informação.

Art. 16. Quando do afastamento, da mudança de responsabilidade, de lotação ou de atribuições do usuário dentro da organização, far-se-á necessária a revisão imediata dos direitos de acesso e uso dos ativos de TI.

§ 1º Os direitos de acesso e uso dos ativos atribuídos ao usuário deverão ser extintos quando da efetivação de seu desligamento.

§ 2º Todo ativo produzido pelo usuário desligado será de propriedade da Codevasf, observadas as disposições da legislação aplicável.

### Seção I
### Do Tratamento da Informação

Art. 17. Toda informação criada, adquirida ou custodiada pelo agente público no exercício de suas atividades na Codevasf será considerada um ativo e deverá ser protegida de acordo com legislações e regulamentações de segurança aplicáveis para com os aspectos inerentes à confiabilidade, integridade, disponibilidade e autenticidade com o objetivo de mitigar os riscos a ela inerentes nas atividades e serviços executados pela Empresa ou delegados a terceiros.

Parágrafo único. O Tratamento da informação para com as questões decorrentes da Lei Geral de Proteção de Dados Pessoais, deverá ser objeto de normativa própria e segundo a legislação aplicável e competente para tal.

### Seção II
### Da Classificação da Informação

Art. 18. A classificação da informação no âmbito da Codevasf deverá observar ao disposto em normas e legislação específica.

Art. 19. As informações produzidas ou custodiadas pela Codevasf deverão ser classificadas quanto aos aspectos de sigilo e disponibilidade e receber o nível de proteção conforme as normas e legislação específicas.

Art. 20. Quaisquer informações produzidas ou custodiadas pela Codevasf deverão, ainda, atender aos critérios objetivos estabelecidos em normativo específico, com vistas ao prévio conhecimento do seu grau de sigilo por empregados, empresas contratadas e partes interessadas.

## Seção III
## Do Tratamento de Incidentes

Art. 21. Procedimentos formais para prevenção, auditoria, detecção, notificação e tratamento de incidentes de segurança deverão ser estabelecidos.

§ 1º Os incidentes de segurança deverão ser registrados e analisados periodicamente, servindo de subsídio para aperfeiçoamento dos procedimentos e controles de segurança vigentes.

§ 2º O Comitê de Segurança da Informação - CSI e a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR da Codevasf deverão, dentro de suas competências, adotar medidas de tratamento de incidentes de segurança ocorridos na Empresa.

## Seção IV
## Da Gestão de Risco

Art. 22. Os procedimentos de segurança da informação deverão ser planejados, documentados, testados, implementados e, periodicamente, avaliados segundo os objetivos institucionais e os riscos inerentes às atividades da Codevasf.

Art. 23. Os riscos, ameaças, vulnerabilidades e controles deverão ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida.

## Seção V
## Da Gestão de Continuidade

Art. 24. A gestão de continuidade é um processo abrangente que contempla normativos específicos que serão estabelecidos de modo a minimizar, em nível aceitável, os impactos sobre a Empresa em caso de ocorrência de falhas ou desastres significativos, por meio da combinação de ações de prevenção e recuperação.

## Seção VI
## Da Auditoria e Conformidade

Art. 25. Os mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de segurança da informação em vigor, deverão ser elaborados e implementados.

Art. 26. As medidas de proteção para que administradores de sistemas não tenham permissão de exclusão ou desativação de registros de *log* de suas próprias atividades deverão ser tomadas.

Art. 27. Os recursos e informações de registro de *log* deverão ser protegidos contra falsificação e acesso não autorizado.

## Seção VII
## Dos Controles de Acesso

Art. 28. Os procedimentos para controles de acesso, como a criação de perfis de acesso às instalações e a concessões de permissão para acesso às informações, deverão ser formalizados e comunicados para que sistemas, informações e recursos de informática tenham a sua confiabilidade, integridade e disponibilidade assegurada.

Parágrafo único. O tratamento às concessões de perfis de acesso delegadas a empresas e profissionais contratados, deverá ser objeto de supervisão e monitoramento continuado, de forma a garantir o propósito de sua utilização.

Art. 29. Para evitar que usuários dos ativos de TI tenham permissão para instalar, remover, modificar, criar ou desenvolver softwares sem justificativa e autorização deverão ser estabelecidas medidas de proteção.

Art. 30. Os procedimentos deverão ser criados e publicados no âmbito da Empresa, com vistas a divulgar a concessão de uso de serviços e dos recursos disponíveis.

## Seção VIII
## Do Uso de E-mail Corporativo

Art. 31. Os procedimentos para utilização do e-mail corporativo deverão ser estabelecidos de forma a assegurar o uso do correio eletrônico somente na execução do trabalho da Codevasf ou em benefício desta não sendo admitidas, sob condições normais, o emprego de e-mails pessoais para atividades do trabalho.

**Seção IX**
**Do Acesso à Rede**

Art. 32. Os procedimentos e controles de acesso à rede deverão ser estabelecidos para proteger a troca de informações em todos os tipos de recursos de comunicação.

**Seção X**
**Dos Dispositivos Móveis**

Art. 33. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da Codevasf deverá ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário.

**Seção XI**
**Da Computação em Nuvem**

Art. 34. As ações de segurança da informação para a implementação ou contratação de tecnologias de computação em nuvem, no âmbito da Codevasf, deverão estar em conformidade com as orientações definidas em normas regulatórias específicas, em vigência.

**Seção XII**
**Da Criptografia**

Art. 35. A cifração e a decifração de informações classificadas em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado, conforme procedimentos definidos em normas e legislação específicas em vigor.

**Seção XIII**
**Das Redes Sociais**

Art. 36. O uso institucional das redes sociais deverá ser norteado por diretrizes, critérios, limitações e responsabilidades estabelecidas, visando ao uso seguro das redes sociais, conforme procedimentos definidos em normas e legislação específicas em vigência.

CAPÍTULO IX
DAS PENALIDADES

Art. 37. Todos os responsáveis descritos no artigo 3º desta Política estão sujeitos às penalidades previstas na legislação, caso não cumpram o determinado nesse instrumento e o seu descumprimento poderá ser apurado, mediante processo administrativo interno pelas instâncias competentes.

## CAPÍTULO X
## DA ATUALIZAÇÃO

Art. 38. Esta Política poderá ter suas diretrizes revisadas anualmente ou sempre que se fizer necessário, não excedendo ao período máximo de 03 (três) anos, a contar da data de sua publicação.

## CAPÍTULO XI
## DAS DISPOSIÇÕES FINAIS

Art. 39. A Política de Segurança da Informação da Codevasf – Posin e suas alterações serão aprovadas pela Diretoria Executiva – DEX.

Art. 40. Esta Política quando necessário, poderá ser complementada por instrumentos, além dos já citados, aprovados pela Diretoria Executiva – DEX.

Art. 41. As dúvidas de interpretação desta Posin serão dirimidas pela Área de Gestão Estratégica – AE quanto ao teor redacional, pelo Gestor de Segurança da Informação quanto ao mérito técnico e operacional e pela Assessoria Jurídica - PR/AJ, quanto ao mérito jurídico.