Deliberação nº 248/2021/CFP

Considerando que compete à Comissão da Função Pública decidir sobre as práticas administrativas e de gestão no sector público, nos termos da alínea g) do n.º 2 do artigo 6.º da Lei n.º 7/2009, de 15 de Julho.

Considerando a necessidade de estabelecer regras sobre a segurança da informação e comunicação na Comissão da Função Pública;

Considerando a deliberação da Comissão da Função Pública na 91ª Reunião Extraordinária, de 2 de março de 2020;

Assim a Comissão da Função Pública, no uso das competências próprias previstas no número 2, do artigo 6º da Lei nº 7/2009, de 15 de Julho, e atendendo o disposto no artigo 20º do Decreto-Lei nr. 38/2012, de 1 de agosto, decide:

APROVAR o Regulamento de Segurança da Informação e Comunicação da Comissão da Função Pública, nos termos em anexo.

Publique-se

Díli, 29 de setembro de 2021.

Faustino Cardoso Gomes

Presidente da CFP

António Freitas

Comissário da CFP

Maria de Jesus Sarmento

Comissária da CFP

Carmeneza dos Santos Monteiro

Comissária da CFP

Fausto Freitas da Silva

Comissário da CFP

O valor dos ativos de informação produzidos pela Comissão da Função Pública (CFP) é medido de acordo com sua relevância social e econômica para a República Democrática de Timor-Leste. A disseminação de tais ativos deve ocorrer no momento certo e para o público certo, considerando que a disseminação interna e externa de informações da CFP deve levar em consideração a classificação das informações.

A elaboração e implementação de um Regulamento de Segurança da Informação e Comunicação (RESIC) é uma prática recomendada pelas normas da família ISO/IEC 27000, elaboradas pela Organisation Internationale de Nomalisation e International Electrotechnical Commission, e a CFP adota tais normas internacionais como referência.

A Comissão da Função Pública entende que a gestão da segurança da informação é um fator crítico de sucesso para o bom desempenho de suas atividades, além de reduzir a ameaças e riscos aos quais suas informações e sistemas estão expostos. Por isso, a CFP define que este RESIC será respeitada por todos que exercem atividades no âmbito da CFP e que tenham acesso às informações de propriedade ou sob custódia da CFP.

Art. 1º

Âmbito

1. A presente deliberação aprova o regulamento de Segurança da Informação e Comunicação da Comissão da Função Pública que possui a finalidade de definir diretrizes, estratégias e competências para assegurar a integridade, confidencialidade e disponibilidade das informações existentes no ambiente da CFP, de modo a preservar os seus ativos e sua imagem institucional.

1. Este RESIC se aplica à todas as unidades da CFP.

Art 2º

Objetivos

O Regulamento de Segurança da Informação e Comunicação da CFP tem os seguintes objetivos:

1. Definir regras para o uso e compartilhamento de dados, informações e documentos em todo seu ciclo de vida no âmbito da CFP, independentemente do meio que se encontrem;

    a) Definir competências e responsabilidades dos utilizadores;

    b) Conscientizar os utilizadores sobre a importância de atuar com ética e conforme as melhores práticas de Segurança da Informação;

    c) Fortalecer a cultura da segurança da informação na CFP;

    d) Definir em conjunto das normas de segurança da informação e dos processos de segurança da informação o modelo completo de Segurança da Informação adotado na CFP.

Art 3º

Definições

Considera-se, para fins deste Regulamento:

1. Ambiente de Formação: sistema utilizado com dados fictícios com fins de capacitação dos utilizadores do ambiente de produção;

a) Ambiente de Produção: sistema utilizado com os dados oficiais;

b) Ambiente de Testes: sistema utilizado para validação das novas funcionalidades desenvolvidas;

c) Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a CFP;

d) Ativo: aquilo que tem valor para a CFP, tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional;

e) Ciclo de vida: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, dado ou documento.

f) Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas, assegurando que indivíduos, sistemas ou entidades não autorizados tenham conhecimento da informação, de forma proposital ou acidental;

g) Dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

h) Descarte: eliminação correta de informações, documentos, mídias e acervos digitais.

i) Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema ou entidade autorizada;

j) Forma verbal “dever”: define como obrigatoriedade;

k) Forma verbal “poder”: define como permissão (opcional);

l) Forma verbal “ser”: define como obrigatoriedade;

m) Forma verbal “ter que”: define como obrigatoriedade;

n) Incidente: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

o) Informação custodiada: informação sob a guarda e responsabilidade da CFP;

p) Informação: conjunto de dados organizados que possam constituir referência sobre um acontecimento, fato ou fenômeno;

q) Integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;

r) Rede corporativa: conjunto de todas as redes locais sob a gestão da CFP;

s) Termo de responsabilidade: termo assinado por uma pessoa que concorda em contribuir com a disponibilidade, integridade e confidencialidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

t) Utilizador: Funcionário Público ou Agente da Administração Pública que possui competência e atribuições na CFP;

Art 4º

Princípios

Este RESIC observa os seguintes princípios:

a) Responsabilidade: os utilizadores devem conhecer e respeitar o RESIC da CFP;

b) Ética: os direitos dos utilizadores devem ser preservados, sem o comprometimento da segurança da informação e comunicação;

c) Celeridade: as ações de segurança da informação e comunicação devem oferecer respostas rápidas a incidentes e falhas de segurança;

d) Clareza: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

e) Identificação do utilizador: deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento;

f) Privacidade: informação relacionada à intimidade e à honra dos cidadãos não pode ser divulgada;

g) Publicidade: dar transparência no trato da informação, observado os critérios legais;

h) Equanimidade: o RESIC e suas normas complementares serão obedecidas por todos, sem distinção de cargo ou função;

i) Serão observados ainda, sem prejuízo das demais, outros princípios constitucionais e legais da República Democrática de Timor-Leste;

Art 5º

Responsabilidade dos Utilizadores

É da responsabilidade dos utilizadores da rede corporativa da CFP:

a) Manter a confidencialidade das informações de que tenha conhecimento por força de suas atribuições, especialmente no que concerne à sua exibição na tela do computador, à sua impressão, gravação e envio por quaisquer meios;

b) Preservar a confidencialidade de suas senhas de acesso;

c) Conhecer e zelar pelo cumprimento do RESIC.

d) Segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como login, senha eletrônica, e endereço de correio eletrônico.

e) Comunicar à autoridade competente irregularidades na utilização das informações e/ou acessos que venha a ter conhecimento.

f) Comunicar ao responsável pela seção de segurança da informação da CFP ou funcionário responsável pela segurança da informação da CFP os casos de incidentes na rede corporativa da CFP.

Art 6º

Vedações

É vedado aos utilizadores da rede corporativa da CFP:

1. Permitir o uso de sua senha de acesso aos sistemas da CFP por terceiros;

a) Divulgar a terceiros ou pessoas não autorizadas, informações ou dados extraídos dos sistemas da CFP;

b) Consultar ou extrair dados ou informações dos sistemas da CFP para fins estranhos às atividades da CFP;

Art 7º

Tratamento da informação

1. Toda informação criada, adquirida ou custodiada pelo utilizador, no exercício de suas atividades para a CFP, é considerada um bem e deve ser protegida pela CFP de acordo com este RESIC e demais regulamentações de segurança existentes.
2. As informações devem ser protegidas com o objetivo de minimizar riscos às atividades e serviços da CFP e preservar a sua imagem.
3. As regras de descarte de informações produzidas ou custodiadas pela CFP serão definidas em regulamento próprio.

Art 8º

Relação com Terceiros

1. Todo edital de licitação, contrato ou acordos de cooperação técnica com entidades externas deverá constar cláusula específica sobre obrigatoriedade de atendimento às diretrizes deste RESIC.
2. Deverá ser exigida a assinatura do termo de responsabilidade pela entidade externa.
3. As particularidades das relações com terceiros deverão ser definidas em regulamento próprio.

Art 9º

Classificação da Informação

1. As informações custodiadas ou de propriedades da CFP devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade.
2. As informações custodiadas ou de propriedades da CFP devem receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.
3. A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

4. Todo utilizador da CFP deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade da CFP e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Art 10º

Conscientização e Formação

1. A CFP desenvolverá um processo permanente de divulgação, sensibilização, conscientização e formação dos utilizadores sobre os cuidados e deveres relacionados à segurança da informação e comunicação.
2. A CFP incluirá em seu plano interno de capacitação de pessoal a participação dos envolvidos na Gestão da Segurança da Informação da CFP em eventos e treinamentos, nacionais e internacionais, relacionados à temas de Segurança da Informação e Comunicação.

Art 11º

Gestão de Riscos

1. A CFP deve adotar um processo de gestão de riscos.
2. A gestão de riscos será aplicada na implantação e operação da gestão de segurança da informação e comunicação.
3. Todas as definições de implantação, operação e manutenção de sistemas deverá ser feita considerando os riscos envolvidos.

Art 12º

Gestão de Continuidade

1. A CFP deve manter o processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos.
2. O processo de gestão de continuidade deve assegurar a retomada de atividades e processos críticos em tempo hábil.
3. As ações de continuidade da CFP devem ser adotadas por todas as unidades da CFP, de forma a proteger a reputação e imagem institucional.
4. As informações de propriedades ou custodiadas pela CFP, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades da CFP.
5. As informações armazenadas em outros meios, que não o eletrônico, devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Art 13º

Gestão de Incidentes de Rede Computacional

1. A CFP designará, em caráter temporário, um funcionário para ser responsável por receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança na rede corporativa da CFP.
2. A CFP manterá uma seção responsável pela gestão da segurança da informação, que será responsável pela gestão dos incidentes de rede computacional.
3. A regulamentação das atividades da seção de segurança da informação será realizada por regulamento próprio e deverá ser aprovada pelos comissários da CFP.

Art 14º

Utilização de Recursos Computacionais e de Comunicações

1. Recursos computacionais e de comunicações da CFP devem ser direcionados prioritariamente para realização de atividades profissionais da CFP.
2. A utilização de tais recursos deve ser baseada nos limites dos princípios da ética, razoabilidade e legalidade.
3. O uso institucional das redes sociais deverá ser regulamentado com diretrizes contendo, no mínimo, estratégia de comunicação social, processo de gestão de conteúdo, permissões de acesso, responsabilidades e outros aspectos relevantes.
4. A CFP nomeará um funcionário público para a gestão do uso seguro de cada perfil da CFP nas redes sociais.

Art 15º

Auditoria

1. A CFP deve criar procedimentos para implementação de auditoria nos sistemas e redes da CFP.
2. A CFP deve manter registros que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas e rede corporativa da CFP.
3. A CFP deve, periodicamente, promover verificação de conformidade às regulamentações e legislações de segurança em vigor.

Art 16º

Controles de Acesso

1. A CFP deve sistematizar a concessão de acesso como forma de evitar a quebra da segurança da informação e comunicação.
2. A CFP deve prover mecanismos de controle de acesso como consequência do processo de gestão de riscos de segurança da informação e comunicação.
3. O acesso às informações custodiadas ou de propriedade da CFP pelos utilizadores deve ser restrito ao que for necessário para o desempenho de suas funções.

4. O acesso físico às instalações da CFP deverá ser regulamentado com o objetivo de garantir a segurança dos funcionários e proteção dos ativos.

Art 17º

Competências

1. Compete ao Secretário Executivo da CFP dar suporte administrativo necessário à gestão do RESIC.
2. Compete ao Chefe de Departamento de Tecnologia da Informação e Manutenção de Redes dar suporte administrativo à implementação e operacionalização do RESIC, assim como implementação de soluções de tecnologia que auxiliem neste processo.
3. O responsável pela Segurança da Informação da CFP deverá propor regulamentos para implementação completa da RESIC na CFP.

Art 18º

Dúvidas

As dúvidas sobre a aplicação deste regulamento são resolvidas pelo Comissário/a Presidente da Comissão da Função Pública.

Art 19º

Divulgação

Após a publicação deste RESIC, deverá ser dada ampla divulgação a todos os utilizadores da CFP, inclusive publicação permanente no website e intranet da CFP.

Art 20º

Atualização e Vigência

1. Este RESIC deverá ser revisada e atualizada quando for identificada necessidade ou a cada 12 meses a contar da sua data de publicação.
1. Este RESIC entra em vigor na data de sua publicação.