Fundo de Garantia de Crédito

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Abril - 2023

Índice

Glossário de Termos

FGC	Fundo de Garantia de Crédito
CA	Conselho de Administração
GGRC	Gabinete de Gestão de Risco e *Compliance*
DTI	Direcção de Tecnologia de Informação

1. INTRODUÇÃO

Sendo a informação uma das variáveis determinantes na composição da oferta de produtos e serviços destinados aos seus clientes e colaboradores, através da presente Política de Segurança Cibernética o Fundo de Garantia de Crédito (FGC) está engajado em garantir a integridade, confidencialidade e disponibilidade da informação dos seus sistemas de informação, da privacidade dos seus clientes e colaboradores, do cumprimento de requisitos legais vigentes fornecendo de uma maneira eficiente e efectiva a gestão desta informação e do negócio.

2. ÂMBITO E APLICABILIDADE

1. A presente Política abrange controlos para assegurar a confidencialidade, integridade e disponibilidade de informações, como os principais pilares para a segurança da Informação, assim como medidas preventivas e correctivas, voltadas ao controlo do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de pontos de vulnerabilidades. Entre os principais controlos adoptados pelo FGC, estão:

    a. Autenticação;
    b. Criptografia;
    c. Prevenção e detecção de invasão;
    d. Prevenção de fuga de informações;
    e. Realização periódica de testes e varreduras para detecção de vulnerabilidades;
    f. Protecção contra *software* maliciosos.
    g. Estabelecimento de mecanismos de rastreabilidade da informação;
    h. Controlos de acesso e de segmentação da rede de computadores;
    i. Manutenção de cópias de segurança dos dados e das informações;
    j. Desenvolvimento seguro;

k. Gestão de incidentes;

l. Sensibilização de utilizadores, clientes e fornecedores:

   i. Iniciativas de sensibilização da cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica da sensibilização de colaboradores;

   ii. Iniciativas de sensibilização sobre segurança cibernética para clientes, empresas terceiras e prestadores de serviços relevantes.

2. Esta Política aplica-se a todos os colaboradores e demais intervenientes nos Sistemas de Informação do FGC.

3. OBJECTIVO

A presente Política tem como principais objectivos:

a. Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, colaboradores internos e fornecedores;

b. Proteger adequadamente os sistemas e informações;

c. Garantir a continuidade dos negócios, protegendo os processos críticos de interrupções; e

d. Garantir que sejam respeitadas as finalidades aprovadas pelo FGC durante a prestação de serviços de terceiros quando da contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

4. RESPONSABILIDADES

A segurança cibernética deve ser garantida pelos vários órgãos de estrutura do FGC no âmbito das suas atribuições descritas nos respectivos Manuais de Estrutura em vigor. As responsabilidades pela gestão da segurança cibernética são asseguradas pela Direcção de Tecnologias da Informação (DTI).

5. PRINCÍPIOS

O FGC possui políticas e procedimentos para assegurar que as informações estejam adequadamente protegidas, baseadas nos requerimentos mínimos exigidos pelo BNA e nas melhores práticas reconhecidas pelo mercado.

5.1. Gestão de Activos da Informação

Os activos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção actualizados.

5.2. Classificação da Informação

1. As informações devem ser classificadas de acordo com a confidencialidade e as protecções necessárias, abrangendo inclusive a criptografia de dados e de acordo com a classificação dos níveis de relevância.

2. Para mais informações, consultar a **Norma de Classificação de Informação e a Norma de Controlo de Acessos e Norma de Criação, Gestão e Senha de Utilizadores**.

5.3. Gestão de Acessos

1. As concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transacção.

2. Os níveis de controlos aplicados na gestão de controlo de acessos variam de acordo com a classificação do activo, incluindo, dentre outros, os seguintes mecanismos de controlo:

    a. Controlos de autenticação;
    b. Criptografia;
    c. Controlos de autorização;
    d. Segregação de funções; e
    e. Revisão periódica de acessos.

5.4. Gestão de Riscos Cibernéticos

Os riscos cibernéticos devem ser mapeados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os activos de informação do FGC, por forma a serem endereçadas as protecções adequadas.

5.5. Gestão da Continuidade de Negócios

1. Os controlos adoptados pelo FGC, na gestão de infraestrutura tecnológica, possuem como objectivo primário garantir que o FGC se mantenha operacional frente a ameaças cibernéticas, de modo a assegurar a confidencialidade, integridade e disponibilidade da informação.

2. A gestão de riscos cibernéticos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações do FGC.

3. Os seguintes controlos devem ser adoptados:

    a. *Backup* (cópias de segurança) dos dados e das informações;
    b. Elaboração de cenários de incidentes considerados nos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos; e
    c. Os resultados dos testes de continuidade de negócios devem ser informados para a confecção do relatório sobre o plano de acção e de resposta a incidentes.

5.6. Gestão da Segurança das Aplicações de Novas Tecnologias

As principais premissas aplicáveis à gestão de segurança das aplicações e adopção de novas tecnologias pelo FGC devem incluir:

a. O desenvolvimento de novas aplicações de serviços relevantes deve estar alinhado com as melhores práticas de segurança cibernética recomendadas por padrões internacionais e pelas políticas do FGC, específicas para desenvolvimento seguro;
b. Na adopção de novas tecnologias também deve ser submetido a controlos de segurança cibernética proporcionais à classificação de criticidade do activo, sendo que estas passam por processos de classificação, avaliação de riscos e implementação de correcções ou adequações antes de serem disponibilizadas no ambiente produtivo;
c. Controlos e mecanismos de rastreabilidade das informações;
d. Testes de segurança, como teste de penetração, código seguro e teste de vulnerabilidade, também devem ser executados para os serviços relevantes antes da implementação no ambiente de produção;
e. Testes de segurança da informação gerais (como, por exemplo, análise de código seguro);
f. Controlos para assegurar a segregação entre os ambientes de desenvolvimento, homologação/teste e produção, com o objectivo de reduzir os riscos de acessos não autorizados ou alterações indevidas no ambiente operacional, FGC de dados e/ou aplicações.

5.7. Testes de Segurança Cibernética

A gestão de testes de segurança cibernética do FGC inclui os seguintes mecanismos de controlo:

a. Testes de segurança cibernética para novas aplicações;
b. Testes de segurança cibernética para aplicações existentes;
c. Testes de segurança cibernética para a infraestrutura de rede;

d. Acompanhamento de correcções segurança de falhas identificadas durante os testes; e
e. Execução de novos testes de segurança cibernética para confirmação de que as falhas foram corrigidas.

5.8. Gestão de Incidentes de Segurança de Informação Tecnológica

A gestão e plano de respostas a incidentes cibernéticos para serviços relevantes do FGC, inclusive os ocorridos em sistemas operados ou instalados em empresas contratadas que prestam serviços relevantes, devem ser executados considerando as análises de causa, impacto e efeito dos incidentes, bem como deve incluir, dentre outros, os seguintes controlos:

a. Plano de Acções de Resposta a Incidentes;
b. Medidas preventivas e mitigantes de incidentes relacionados com o ambiente cibernético;
c. Processos e ferramentas utilizados na prevenção e resposta a incidentes;
d. Designação de área responsável pelo registo e controlo dos efeitos de incidentes relevantes;
e. Registo de incidentes, com informações sobre papéis e responsabilidades;
f. Classificação do incidente cibernético;
g. Análise de causa e impacto;
h. Recebimento de informações de fornecedores, relacionadas com incidentes com impacto na prestação de serviços relevantes;
i. Definição de mecanismos para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
j. Elaboração do relatório anual sobre o plano de acção e de resposta para incidentes;
k. Iniciativas para compartilhamento de informações sobre os incidentes cibernéticos relevantes com outras instituições financeiras autorizadas

pelo BNA ocorridos no FGC e/ou comunicados pelos prestadores de serviços relevantes do FGC; e

l. Comunicação tempestiva ao BNA das ocorrências de incidentes cibernéticos relevantes e das interrupções de serviços relevantes.

5.9. Monitoramento de segurança da informação e prevenção contra ciberataques

O processo de monitoramento de segurança da informação e prevenção contra ciberataques do FGC deve ter um conjunto de controlos e correctivos, com o objectivo de evitar a concretização de ameaças cibernéticas, dentre os quais destacam-se:

a. Aplicação de actualizações e correcções de segurança;
b. Monitoramento contra-ataques cibernéticos e prevenção contra invasões;
c. Verificação de conformidade de requisitos de segurança cibernética;
d. Realização periódica de testes e varredura de vulnerabilidades;
e. Monitoramento de status das ferramentas de antivírus e de alertas gerados;
f. Protecção contra *softwares* maliciosos;
g. Prevenção de fuga de dados.

5.10. Sensibilização sobre Segurança Cibernética

O FGC deve garantir a disseminação dos princípios e directrizes de Segurança Cibernética por meio de programas de sensibilização e capacitação, fortalecendo a cultura de segurança cibernética e informação, em todos os níveis operacionais.

5.11. Adopção da computação em nuvem

1. O FGC, quando da utilização de serviços em nuvem, atenderá aos critérios previstos no Aviso n.º 08/2020, do BNA, considerando a criticidade e a sensibilidade dos dados e das informações suportadas pelo referido serviço, de acordo com a sua classificação, bem como o risco associado em caso de acesso indevido;

2. Na gestão dos seus fornecedores de serviços em nuvem, o FGC busca principalmente garantir a execução de controlos para prevenção de incidentes a serem adoptados

por fornecedores que manuseiam dados sensíveis ou que sejam relevantes para as actividades do FGC. Os referidos controlos devem ser compatíveis com os processos e mecanismos de segurança cibernética adoptados pelo próprio FGC.

6. APROVAÇÃO E REVISÃO DA POLÍTICA

1. A presente Política, e quaisquer alterações futuras, serão aprovadas pelo Conselho de Administração (CA), a DTI coordenará a revisão regular da Política conforme solicitação do CA.
2. A Política deverá ser revista anualmente ou sempre que necessário, de forma a garantir a respectiva actualização, face a eventuais alterações legais, regulamentares e às evoluções do negócio do FGC.

7. DIVULGAÇÃO, REVISÃO E ACTUALIZAÇÃO DA POLÍTICA

1. A presente Política encontra-se disponível para consulta na Intranet do FGC e no Website disponível na Internet.
2. Esta Política deve ser revista periodicamente ou sempre que se verifiquem alterações que justifiquem a sua revisão.

8. MEDIDAS A TOMAR EM CASO DE INCUMPRIMENTO

As disposições da presente Política são aplicáveis e obrigatórias para todos os Colaboradores do FGC, independentemente da respectiva função e/ou responsabilidades, os casos de inobservância das normas estabelecidas pela presente Política deverão ser imediatamente comunicados a DTI, e constitui violação grave dos deveres de conduta e, em consequência, susceptível de aplicação de acção disciplinar contra as partes envolvidas, incluindo despedimento ou até processo criminal.

9. ENQUADRAMENTO REGULAMENTAR

O modelo de Gestão da Segurança Cibernética está apoiado em frameworks, princípios e directrizes nacionais e internacionalmente aceites, que visam assegurar a

confidencialidade, integridade e a disponibilidade das redes, dados e dos sistemas de informação utilizados, sendo eles:

- **Aviso 08/2020** - Política de Segurança Cibernética e Adopção de Computação em Nuvem do Banco Nacional de Angola;
- **ISO/IEC 27001** – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação;
- **ISO/IEC 27035** – Gestão de Incidentes de Segurança de Informação Tecnológica;
- **ISO/IEC 27002:2022** – Segurança da informação, cibersegurança e proteção da privacidade - Controles de segurança da informação.

10. ENTRADA EM VIGOR

A presente política entra em vigor imediatamente.