Política de Segurança

Sistema de Gestão da Segurança da Informação

Política de Segurança Cibernética

Documento com informação Pública	Referência EMISSI2301.PS	Versão 1.1 (Final) de 2024-03-18
Impresso para EMIS S.A.	Gestão de Sistemas de Informação	10 páginas

EMIS S.A. Rua Joaquim Kapango, nº 5 – 3º Andar, Edifício Kimpa Vita Atrium, CP 6189 Luanda, Angola
Telefone: +241 222 641 800 / Fax: +241 222 444 662

Ficha Técnica

Referência EMIS	EMISSI2301.PS
Tipo do Documento	Política de Segurança
Área de Conhecimento	Sistema de Gestão da Segurança da Informação
Título do Documento	Política de Segurança Cibernética
Versão	1.1
Estado	Final
Data de publicação	2024-03-18
Classificação de Informação	Pública
Unidade de Estrutura Responsável	DSC
Impresso para	EMIS S.A.

Autores e Participantes

Nome	Contacto	Função
DSC		Elaboração
DSC		Revisão
PCE		Aprovação

Revisões

Versão	Data	Descrição	Autores (Elabora, Revê, Aprova)
1.0	2023-04-16	Criação	DSC
1.1	2024-03-18	Alteração da “Classificação de Informação”; Inserção de novos destinatários na Lista de Distribuição	DSC

Lista de Distribuição

Nome
Colaboradores da EMIS
Prestadoras de Serviços de Pagamentos
Público

Índice

1 Introdução

A presente Política de Segurança Cibernética ("Política") é o documento que estabelece conceitos, directrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética, visando preservar todo e qualquer activo que intervém no negócio da Sociedade.

1.1 Objectivo

O presente documento serve como instrumento orientador sobre as responsabilidades da Sociedade na preservação, melhoria e resposta pela segurança cibernética dos seus sistemas de informação, a fim de protegê-los de uma variedade de ameaças cibernéticas.

Serve também para efeitos de cumprimento dos requisitos do Aviso n.º 08/2020, de 02 de Abril e do Instrutivo nº 10/2020, de 29 de Maio do Banco Nacional de Angola, bem como dos requisitos definidos pelo Conselho de Normas de Segurança da Indústria de Meios de Pagamento (*Payment Card Industry Security Standards Council*).

1.2 Âmbito

Essa versão do documento é aplicável ao desenho, implementação, operação e descomissionamento de todos os sistemas de informação existentes/operados pela Sociedade, tendo todos os colaboradores internos ou externos, parceiros e prestadores de serviços, a responsabilidade de serem diligentes no cumprimento das directrizes nela definidas.

1.3 Audiência

Este documento destina-se a todos os colaboradores da Sociedade, prestadores de serviço e utilizadores externos dos serviços e sistemas de informação geridos ou pertencentes a Sociedade.

1.4 Referências

São utilizadas ao longo de todo o documento as referências de documentação abaixo descritas.

01	Código de Conduta EMIS – Fev 2022
02	EMISSI1312.RS.Termos de Utilização Aceitável.v1.04F.20201110
03	EMISSI1302.PS.Princípios Gerais de Segurança de Informação.v1.05F.20240122
04	EMISSI1301.PS.Sistema de Gestão de Segurança de Informação.v1.03F.20201130
05	BNA – Aviso n.º 08/2020, de 02 de Abril: Sistema Financeiro – Política de Segurança Cibernética e Adopção de Computação em Nuvem
06	BNA – Instrutivo n.º 10/2020, de 29 de Maio: Sistema Financeiro – Reporte de Incidentes de Segurança Cibernética

1.5 Terminologia

No contexto deste documento, os seguintes termos devem ter a interpretação que se descreve abaixo.

Termo	
Sociedade	EMIS – Empresa Interbancária de Serviços, SA
UE	Unidade de Estrutura
PCI SSC	Payment Card Industry Security Standards Council
NIST	National Institute of Standards and Technology

1.6 Definições

Activos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Controlo de segurança: qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controlos materializa a segurança das informações. Podem ser interpretados como controlos: políticas, processos, estruturas organizacionais, técnicas padrão, software, hardware e outros.

Informação: qualquer conjunto organizado de dados que possua algum propósito e valor para a Sociedade, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.

Princípios de "*Least Privilege*" e "*Need to Know*": princípios que regem a autorização de qualquer acesso a sistemas e informações, segundo os quais deve ser concedido apenas o nível mínimo de acesso (*Least Privilege*) a quem realmente tenha a necessidade de acesso (*Need to Know*) para a realização das suas funções.

Segurança Cibernética: conjunto de políticas e controlos, meios e tecnologias que visam a prevenção de danos, proteção e restauração de programas, computadores, redes e dados da intrusão ilícita ou ataques digitais que provoquem danos aos mesmos.

Vulnerabilidade: conjunto de factores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou para a organização como um todo, os quais podem ser evitados por uma ação interna de segurança da informação.

2 Princípios da Segurança Cibernética

A Segurança Cibernética é baseada nos seguintes princípios:

- **Confidencialidade:** Garantia de que a informação seja acessível somente a pessoas com acesso autorizado.
- **Integridade:** Garantia ou salvaguarda da exactidão da informação e dos métodos de processamento, sem a ocorrência de alterações não autorizadas.
- **Disponibilidade:** Garantia de que os utilizadores autorizados obtenham acesso aos dados e aos activos correspondentes, sempre que necessário.
- **Autenticidade:** Garantia da propriedade de ser genuíno e poder ser verificado e confiável; confiança na validade de uma transmissão, da mensagem ou da fonte da mensagem.
- **Não repúdio:** Garantia de protecção contra utilizadores que negam falsamente a realização de acções, por via da capacidade de inspecção e identificação dos utilizadores.
- **Privacidade:** Garantia de protecção contra a intrusão na vida privada ou assuntos de um indivíduo quando essa intrusão resulta da colecta e uso indevido ou ilegal de dados sobre esse indivíduo.

3 Diretrizes Gerais

A Sociedade e seus executivos comprometem-se a conduzir uma cultura de excelência em segurança e uma sólida governança de eficácia no controlo, devendo observar as seguintes diretrizes:

- Estar em conformidade com a legislação e normativos de segurança, em vigor, tais como o Aviso n.º 08/2020, de 02 de Abril e o Instrutivo nº 10/2020, de 29 de Maio do BNA que dispõe, respectivamente, sobre a Política de Segurança Cibernética e o Reporte de Incidentes de Segurança Cibernética, e as

normas de segurança reconhecidas pela industria, tais como, as publicadas pelo PCI SSC (PCI-DSS, PCI-3DS e PCI-PIN);
- Assegurar que os procedimentos contenham no mínimo a descrição dos controlos referentes à segurança;
- Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, colaboradores e proteger os dados e os sistemas da informação, contra acessos indevidos, pessoas e alterações não autorizadas;
- Definir procedimentos para prevenção, identificação e tratamento de incidentes de Segurança Cibernética;
- Definir mecanismos de manutenção e actualização técnica e de segurança dos sistemas;
- Comunicar de forma tempestiva aos reguladores das ocorrências de incidentes de segurança cibernética relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise à empresa, bem como das providências tomadas para a recuperação das actividades;
- Definir procedimentos e controlos voltados à prevenção e ao tratamento dos incidentes a serem adoptados por empresas prestadoras de serviços que manuseiem dados ou informações sensíveis, ou que sejam relevantes para a condução das actividades operacionais da instituição;
- Definir procedimentos e controlos voltados ao descarte e manutenção segura de dados e equipamentos;
- Definir os parâmetros para classificação de dados e as informações quanto à relevância;
- Monitorar serviços contratados;
- Adoptar práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e
- Criar programas de conscientização e treinamento para os colaboradores sobre a segurança da informação.

4 Controlos para Garantia dos Objectivos de Segurança Cibernética

4.1 Tratamento da informação

O acesso à informação rege-se pelos princípios de "*Least Privilege*" e "*Need to Know*". Os colaboradores não devem efectuar tentativas de obter acesso às informações que não lhes são permitidos, devendo solicitá-los ao respectivo proprietário ou gestor da informação.

A elaboração das normas e procedimentos de acesso leva em consideração os riscos do acesso e a alteração não autorizada, de divulgação indevida e de indisponibilidade dos dados os quais, caso não sejam devidamento tratados, propriciam a ocorrência de fraudes, perdas financeiras, problemas legais e danos à imagem e reputação da instituição.

4.2 Classificação da informação

As informações da Sociedade, inclusive associadas aos processos de negócios, é classificada considerando-se o valor da informação, os requisitos legais, a sensibilidade, a criticidade, a necessidade de compartilhamento e restrição, a análise de riscos e os impactos para o negócio em todo o seu ciclo de vida, que compreende a: Geração, Manuseio, Armazenamento, Transporte e Descarte.

4.3 Controlo de acesso

O acesso às informações é autorizado de acordo com a necessidade de desempenho das actividades dos colaboradores, sendo estabelecido controlos para evitar acessos não autorizados, furtos, alterações indevidas ou sua fuga. Os acessos são rastreáveis, a fim de garantir que seja possível identificar individualmente o proprietário da credencial.

4.4 Autenticação

Para o acesso aos seus sistemas, a Sociedade adopta métodos de autenticação segura reconhecidos pela indústria, incluindo a autenticação forte por multifactor. A escolha do procedimento de validação observa a especificidade do acesso e o grau de confidencialidade da informação.

4.5 Gestão dos activos de tecnologia da informação

Os activos de Tecnologia da Informação são categorizados, inventariados e geridos durante todo o seu ciclo de vida, inclusive no descarte, que é realizado de modo a preservar a confidencialidade das informações e minimizar possíveis impactos ambientais.

4.6 Aquisição, desenvolvimento e manutenção de sistemas

Sistemas desenvolvidos internamente ou adquiridos externamente, contam com atributos e funcionalidades de segurança, que protegem adequadamente as informações e são aderentes às boas práticas de segurança. Os requisitos de segurança são estabelecidos, identificados e documentados na fase de concepção do sistema para assegurar que as medidas de protecção sejam implementadas.

4.7 Controlos criptográficos

É assegurado pelos colaboradores das distintas UE o uso efectivo da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade das informações corporativas.

4.8 Prevenção e a detecção de intrusão

As UE dedicadas, detectam as tentativas de intrusão através da monitorização permante do tráfego de rede e a detecção de tentativas de enumeração de portas, bem como de vários outros padrões de ataques cibernéticos que tenham como alvo os serviços ou a infraestrutura tecnológica da Sociedade.

4.9 A prevenção de fuga de informações

Seguindo as directrizes estabelecidas na Política de Segurança de Informação, a UE responsável pela Segurança Cibernética, acompanha e monitoriza o fluxo de informação por meio de ferramentas de protecção de dados em transição, repouso ou memória, garantindo a rastreabilidade.

4.10 A realização periódica de testes para detecção de vulnerabilidades

A identificação preventiva de vulnerabilidades de segurança na infraestrutura de tecnologias de informação da Sociedade é garantida por análises periódicas de segurança, respeitando o Calendário Operacional em vigor e obdecendo às etapas de execução definidas na documentação que rege o Processo de Gestão de Vulnerabilidades na Sociedade.

4.11 A protecção contra softwares maliciosos

A protecção contra Softwares Maliciosos é garantida pelo uso de soluções de *anti-malware* para monitorização, detecção, quarentena e erradicação de softwares maliciosos como vírus, *ransomwares*, *spywares* que possam surgir na infraestrutura de tecnologias de informação da Sociedade.

4.12 Segmentação das redes

É adoptada a divisão entre ambientes de homologação, pré-produção e produção, com controlos de acesso e diferenciação em termos de nível de segurança para cada ambiente, seguindo as melhores práticas e o conceito de dados seguros.
O acesso à cada ambiente é restrito às necessidades de utilização e contratos preestabelecidos.

4.13 Manutenção de cópias de segurança dos dados e das informações

Garantido com a realização de backups, conforme as Políticas e Procedimentos de Backup, em vigor na Sociedade, respeitando o grau de classificação da informação e realizados em conformidade com as leis e normas vigentes, incluindo o descarte e a reposição.

4.14 Novas tecnologias

São testadas e validadas considerando a convergência com a estratégia de negócio e a infraestrutura de tecnologias de informação da Sociedade, a fim de mitigar as potenciais ameaças cibernéticas.

4.15 Licenciamento de software

Todo equipamento tem o seu sistema operacional devidamente licenciado obedecendo os termos de utilização do fabricante. Softwares de uso diário, que não possuírem licenças gratuitas, também obedecem às regras de licenciamento do fabricante.
Não é autorizada a instalação e uso de softwares não licenciados sob pena de quem assim proceder, vir a ser responsabilizado por tal acção.

4.16 Segurança física

São implementados controlos físicos para prevenir o acesso não autorizado aos ambientes da Sociedade, sendo utilizados locais adequados para o armazenamento, processamento e manipulação da informação. Os detalhes sobre os pressupostos de segurança física da Sociedade, são considerados em documento autónomo, conforme referência em EMISSI1302.PS e EMISSI1301.PS.

4.17 Segurança nas operações e comunicações

São estabelecidos controlos de segurança para proteger e garantir a normalidade das operações relacionadas à manipulação e processamento das informações, medidas para prevenção e tratamento de incidentes operacionais, incluindo procedimentos formais para registo, reporte e escalonamento.

As redes de comunicação dispõem de uma infraestrutura adequada de protecção, de modo a prevenir a fuga, modificação e perda de informações, além de impedir a interrupção da comunicação.

4.18 Gestão dos riscos de segurança cibernética

Os riscos de segurança cibernética são identificados por meio de um processo assente na avaliação dos cenários de risco, considerando as vulnerabilidades e ameaças sobre os activos da Sociedade – dados, informações e sistemas de informação – para que sejam avaliadas as probabilidades de ocorrência e o impacto caso o risco se materialize.

4.19 Conformidade

Programas de conformidade são estabelecidos para a garantia da manutenção da conformidade da socieade às leis e normas em vigor.

Os contratos de prestação de serviços contêm cláusulas específicas relacionadas a confidencialidade das informações, com o intuito de proteger os interesses da Sociedade.

4.20 Continuidade de negócio

São estabelecidos, documentados, implementados e mantidos processos, procedimentos e controlos para assegurar o nível requerido de continuidade para os serviços e processos de negócio da Sociedade, durante situações adversas. O modelo adoptado para a Gestão de Continuidade de Negócios baseia-se na Norma ISO 22301.

4.21 Plano de Resposta a Incidentes

Os incidentes de Segurança da Informação são identificados e registados para a activação do plano de resposta, compreendendo a contenção, erradicação e recuperação dos níveis normais de operação, com a alimentação da base de dados de conhecimento para a retenção das lições aprendidas.

4.22 Tratamento de excepções

Excepções são documentadas de acordo com seu mapeamento, sempre que a tecnologia ou processo em questão não pode seguir ou implementar os controlos descritos nas normas ou na política de segurança vigente por uma necessidade de negócio ou limitação tecnológica, visando gerar visibilidade e rastreabilidade para tratamento.

4.23 Termos e Condições

Os produtos e serviços – internos e externos – da Sociedade são disponibilizados a colaboradores, parceiros e clientes mediante a declaração de leitura, entendimento e aceitação de termos e condições que regem o seu funcionamento, incluindo as disposições relacionadas à segurança, delineando as responsabilidades e as condições a observar na utilização dos sistemas de informação usados no negócio da Sociedade, que visam manter elevados padrões de segurança.

5 Papeis e Responsabilidades

Conselho de Administração: garantir a aprovação das iniciativas e estratégia de Cibersegurança proposta pela CE e supervisiona a evolução do nível de maturidade sobre segurança cibernética da Sociedade.

Comissão Executiva: garantir a implementação dos controlos de segurança cibernética no âmbito do Sistema de Gestão de Segurança da Informação da Sociedade (desenha a estratégia e a afectação dos recursos e meios subjacentes à salvaguarda da segurança da Instituição), respectivas políticas e limites de risco.

UE Responsável pela Segurança Cibernética: em articulação com as demais UE, desenvolver na Sociedade as capacidades de Detecção, Resposta e Recuperação face a potenciais incidentes cibernéticos e a capacidade de antecipar, resistir, recuperar e adaptar-se a quaisquer estresses, falhas, perigos e ameaças aos seus recursos cibernéticos no ecossistema em que opera, mantendo os níveis operacionais definidos.
Deve, igualmente, disponibilizar e divulgar esta Política aos colaboradores da Sociedade, além de outras Normas relacionadas à segurança da informação e protecção de dados, bem como promover a conscientização sobre o tema por meio do programa de sensibilização para a segurança da informação e outras acções de treinamentos e demais acções educativas.

Recursos Humanos: atribuir aos colaboradores na fase de formalização do contrato individual de trabalho, estágio, entre outros, a incumbência do cumprimento das responsabilidades para a manutenção da segurança da informação, através da assinatura do termo compromisso, bem como o comprometimento de manter sigilo e confidencialidade mesmo após o término do vínculo com a Sociedade, sobre todos os seus activos de informação.

Gestores: Cumprir e fazer cumprir esta política organizacional e seus documentos complementares, assegurando que os colaboradores sob sua gestão tenham ciência e acesso aos documentos de Segurança da Informação. Comunicar imediatamente eventuais casos de violação para a Segurança da Informação. Garantir a assinatura do termo de compromisso de todos os colaboradores que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Colaboradores: Estar ciente desta política organizacional, bem como das instruções normativas e procedimentos operacionais que a complementam. Participar das campanhas de conscientização em Segurança da Informação. Utilizar somente equipamentos e serviços disponibilizados pela Sociedade, para os quais possua permissão. Solicitar acesso somente aos recursos computacionais e sistemas

imprescindíveis para o pleno desempenho de suas atividades. Adotar uma postura ética e profissional com relação aos recursos computacionais e informações da Sociedade, principalmente as de caráter confidencial.

Terceiros: Estar ciente desta Política organizacional, bem como das instruções normativas e procedimentos operacionais que a complementam. Adoptar uma postura ética e profissional com relação aos recursos computacionais e informações da Sociedade, principalmente as de caráter confidencial.

6 Disposições Finais

6.1 Divulgação e Acesso

1. A presente Política encontra-se divulgada em ficheiro electrónico e disponível no website institucional da Sociedade para que o seu conteúdo possa ser consultado pelos clientes, parceiros, *stakeholders* e organismos externos, de acordo com a classificação dos respectivos documentos e autorização de acesso.
2. Todos os exemplares impressos são considerados cópias não controladas.

6.2 Revisão e Actualização

A actualização ocorre sempre que se fizer necessário, caso haja alguma mudança nas normas da Sociedade, alteração de diretrizes de segurança cibernética, objetivos de negócio ou se requerido por legislação ou pelo regulador local.

-=< FIM DE DOCUMENTO >=-