Zona Económica Especial
LUANDA | BENGO
ANGOLA
Special Economic Zone

ZONA ECONÓMICA ESPECIAL LUANDA – BENGO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Rev:00 Data 10/10/2024

Índice

1 Introdução 3
2 Abrangência e Objectivos da Política 3
3 Enquadramento legal 4
4 Termos e Definições 5
4.1 Termos 5
4.2 definições 5
5 Princípios Gerais 9
5.1 Definição de Segurança da Informação 10
5.2 Gestão de Riscos 11
5.3 Monitorização, controle e auditoria 11
6 Divulgação e Acesso à Estrutura Normativa 12
7 Responsabilidades 12
7.1 Gerais 12
7.2 Comité de Segurança da Informação 13
7.3 Direcção de Tecnologias da Informação e Comunicação (DTIC) 14
7.4 Adopção de Comportamento Seguro 15
7.5 Controlo de Acesso 16
7.6 Uso e Acesso à Internet e à Intranet 17
7.7 Uso do Correio Electrónico 18
7.8 Uso das Mídias Sociais 18
7.9 Uso da Impressora 19
7.10 Protecção Contra Softwares Maliciosos 19
7.11 Datacenter (centro de processamento de dados) 20
7.12 Backup (cópia de segurança) 20
7.12 Violações da Política De Segurança Da Informação E Sanções 21
7.13 Considerações Finais 22

1 INTRODUÇÃO

A Política de Segurança da Informação (PSI) enquadra-se no nível estratégico da estrutura documental do Sistema de Gestão de Segurança da Informação (SGSI) da Zona Económica Especial EP (ZEE EP), define e promove a estratégia de Segurança da Informação e tem na informação um dos seus principais activos, devendo ele ser adequadamente utilizado e protegido contra riscos, ameaças, violações, acessos não autorizados e danos. É imprescindível, a adopção de condutas, normas e procedimentos padronizados que tenham como objectivo garantir a proteção dos três aspectos básicos da segurança da informação: **confidencialidade, integridade e disponibilidade.**

Neste sentido, todos os documentos enquadrados nos níveis tático e operacional da estrutura documental (políticas específicas, normas, regulamentos, processos, procedimentos, modelos e outras evidências), devem ter como base o conteúdo vertido pelo presente documento e emanar as preocupações e considerações por ele estabelecidas e possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário.

2 ABRANGÊNCIA E OBJECTIVOS DA POLÍTICA

Os objectivos e diretrizes descritos neste documento serão desenvolvidos para toda a ZEE EP, devendo ser observados por todos colaboradores, fornecedores, prestadores de serviço e parceiros, e aplicam-se à informação em qualquer forma (arquivos eletrônicos, mensagens eletrônicas, dados de intranet e internet, bancos de dados, arquivos impressos, mídias de áudio e vídeo, dentre outros) e em qualquer meio ou suporte, durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte).

Contudo, nesta PSI, estarão integradas todos as políticas existentes, os regulamentos, manuais, instrutivos, procedimentos e modelos complementares, destinados à protecção da informação e à disciplina ao longo da sua utilização.

Apresenta-se o presente documento para explanar a estrutura da Segurança da Informação da ZEE EP, de modo a atingir os seguintes objectivos:

- Proteger a informação da ZEE EP, para garantir sua confiabilidade, autenticidade e integridade;
- Estabelecer directrizes para a utilização dos recursos de informação, serviços de redes de dados, estações de trabalho, *Internet*, telecomunicações, correio eletrônico e outros;
- Designar papéis e responsabilidades relativas à segurança da informação na ZEE EP;
- Ser transparente e inclusiva, de forma a conscientizar todos os colaboradores da ZEE EP, sobre a importância das informações e de suas vulnerabilidades;
- Promover e desenvolver a cultura de segurança da informação em todos os níveis da empresa;
- Ser parte integrante dos processos organizacionais;
- Possibilitar a criação de controles e promover a optimização dos recursos de tecnologia da informação.

3 ENQUADRAMENTO LEGAL

- Resolução n.º 33/19, de 09 de julho (União Africana) aprovada pela Assembleia Nacional aos 23 de maio de 2019 - Convenção da União Africana sobre Ciber Segurança e Protecção de Dados Pessoais, e tem por objectivo combater as Violações da Privacidade através da recolha, tratamento, transmissão, armazenamento e utilização de dados pessoais; • Lei n.º 7/17, de 16 de fevereiro (Assembleia Nacional);
- Lei de Protecção das Redes e Sistemas Informáticos, que estabelece o regime jurídico sobre as medidas de Protecção das Redes e Sistemas Informáticos; • Lei n.º 22/11, de 17 de junho (Assembleia Nacional);
- Lei da Protecção de Dados Pessoais, que estabelece as regras jurídicas aplicáveis ao tratamento de dados pessoais, com o objectivo de garantir o

respeito pelas liberdades públicas e os direitos e garantias fundamentais das pessoas singulares;

- Livro Branco das Tecnologias de Informação e Comunicação.

4 TERMOS E DEFINIÇÕES

4.1 Termos

CA- Conselho de Administração;
CSI – Comissão de Segurança da Informação;
DAC – Direcção de auditoria e Compliance;
DCM – Direcção de Comunicação e Marketing;
DJUR – Direcção Jurídica;
DSV – Direcção de Segurança e Vigilância;
DTIC – Direcção de Tecnologias de Informação e Comunicação;
PSI - Política de Segurança da Informação;
SGSI - Gestão de Segurança da Informação;
TI - Tecnologia de Informação;
ZEE EP - Zona Económica Especial Empresa Pública.

4.2 definições

Abaixo seguem, em ordem alfabética, os principais conceitos referidos neste documento, de forma a evitar dificuldades de interpretação ou ambiguidades:

- **Activo de Informação:** meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que têm acesso a eles;
- **Algoritmo:** conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas;
- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

- ***Antispyware*:** *software* de segurança que tem o objetivo de detectar e remover *softwares* maliciosos;
- **Assinatura Digital:** recurso criptográfico que tem por objectivo assinar documentos digitalmente;
- **Autenticidade:** propriedade que determina que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Backup:** é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais;
- **Certificado Digital:** é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, e por ele podem ser feitas transações *online* com garantia de autenticidade e proteção das informações trocadas;
- **Classificação da informação:** processo que tem como objectivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo sua importância;
- **Código Malicioso:** tipo de código de computador ou *script* da *Web* nocivo que tem como objectivo criar vulnerabilidades no sistema, violações de segurança, roubo de dados e informações, além de outros danos possíveis;
- **Confidencialidade:** somente pessoas devidamente autorizadas pelo órgão devem ter acesso à informação;
- **Controle de Acesso:** processo por meio do qual os acessos aos sistemas e a seus respectivos dados são autorizados ou negados; os acessos autorizados e, em alguns casos, também os negados ficam registrados para posterior auditoria;
- **Criptografia:** mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos, entre outros)

ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem;

- **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- **Dispositivos Móveis:** equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;
- **Engenharia Social:** habilidade de conseguir acesso a informações confidenciais ou a áreas importantes de uma instituição por meio de habilidades de persuasão;
- **FTP (*File Transfer Protocol*):** protocolo que permite a transferência de arquivos entre computadores conectados à *Internet*;
- **Gestão de Segurança de Informação e Comunicação:** processo que visa a proteção dos activos de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados armazenados ou em trânsito, inclusive a segurança dos recursos humanos, da documentação, das áreas e das instalações computacionais e de comunicações;
- **Governance-** garantia de que a Segurança da Informação se encontra alinhada com os objectivos de negócio, através do desenvolvimento de processos de gestão eficientes e eficazes que suportem a tomada de decisão;
- **Incidente:** qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança dos sistemas, das informações ou das redes de computadores
- **Informação:** dados estruturados, organizados e processados, apresentados dentro do contexto, o que o torna relevante e útil para a pessoa que o deseja.
- **Integridade:** alterações, supressões e adições nas informações devem ser realizadas apenas sob processos legalmente válidos, por pessoas

devidamente autorizadas para tal (autênticas). Garante que as acções que modifiquem as informações não ocorram de forma acidental ou não autorizada;

- ***Login*:** processo para acessar um sistema informático restrito feita por meio de autenticação ou identificação do utilizador;
- **Mídia Removível:** tipo de memória que pode ser removida do seu aparelho de leitura, conferindo portabilidade para os dados que carrega;
- **Plano de Continuidade de Negócio:** documento que estabelece mecanismos para restabelecer a actividade de uma organização, em caso de interrupção;
- **Programas Antivírus:** programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário;
- **Risco:** efeito da incerteza no alcance dos objectivos definidos;
- **Servidor:** *software* ou *hardware* que fornece um ou mais serviços a uma rede de computadores;
- **Sistema de Gestão de Segurança da Informação:** abordagem sistemática para gerir e proteger os activos de informação da ZEE EP, sendo materializado por um conjunto de políticas, normas e procedimentos, bem como os controlos que definem toda a estratégia e operacionalização da Segurança da Informação. Os tipos de controlos que devem ser implementados são maioritariamente determinados com base nos resultados de avaliações de risco, mas também pelas exigências das partes interessadas, definidas pelo contexto da ZEE EP.
- ***Software*:** programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador;
- **Termo de Responsabilidade e Sigilo:** documento pelo qual o colaborador se compromete a não revelar as informações de caráter secreto, sigiloso e confidencial da empresa;

- ***Torrent*:** extensão de arquivos utilizados por um protocolo de transferência do tipo P2P (*Peer to Peer*);
- **Vírus de Computador:** *software* malicioso capaz de infectar um sistema, fazer cópias de si e se espalhar para outros computadores e dispositivos;
- ***Wireless*:** tecnologia que significa "sem fio" (em livre tradução), e possibilita a transmissão da conexão entre pontos distantes sem precisar usar fios (como ocorrem em telefones sem fio, rádios ou celular).

5 PRINCÍPIOS GERAIS

Esta política aplica-se a todos os colaboradores da ZEE EP, de modos a garantir o uso responsável das ferramentas de trabalho de TI que são disponibilizadas a todos, devendo ser observado todos os requesitos e orientações aqui descritas.

O conjunto de documentos que compõe está PSI deverá se guiar pelos seguintes princípios:

- **Simplicidade**: a complexidade aumenta a chance de erros, portanto, todos os controles de segurança deverão ser simples e objectivos;
- **Privilégio Mínimo:** utilizadores devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;
- **Segregação de função:** funções de planeamento, execução e controle devem ser segregadas, de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos activos, bem como para permitir maior eficácia dos controles de segurança;
- **Auditabilidade:** todos os eventos significantes de usuários e os processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;
- **Mínima dependência de segredos:** os controles deverão ser efectivos, ainda que se conheça a existências deles e como eles funcionam;

- **Resiliência:** os controles de segurança devem ser projectados para que possam resistir ou se recuperar dos efeitos de um desastre;
- **Defesa em profundidade:** os controles de segurança devem ser concebidos em múltiplas camadas, de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado.

5.1 Definição de Segurança da Informação

A segurança da informação é parte vital de todo o negócio, pois acopla uma série de acções adoptadas estrategicamente para controlar e evitar riscos de roubo, danos e perdas dos dados, dispositivos, servidores, sistemas e redes. Sua função é identificar, registar e combater as ameaças que surgem no meio do caminho.

Com a definição de metodologias para assegurar a informação e monitorizar os riscos associados a informação, a ZEE EP, formalmente definiu três pilares como a preservação da **confidencialidade, integridade e disponibilidade** da informação.

Os três pilares definidos para a segurança da informação da ZEE EP são importantes nas seguintes medidas:

- **Confidencialidade:** manter informações em sigilo, protegendo os dados para que eles não fiquem vulneráveis, sendo concedida apenas a pessoas autorizadas;
- **Integridade:** Salvaguarda da exactidão da informação e dos métodos de processamento;
- **Disponibilidade:** Garantia de que os utilizadores autorizados têm acesso à informação e activos correspondentes sempre que necessário. Estes conceitos são complementares e devem ser entendidos como um todo. Assim, só garantindo que a informação seja acessível apenas por aqueles que têm autorização para o fazer, que a sua integridade e completude é rigorosa.

A relevância dos conceitos apresentados deve ser entendida como um todo, de modos a garantir maior segurança da informação, que deve ser acessível apenas

por pessoas devidamente autorizadas e responsáveis, obedecendo todo o rigor desta política, oferecendo assim um sistema devidamente seguro e eficaz.

Além dos conceitos acima descritos, importa considerar que, para a segurança da informação e de todos que manuseiam, deve haver Autenticidade, Não Repudiação e Privacidade.

- **Autenticidade:** consiste na certeza absoluta em manter a veracidade ou originalidade da informação, sem que a mesma sofra alguma alteração por quem manuseia sem previa autorização;
- **Não Repudiação:** a informação não pode ser negada pelo emissor ou receptor;
- **Privacidade:** Garantia total de que toda a informação pessoal (de cada colaborador) deve ser assegurada e mantida em sigilo em toda a ZEE EP.

5.2 Gestão de Riscos

A DTIC alinhada a DSV, deve proporcionar condições úteis para monitorizar os riscos associados a informação e comunicação, com vista a controlar e minimizar os impactos associados aos activos de informação e comunicação, adoptando as boas práticas e normas aplicáveis.

5.3 Monitorização, controle e auditoria

A rede, os sistemas, as informações e os serviços utilizados pelos utilizadores são de exclusiva propriedade da ZEE EP, não podendo ser interpretados como de uso pessoal. Visando efectivar esse controle, a ZEE EP poderá:

a) Implementar sistemas de monitorização em estações de trabalho, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de forma que a informação gerada ou trafegada por eles permita a sua rastreabilidade, identificando utilizador e respectivos acessos efetuados;

b) Tornar públicas as informações obtidas pelos sistemas de monitorização e auditoria no caso de exigência judicial, solicitação de coordenador ou gerente (ou autoridade superior), ou por determinação do COMITÊ DE SEGURANÇA DA INFORMAÇÃO;

c) Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

d) Instalar sistemas de protecção, preventivos e/ou repressivos, para garantir segurança das informações e dos perímetros de acesso;

e) Desinstalar a qualquer tempo, qualquer *software* ou sistema que represente risco ou esteja em desconformidade com políticas, normas, procedimentos e princípios vigentes.

6 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política de Segurança de Informação deve ser divulgada a todos os colaboradores da ZEE EP e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento por qualquer colaborador.

Os Procedimentos de Segurança da Informação ficarão disponíveis na rede interna da empresa, e devem ser divulgados às áreas directamente relacionadas à sua aplicação.

7 RESPONSABILIDADES

7.1 Gerais

Cabe a todos aos membros do CA, directores, colaboradores, estagiários, prestadores de serviço e terceirizados da ZEE EP:

a) Cumprir fielmente com a PSI;

b) Manter-se actualizado em relação a esta Política, demais normas e procedimentos relacionados, buscando informação junto ao seu superior ou

junto à autoridade competente, sempre que não estiver absolutamente seguro quanto a obtenção, uso e/ou descarte de informações;

c) Promover a segurança do seu usuário corporativo, departamental ou de rede local, bem como dos seus respectivos dados, credenciais de acesso e quaisquer informações a que tenha acesso em virtude do cargo que ocupa;

d) Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da ZEE EP, estando ciente de que sua estrutura não poderá ser utilizada para fins particulares e que quaisquer ações que tramitem em sua rede poderão ser auditadas;

e) Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela ZEE EP;

f) Cumprir as leis e as normas que regulamentam os aspectos da propriedade intelectual;

g) Comunicar imediatamente à DTIC qualquer incumprimento ou violação desta Política;

h) Ser responsável por qualquer prejuízo ou dano que vier a sofrer ou causar à ZEE EP., em decorrência da não obediência às directrizes e às normas referidas na PSI, nos procedimentos e política de comunicação, e aos procedimentos específicos dela decorrentes.

7.2 Comité de Segurança da Informação

A gestão da segurança da informação na ZEE EP. será realizada por um comitê multidisciplinar, denominado CSI, que é composto pela DTIC, DSV, DAC, DCM e DJUR. Compete ao CSI:

a) Propor normas relativas à segurança da informação e de comunicação;

b) Assessorar a implementação das acções de segurança da informação e comunicação da empresa;

c) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e de comunicação;

d) Analisar os casos de violação da PSI, encaminhando-os à autoridade competente, quando for o caso;

e) Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

f) Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;

g) Acompanhar o andamento dos principais projectos e iniciativas relacionados com à segurança da informação;

h) Propor a relação de "responsáveis" pelas informações da ZEE EP.

7.3 Direcção de Tecnologias da Informação e Comunicação (DTIC)

Compete à DTIC:

a) Propor ajustes, aprimoramentos e modificações de regras, em relação à Segurança da Informação;

b) Propor projectos e iniciativas relacionadas ao aperfeiçoamento da segurança da informação da ZEE EP, mantendo-se actualizada em relação às melhores práticas existentes no mercado e em relacção às tecnologias disponíveis;

c) Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso lógico da ZEE, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;

d) Prover todas as informações de gestão de segurança da informação solicitadas pelo CSI, podendo solicitar informações às demais áreas, caso necessário;

e) Prover ampla divulgação da PSI para todos os colaboradores da ZEE EP;

f) Oferecer orientação e treinamento sobre a PSI a todos os colaboradores da ZEE EP;

g) Realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da PSI;

h) Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações;

i) Estabelecer um mecanismo de registo e controlo de não-conformidades com a Política da Informação, solicitando que o CSI tome as providências

7.4 Adopção de Comportamento Seguro

Independentemente do meio ou da forma em que se encontra, a informação está presente no quotidiano de todos os colaboradores da ZEE EP. Portanto, é fundamental para a sua protecção que seja adoptado um comportamento seguro e condizente com o objectivo de proteger os activos informacionais da empresa, com destaque para os seguintes itens:

a) Todos os colaboradores e prestadores de serviços devem assumir uma atitude proactiva e engajada no que diz respeito à protecção das informações da ZEE EP;

b) Todos os colaboradores da empresa devem compreender as ameaças externas e internas que podem afectar a segurança da informação na empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, bem como engenharia social e outras artimanhas frequentemente utilizadas para a defraudar senhas e obter acesso a sistemas de informação;

c) Todos os recursos de informação da ZEE EP devem ser projectados e utilizados para a consecução dos objetivos finalísticos da empresa. É vedada a utilização desses recursos para fins particulares;

d) Toda informação produzida ou recebida pelos colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou actividade profissional contratada é de propriedade da empresa. Quaisquer excepções devem ser devidamente formalizadas;

e) Cada usuário é responsável pela segurança das informações dentro da ZEE EP;

f) Todo tipo de acesso à informação da ZEE EP que não for explicitamente autorizado é proibido;

g) As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não protegido;

h) Qualquer tipo de dúvida sobre a PSI deve ser imediatamente esclarecido com o CSI ou com a DTIC.

7.5 Controlo de Acesso

Todo acesso às informações e aos ambientes lógicos da ZEE EP, deve ser controlado, de forma a garantir permissão apenas às pessoas autorizadas pelo respectivo proprietário da informação, observando as seguintes directrizes:

a) Procedimento formal de concessão e cancelamento de autorização de acesso aos sistemas de informação;

b) Comprovação da autorização do proprietário da informação;

c) Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas acções;

d) Verificação se o nível de acesso concedido é apropriado ao propósito da actividade exercida e se é consistente com a PSI;

e) Remoção imediata de autorizações dadas a usuários afastados ou que terminaram seu vínculo contratual com ZEE EP, ou que tenham mudado de função;

f) Processo de revisão periódica das autorizações concedidas;

g) Política de atribuição, manutenção e uso de senhas;

h) O controle de acesso deverá considerar e respeitar o princípio do menor privilégio, em que cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas tarefas.

7.6 Uso e Acesso à Internet e à Intranet

A utilização dos recursos informacionais da empresa deve ser pautada de forma ética e profissional, sempre priorizando a proteção dos activos de informação da ZEE EP.

a) O uso de recursos e serviços de TI da empresa é restrito aos colaboradores da ZEE EP e usuários externos credenciados e autorizados, sendo vedada a sua utilização fora dessas condições;

b) A ZEE EP poderá, a qualquer momento e sem aviso prévio aos usuários, bloquear, restringir, filtrar, monitorizar, capturar, controlar ou auditar todos os recursos e os serviços de TI que no âmbito da empresa, estejam eles nas estações de trabalho ou nos servidores de rede, visando assegurar o cumprimento da PSI;

c) É proibido o uso de recursos computacionais e de comunicação da ZEE EP para disseminação de conteúdo protegido por direitos autorais, ilegais, via *Torrent*, FTP ou qualquer outro mecanismo de compartilhamento de arquivos;

d) É proibido o uso de *Internet* para acesso de conteúdos que não estejam relacionados às actividades laborais, sendo prerrogativa do CA a avaliação da liberação de acessos a sites bloqueados;

e) É proibida a concessão de privilégio de administrador local aos computadores, salvo quando expressamente autorizada, de acordo com os critérios técnicos por ela definidos;

f) Possíveis excepções de privilégios para acesso a ambientes bloqueados devem ser solicitadas formalmente e somente serão liberadas após avaliação e autorização da DTIC, que terá a responsabilidade da gestão das excepções;

g) É proibida, sob qualquer alegação ou pretexto, o uso de qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a acção dos sistemas de segurança da informação implementados na ZEE EP;

h) Falhas de segurança da informação percebidas pelos usuários deverão ser comunicadas à DTIC imediatamente para que sejam tomadas as devidas providências;

i) Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por colaboradores da empresa.

7.7 Uso do Correio Electrónico

O correio eletrônico é uma ferramenta de trabalho disponibilizada para todos os usuários da ZEE EP, independentemente de seu vínculo funcional. Dessa forma, ela deverá ser utilizada somente para fins corporativos e relacionados às actividades do colaborador, sendo proibida a sua utilização para tratar de assuntos de cunho pessoal.

7.8 Uso das Mídias Sociais

O uso de mídeas sociais, deve ser de responsabilidade da DCM alinhada a DTIC, de modos a garantir a comunicação segura e estratégica podendo alcançar o maior número de pessoas. Qualquer informação relacionada a ZEE EP, apenas deve ser divulgada pela DCM.

7.9 Uso da Impressora

Seguem as regras que devem ser observadas por todos os colaboradores aquando da utilização deste equipamento:

- Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;
- O seu uso deve ser apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;
- As impressoras são ferramentas para fins profissionais, com o objectivo de aumentar a produtividade nas actividades desenvolvidas pela ZEE EP.
- Impressões coloridas apenas devem ser feitas em carácter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

7.10 Protecção Contra Softwares Maliciosos

a) Os Recursos tecnológicos devem estar sempre munidos de soluções de detecção e bloqueio de programas de código malicioso *antispyware*, programas antivírus, programas de análise de conteúdo de correio eletrônico e de acesso à Internet;

b) A instalação e a configuração da solução de detecção e bloqueio de programas maliciosos somente devem ser realizadas pela DTIC;

c) Tais softwares devem ser licenciados e actualizados constantemente, e a sua execução deve ser agendada para ocorrer periodicamente, fazendo uma varredura completa nas estações de trabalho ou dispositivos móveis da empresa;

d) Qualquer mídia removível de origem duvidosa ou não autorizada deve ser avaliada quanto à presença de vírus ou outros *softwares* maliciosos antes de ser utilizada. Arquivos recebidos por correio eletrônico também devem ser inspecionados;

e) É proibida a instalação de *softwares* (programas) nos computadores da empresa sem o prévio conhecimento e autorização da área responsável. Os

usuários devem fazer uso apenas de *softwares* licenciados e homologados pela DTIC.

7.11 Datacenter (centro de processamento de dados)

a) O datacenter deverá ser mantido fechado com o sistema de controlo de acesso e monitorizado 24 horas ao dia, 07 dias por semana, e o seu acesso somente a pessoas autorizadas;

b) Quando houver a necessidade de entrada de terceiros no interior do datacenter, o acesso deve ser realizado com a presença de um colaborador da DTIC;

c) Imediatamente após o desligamento de usuários que possuam acesso ao data center, deve ser providenciada a sua exclusão da relação de pessoas autorizadas para realizarem o acesso às suas instalações;

d) A função de administrador do datacenter deve ser atribuída exclusivamente a um colaborador efetivo, preferencialmente vinculado à área de Infraestrutura de TI.

7.12 Backup (cópia de segurança)

a) A realização do *backup* institucional consiste no armazenamento da cópia dos dados contidos nos computadores servidores da ZEE EP. A realização de *backup* dos dados contidos nas estações de trabalho é da responsabilidade de cada usuário. A empresa não se responsabiliza por nenhum conteúdo presente nas máquinas utilizadas pelos usuários;

b) Todos os documentos pertinentes às actividades institucionais da ZEE EP, devem ser armazenados nos servidores da empresa. Tais arquivos, se gravados apenas localmente nos computadores dos usuários, não serão incluídos na rotina de *backup* e poderão ser perdidos caso ocorra uma falha na máquina, situação em que a responsabilidade será inteiramente do utilizador, podendo ele ser responsabilizado por quaisquer prejuízos à empresa;

c) Arquivos pessoais e/ou não pertinentes às actividades institucionais da ZEE EP, (fotos, músicas, vídeos, entre outros) não devem ser copiados ou movidos para os *drives* de rede. Caso identificados, esses arquivos poderão ser excluídos sem a necessidade de comunicação prévia ao utilizador;

d) É proibido o armazenamento de informações corporativas, tais como bases de dados, arquivos, ou demais documentos em locais inadequados, tais como serviços de armazenamento em nuvem, computadores pessoais ou servidores de prestadores de serviço, salvo com a autorização expressa da DTIC.

7.12 Violações da Política De Segurança Da Informação E Sanções

O incumprimento ou a inobservância de quaisquer regras ou directrizes definidas nesse instrumento e nas suas normas complementares constituem falta grave, sobre as quais a ZEE EP., aplicará todas as medidas cabíveis nos âmbitos administrativo, civil e judicial.

São considerados comportamentos contrários à PSI:

a) Qualquer comportamento comissivo ou omissivo no tratamento das informações, na guarda e no manuseio dos sistemas e das redes de computadores e dados que lesem a ZEE EP, quem nela trabalha ou terceiros;

b) Apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, dados, programas de computador, documentos físicos ou quaisquer outros de forma indevida ou não autorizada;

c) Obter, manter ou fornecer a terceiro acesso de forma indevida ou não autorizada a dados, instrução, computador, rede de computadores, ambientes ou qualquer meio de identificação, tais como crachás, senhas, *logins*, entre outros;

d) Obter segredos, informações sigilosas ou dados pelos quais o usuário não possui acesso, armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, bem como documentos físicos, de forma indevida ou não autorizada;

e) Criar, desenvolver ou inserir dados ou programas em computadores ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar,

destruir, inutilizar ou modificar dados ou programas de computador, ou de qualquer forma a dificultar ou impossibilitar, total ou parcialmente, a utilização de computadores ou rede de computadores;

f) Realizar *download* e *upload* de jogos, filmes, conteúdo pornográfico, bem como de qualquer outro programa que atenda única e exclusivamente aos interesses do usuário e não da empresa;

g) Distribuir cópia não autorizada de arquivos, informações, *software* ou qualquer outro activo da empresa;

h) Utilizar o serviço de correio eletrônico para envio de mensagens com teor político/partidário, racista, comercial, preconceituoso, pornográfico, pejorativo, publicitário ou com outros fins não pertinentes às actividades da empresa;

i) Valer-se de qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a acção dos sistemas de segurança da informação implementados;

j) Agir em desacordo com padrões e procedimentos específicos de utilização dos recursos e serviços de rede corporativa.

7.13 Considerações Finais

Para a uniformização da informação organizacional, esta PSI deve ser distribuída a todos colaboradores, prestadores de serviços e fornecedores da ZEE EP, a fim de que seja conhecida e cumprida.

Luanda, aos 10 de Outubro de 2024.

O Presidente do
Conselho de Administração

Sociedade de Desenvolvimento da Zona Económica Especial LUANDA • BENGO NIF: 5401176452

Manuel Francisco Pedro