DESENVOLVIMENTO DO MANUAL DE OPERAÇÕES

Estudo de viabilidade sobre cibersegurança e dados
Modelos de governação da proteção, funcionamento
Capacidade manual e de cibercriminalidade
Reforçar o apoio na Guiné-Bissau

Para
Programa Regional de Integração Digital da África Ocidental Guiné-Bissau

GoSecure

Criado por :
BS Innovations e GoSecure
09/2024

ÍNDICE DE CONTEÚDO

LISTA DE FIGURAS

LISTA DE QUADROS

DEFINIÇÃO DE ACRÓNIMOS

EPI	Equipamento de proteção individual
ILP	Invalidez a longo prazo
BCP	Plano de Continuidade do Negócio
DRP	Plano de recuperação de desastres
IRT	Equipa de resposta a incidentes
SIEM	Gestão de informações e eventos de segurança
IDS/IPS	Sistemas de deteção/prevenção de intrusões
DSARs	Pedidos de acesso do titular dos dados
DPIA	Avaliações de impacto sobre a proteção de dados
EP	Empresas Públicas
PIR	Revisão Pós-Incidente
IOCs	Indicadores de Compromisso
PIAs	Plataformas de informação sobre ameaças
OSINT	Inteligência de fonte aberta
HUMINT	Inteligência humana
ISACs	Centros de Análise e Partilha de Informação
PUA	Política de utilização aceitável
RBAC	Controlo de acesso baseado em funções
MFA	Autenticação multi-fator
PAM	Gestão de Acesso Privilegiado
DPAs	Autoridades de Proteção de Dados
CPD	Comissão de Proteção de Dados
DPOs	Responsáveis pela proteção de dados
CEDEAO	Comunidade Económica dos Estados da África Ocidental
UE	União Europeia
GDPR	Regulamento Geral sobre a Proteção de Dados
TIC	Tecnologias da Informação e da Comunicação
IGF	Fórum de Governação da Internet
IT	Tecnologias da informação
ANPD	Agência Nacional de Proteção de Dados
COS	Centro de Operações de Segurança
SOPs	Procedimentos Operacionais Normalizados
WARDIP	Programa Regional de Integração Digital da África Ocidental

I. INTRODUÇÃO

Reconhecendo a necessidade de a Guiné-Bissau desenvolver uma economia digital, ao mesmo tempo que se alinha e integra num mercado digital regional da África Ocidental e internacional, o Banco Mundial (BM) está a financiar a preparação do Programa de Integração Digital Regional da África Ocidental (WARDIP) - Guiné-Bissau.

O objetivo do programa WARDIP - Guiné-Bissau é liderar a transformação digital em todo o país. Apoiará o desenvolvimento de modelos de governação, políticas e regulamentos nacionais, bem como a implementação de programas estratégicos que devem ser melhorados para eliminar os obstáculos à conectividade transfronteiriça dos fluxos e serviços de dados digitais. Deste modo, permitirá a emergência de um sistema nacional e regional integrado e competitivo, posicionando o país de forma vantajosa na região africana e a nível mundial, promovendo simultaneamente a inovação e a prosperidade.

Nos últimos anos, a Guiné-Bissau registou um rápido progresso tecnológico e uma maior penetração da Internet. Com a crescente dependência das tecnologias de informação e comunicação (TIC), o país enfrenta um risco acrescido de ameaças e vulnerabilidades cibernéticas. Reconhecendo a importância da cibersegurança e da proteção de dados para garantir a segurança dos cidadãos, das empresas e das infraestruturas críticas, foi criado o projeto WARDIP. Estes desafios exigem respostas múltiplas, reunindo o governo, o setor privado e a sociedade civil para enfrentar os desafios da cibersegurança e da governação da privacidade. A tónica é colocada no alinhamento com as realidades políticas nacionais e no cumprimento dos requisitos regulamentares regionais e internacionais. No centro da iniciativa está a facilitação das ligações transfronteiriças e o fluxo contínuo de dados entre as economias digitais regionais africanas e os mercados internacionais no ecossistema digital.

O estabelecimento de um modelo de governação robusto, que engloba elementos essenciais como a estrutura, os mecanismos de supervisão, as políticas e os processos, é fundamental para alcançar estes objetivos. Prevê-se que esta base estimule a criação de emprego e atrair investimentos para o país.
A fase inicial do projeto, Etapa 1, consistiu na realização de um estudo de viabilidade dos modelos de governação da cibersegurança e da proteção de dados. A segunda fase do projeto, Etapa 2, consistiu em prestar assistência ao Governo da Guiné-Bissau na conceção das agências de proteção de dados e de cibersegurança, fornecendo aconselhamento e conhecimentos especializados. A terceira fase do projeto, Etapa 3, consiste na elaboração de um manual de operações abrangente para as agências de proteção de dados e de cibersegurança recentemente criadas. Começaremos por definir o que é um manual de operações, o que deve incluir e o seu ciclo de vida. Em seguida, definiremos os componentes do manual de operações, incluindo as atividades de acompanhamento e as normas de qualidade. Este manual servirá como um farol de orientação para as agências de proteção de dados e de cibersegurança.

II. O PLANO DE CRIAÇÃO E O CICLO DE VIDA DO MANUAL DE OPERAÇÕES

1. Definição do manual de instruções

Um manual de operações é um documento que fornece orientações aos funcionários e outras partes interessadas para que desempenhem correta e eficientemente as suas funções numa organização. Descreve as normas, procedimentos, políticas e protocolos de incidentes aprovados pela organização.

À medida que navegamos através das complexidades da proteção de dados e da cibersegurança, este manual de operações constitui uma pedra angular da excelência operacional das agências, incorporando a sua dedicação à manutenção da integridade, confidencialidade e disponibilidade dos dados num cenário cibernético em constante evolução.

2. Estabelecimento e aprovação

A elaboração de um manual de operações dependerá do tipo de operação. Identificámos os seguintes tipos de operações:

- **Operações a nível da empresa:** por exemplo, o processo de contratação, o plano de continuidade das atividades.

- **Operações de nível técnico:** por exemplo, o processo para emitir a autorização de recolha de dados privados ou o processo para monitorizar a rede e alertar em caso de problemas.

O manual de operações deve ser aprovado por um gestor, um gestor de topo ou um diretor, ou pelo diretor-geral. Por exemplo, um manual para toda a empresa deve ser aprovado pelo Diretor-Geral, enquanto um manual técnico ou específico de um setor deve ser aprovado pelo responsável desse setor

3. Atualizações responsáveis

A responsabilidade pela elaboração de um manual de operações recai normalmente sobre os gestores de topo e os chefes de departamento de uma organização. Estes são responsáveis por garantir que o manual reflete as políticas, os procedimentos e as normas operacionais da organização. No caso das agências de proteção de dados e de cibersegurança, o manual de operações é da responsabilidade do diretor-geral de cada agência, que aprova a sua criação e manutenção. Uma vez elaborado, o manual é mantido com a colaboração dos diretores de serviço para garantir a sua pertinência e precisão permanentes. Isto permite a incorporação de quaisquer alterações nos procedimentos, na tecnologia ou nos regulamentos, e assegura que o manual continua a ser um recurso fiável para os funcionários e outras partes interessadas. O manual de operações será revisto e atualizado pelo menos uma vez por ano ou mais frequentemente em caso de alterações significativas.

4. Análise jurídica e conformidade do manual de operações

O manual de operações pode ser elaborado em colaboração com peritos técnicos e responsáveis pela conformidade, a fim de garantir que cumpre as normas legais e regulamentares. Este aspeto é obrigatório para garantir que todas as operações são efetuadas em conformidade com a legislação e os regulamentos da Guiné-Bissau. Por exemplo, a agência de proteção de dados não deve realizar operações que entrem em conflito com as disposições da Constituição da Guiné-Bissau.

5. Publicação e distribuição

Para que um manual de operações seja útil, deve ser distribuído às pessoas que o vão utilizar e estas devem ter a versão atualizada. Eis os passos a seguir para garantir a publicação e distribuição efectivas do manual de operações.

Controlo de versão	Cada iteração do manual de operação será claramente numerada e datada. A versão mais atual será disponibilizada a todos os colaboradores, sendo que as versões anteriores serão arquivadas para consulta.
Aprovação	Antes da publicação, o manual de operação será revisto e aprovado pelo diretor geral.
Distribuição	O manual de operação será distribuído eletronicamente a todos os colaboradores através da intranet das agências. Uma cópia impressa também pode ser fornecida mediante pedido. O funcionário será notificado por e-mail assim que o manual for estabelecido.
Acessibilidade	O manual de operação será disponibilizado a todos os colaboradores e serão feitos esforços para acomodar necessidades especiais, como a disponibilização do manual em diversos formatos ou em inglês, se necessário.
Confidencialidade	O manual de operação pode conter informações confidenciais. Os colaboradores são obrigados a usarem o manual com cuidado e a não o partilhar com pessoas não autorizadas.
Formação	Após a distribuição, serão realizadas formações para familiarizar os colaboradores com o conteúdo do manual e como utilizá-lo de forma eficaz. As sessões de formação irão enfatizar a importância da adesão aos procedimentos descritos.
Feedback	Os colaboradores são encorajados a fornecer feedback sobre o manual de operação. Este feedback será considerado durante o processo periódico de revisão e atualização do manual.
Atualizações	O manual de operação será revisto pelo menos uma vez por ano ou com maior frequência, se necessário, e as atualizações serão publicadas, distribuídas e notificadas seguindo o mesmo processo descrito acima.
Manutenção de registos	Será mantido um registo da lista de distribuição para garantir que todos os colaboradores receberam a versão mais recente do manual.

Figura 01: Etapas da publicação e distribuição do manual de operações

6. Informações de contacto

Para quaisquer questões ou informações adicionais relativas ao manual de instruções, contactar as seguintes pessoas :

- Agência de proteção de dados

Eis a lista de pessoas que devem constar da lista de contactos:

- Diretor Geral
- Diretor de Regulamentação e Conformidade
- Diretor de Recursos
- Serviço de apoio informático (no seu cartão de informação, deve ser mencionado "Disponível 24 horas por dia, 7 dias por semana para questões urgentes", quando aplicável)

Para cada pessoa de contacto ou serviço, deve ser preenchido o cartão de informação de contacto. Na seção X do presente relatório é fornecido um modelo do cartão de informação.

- Agência para a cibersegurança

Eis a lista de pessoas ou serviços que devem constar da lista de contactos:

- Diretor Geral
- Diretor de Departamento de Estratégia e Política
- Chefe de Departamento de Resposta a Emergências
- Chefe de Departamento de Recursos
- Serviço de apoio informático (no seu cartão

de informação, deve ser mencionado "Disponível 24 horas por dia, 7 dias por semana para questões urgentes", quando aplicável)

Para cada pessoa de contato ou serviço, deve ser preenchido o cartão de informação de contacto.

Na seção X do presente relatório é fornecido um modelo do cartão de informação.

Contate o contato adequado para obter assistência em secções específicas do manual de operações ou para questões de carácter geral.

III. COMPONENTES DO MANUAL DE INSTRUÇÕES

1. Organigrama

A. Estrutura organizativa da agência

Tal como apresentado no produto 2, cada agência tem a sua própria estrutura. O organograma abaixo descreve a estrutura da Agência Nacional de Proteção de Dados, criada para salvaguardar a privacidade dos dados em todo o país.

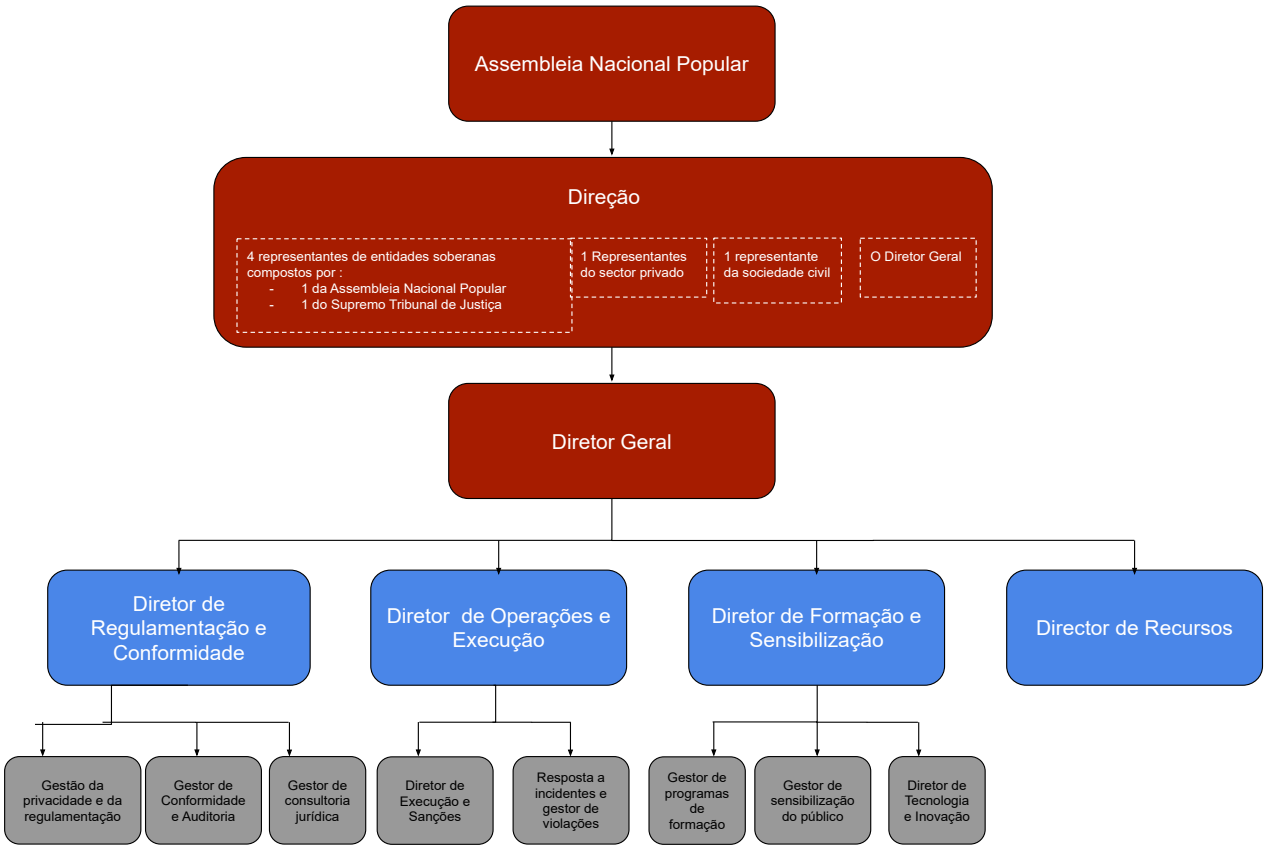

Figura 02 : Organograma da agência de proteção de dados

A descrição da função e os detalhes relacionados com este diagrama estão disponíveis no documento 2 deste projeto.

Agência para a Cibersegurança, criada para garantir um ecossistema digital seguro e resiliente.

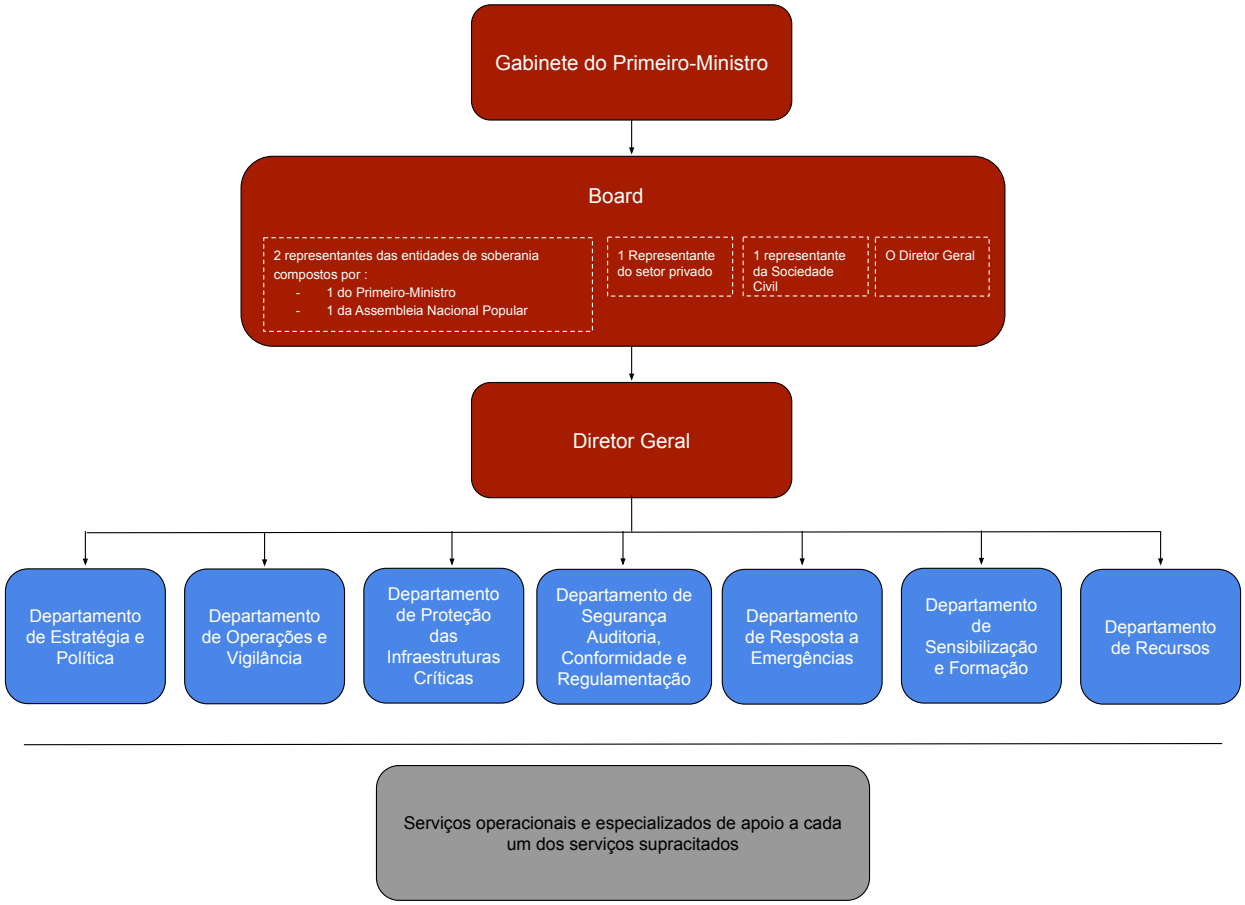

Figura 03: Organograma da agência de cibersegurança

Para mais pormenores sobre cada posição nos diagramas anteriores, consultar o documento 2.

Uma vez que estamos a centrar-nos no manual de operações, a próxima seção irá expor o RACI em concordância com os diagramas.

B. Funções e responsabilidades dos membros das agências (RACI)

Nesta seção, apresentaremos o RACI relacionado com o manual de operações. Começaremos por explicar cada responsabilidade no acrónimo RACI:

- **"R"** de Responsável : é o responsável pela realização da atividade
- **"A"** de Accountable (responsável): aquele que é responsável pelo progresso. É responsável por quaisquer falhas no desempenho da atividade.
- **"C"** para recurso a consultar: pessoa a consultar em relação à atividade.
- **"I"** para recurso a informar: pessoa a informar em relação à atividade.

Para podermos completar o RACI, vamos identificar as funções-chave em relação ao ciclo de vida do manual de operações. As etapas apresentadas na secção ***"II.5 Publicação e distribuição"*** acima foram identificadas como a função-chave do ciclo de vida do manual de operações. Apresentamos de seguida o RACI para cada agência.

RACI para a agência de proteção de dados

O seguinte RACI é feito partindo do princípio de que os manuais de operações sectoriais técnicas e a nível da empresa estão juntos.

	Empregado	Diretor geral	Diretor de Regula-mentação e Conformidade	Diretor de Funciona-mento e Execução	Diretor de Formação e Sensibilização	Diretor de Recursos
Controlo de versões	I		I	I	R	A
Aprovação		R,A	C,I	C,I	C,I	C,I
Distribuição			R	R	A	R
Acessibilidade					A	C
Confidenciali-dade	R	A	C			
Formação	I				R,A	
Feedback	R	I			I	A
Atualização	I		R	R	R,A	R
Manutenção de registos	I				R	A

Quadro 01: RACI para a agência de proteção de dados

RACI para a agência de cibersegurança

O seguinte RACI é feito partindo do princípio de que os manuais de operações sectoriais técnicas e a nível da empresa estão juntos.

	Empregado	Diretor geral	Chefe de outro serviço técnico	Chefe do Departamento de Auditoria de Segurança, Conformidade e Regulamentação	Chefe do departamento de sensibiliza-ção e formação	Chefe do departamento de recursos
Controlo de versões	I		I	I	R	A
Aprovação		R,A	C,I	C,I	C,I	C,I
Distribuição			R	R	A	R
Acessibilidade					A	C
Confidenciali-dade	R	A	C			
Formação	I				R,A	
Feedback	R	I			I	A
Atualização	I		R	R	R,A	R
Manutenção de registos	I				R	A

Quadro 02: RACI para a agência de cibersegurança

O RACI também pode ser implementado para cada operação identificada no manual. Ajudará a identificar facilmente quem é responsável por fazer o quê.

2. Políticas

A. Políticas e orientações gerais

Entende-se por política os requisitos obrigatórios impostos a cada organização governamental que devem ser cumpridos o mais rigorosamente possível. As orientações são apenas de carácter consultivo e devem apoiar as equipas no cumprimento dos seus objectivos estratégicos.

As políticas gerais estabelecem as bases da cultura operacional e da conformidade legal da agência. Asseguram que todos os funcionários e partes interessadas compreendem as regras que orientam as funções da agência.

O objetivo final é servir de guia para que as agências possam desenvolver abordagens e implementar soluções para proteger as infraestruturas nacionais contra as ciberameaças, responder e recuperar de ciber incidentes em tempo útil e, por conseguinte, resistir a novas ameaças sem perturbações significativas.

É essencial delinear os elementos-chave que orientarão as operações da agência, estabelecer expectativas claras e fornecer um quadro para uma tomada de decisões coerente a todos os níveis da organização:

- Quadro para a tomada de decisões: Isto envolve a criação de uma abordagem padronizada para a tomada de decisões dentro da agência, garantindo consistência, justiça e alinhamento com os objetivos nacionais.
- Conformidade legal: A agência deve cumprir todas as leis nacionais relevantes, acordos internacionais e normas do sector. Isto inclui revisões regulares para garantir que a agência se mantenha em conformidade com a evolução dos quadros jurídicos.
- Consistência operacional: Assegura que todos os processos e atividades da agência seguem os mesmos princípios, conduzindo a uma abordagem operacional unificada e coerente.
- Revisão periódica e atualizações: As políticas e o próprio manual devem ser revistos periodicamente (por exemplo, anualmente) para refletir novos desafios, atualizações legais ou alterações operacionais. Uma equipa ou comité específico deve ser responsável por esta revisão, garantindo que o manual continua a ser um documento vivo que evolui com as necessidades da agência.
- Código de conduta: O código estabelecerá expectativas claras de comportamento ético e profissional para todos os funcionários da agência. O Código de Conduta é um conjunto de princípios e diretrizes que definem os comportamentos esperados e as normas éticas para todos os funcionários, contratantes e partes interessadas associados à Agência Nacional de Cibersegurança ou à Agência Nacional de Proteção de Dados. Este Código foi concebido para promover um ambiente de integridade, respeito e profissionalismo, garantindo que a agência funciona de forma a manter a confiança do público e a cumprir a sua missão de proteger a cibersegurança nacional. Os principais elementos do código de conduta serão :
  - *Integridade e honestidade*
  - *confidencialidade*
  - *conflito de interesses*
  - *utilização dos recursos da agência*
  - *cumprimento das leis e regulamentos*
  - *respeito e profissionalismo*
  - *comunicação de má conduta*

i. Políticas/orientações em matéria de cibersegurança

As políticas e diretrizes de cibersegurança são componentes essenciais da estratégia global de segurança de uma organização, em particular para uma Agência Nacional de Cibersegurança. Estes documentos estabelecem as regras, práticas e procedimentos que os funcionários, contratantes e partes

interessadas devem seguir para proteger os sistemas de informação, dados e redes da organização contra ciberameaças.

Estas políticas de cibersegurança são inestimáveis para outras entidades governamentais e privadas, uma vez que fornecem um quadro sólido para melhorar a segurança, garantir a conformidade e promover a colaboração. Ao adotarem políticas semelhantes, as organizações podem normalizar as suas práticas de cibersegurança, o que é crucial para proteger as infraestruturas críticas e os dados sensíveis das ciberameaças. Estas políticas também facilitam a utilização eficiente dos recursos, melhoram a preparação e a resposta a incidentes e garantem a continuidade do negócio, minimizando o tempo de inatividade e as perdas económicas durante as interrupções. Além disso, ajudam a criar confiança pública e resiliência organizacional, tornando-as modelos adaptáveis para que entidades de todas as dimensões reforcem a sua postura geral de cibersegurança. Segue-se uma descrição pormenorizada das principais políticas e diretrizes de cibersegurança:

- **Política de controlo de acesso:** A política de controlo de acesso garante que apenas o pessoal autorizado tem acesso aos sistemas de informação e aos dados da organização. Para aplicar esta política de controlo de acesso, os princípios e atividades principais incluem o controlo de acesso baseado em funções (RBAC), a autenticação multi factor (MFA), o princípio do privilégio mínimo, um bom programa de gestão de acesso privilegiado (PAM) e revisões regulares do acesso.

- **Política de resposta a incidentes :**
A política de resposta a incidentes estabelece procedimentos estruturados e diretrizes para a identificação, gestão e mitigação de incidentes de cibersegurança. O principal objetivo desta política é garantir que a agência possa responder a incidentes de segurança de forma rápida e eficaz, minimizando potenciais danos, preservando provas para análise e mantendo a continuidade operacional.
Esta política é uma componente essencial da estratégia global de segurança da Agência Nacional de Cibersegurança. Desempenha um papel fundamental para garantir que a agência possa proteger a infraestrutura digital nacional, manter a confiança do público e salvaguardar os dados sensíveis das ciberameaças.
Eis os principais elementos desta política:

  - ***Deteção e comunicação de incidentes***
    Esta secção da política explica como a agência identificará potenciais incidentes de segurança e como estes devem ser comunicados. Inclui os métodos e ferramentas utilizados para monitorizar o ambiente de TI da agência (por exemplo, SIEM) e define os protocolos para a forma como os funcionários ou os sistemas automatizados devem comunicar atividades suspeitas. Esta secção também destaca a forma como a outra entidade governamental ou privada comunicará incidentes. Definiremos os passos para a comunicação de um incidente, incluindo a quem comunicar, as informações a incluir e a rapidez com que as comunicações devem ser efectuadas.

  - ***Equipa de resposta a incidentes (IRT)***
    Esta seção descreve e designa a equipa responsável pelo tratamento de incidentes. Descreve as funções e responsabilidades específicas da equipa, tais como quem lidera a resposta, quem efectua a análise forense e quem comunica com as partes interessadas.

  - ***Classificação de incidentes***
    Esta seção explica como os incidentes serão

classificados e priorizados com base na sua gravidade e potencial impacto. A classificação dos incidentes ajuda a agência a dar prioridade aos recursos e às respostas de forma adequada.

- ***Contenção e Erradicação***
  Esta seção descreve as medidas que a agência tomará para conter um incidente em curso e erradicar a causa subjacente. A contenção impede a propagação do ataque, enquanto a erradicação elimina a ameaça do ambiente.

- ***Recuperação e análise pós-incidente***
  Esta secção abrange a forma como a agência restabelecerá as operações normais após um incidente e efetuará uma análise exaustiva para compreender o que aconteceu e como o evitar no futuro.

• ***Política de segurança da rede :***
Esta política descreve as medidas e os controlos necessários para proteger a integridade, a confidencialidade e a disponibilidade da infraestrutura de rede da agência. Garante que todas as atividades da rede são seguras e que a rede está protegida contra o acesso não autorizado, a utilização indevida e as ciberameaças. A política de segurança da rede é essencial para salvaguardar a infraestrutura digital da agência.
Inclui a definição de controlos de acesso, em que são concedidas permissões aos utilizadores com base nas suas funções e no princípio do menor privilégio. A política também obriga à segmentação da rede, garantindo que diferentes partes da rede são isoladas para conter potenciais ameaças. Além disso, descreve a implementação de firewalls e sistemas de deteção/prevenção de intrusões (IDS/IPS) para monitorizar e filtrar o tráfego da rede, bem como a utilização de encriptação para proteger os dados em trânsito. A monitorização contínua da rede é uma componente essencial, permitindo a deteção de atividades suspeitas e respostas rápidas a potenciais ameaças.

• ***Política de proteção de dados e de encriptação :***
A política de proteção e encriptação de dados centrar-se-á na segurança das informações sensíveis ao longo do seu ciclo de vida. Começa com a classificação dos dados, categorizando-os com base na sensibilidade, e especifica as normas de encriptação para proteger os dados em repouso, em processo e em trânsito.
A política também especificará as práticas de gestão de chaves para garantir que as chaves de cifragem são geradas, armazenadas e retiradas de forma segura.
Serão fornecidas diretrizes para o tratamento e armazenamento de dados, incluindo soluções de armazenamento seguro e medidas de segurança física. Os controlos de acesso são cruciais, limitando o acesso aos dados ao pessoal autorizado e assegurando que o acesso é registado e monitorizado.

• ***Política de sensibilização e formação dos utilizadores :***
A Política de Formação e Sensibilização dos Utilizadores garante que todos os funcionários da agência são informados sobre os riscos de cibersegurança e estão equipados com os conhecimentos necessários para proteger os sistemas de informação da agência. Esta política foi concebida para cultivar uma cultura de sensibilização para a segurança na agência.
Exige programas de formação obrigatórios para todos os funcionários, abrangendo tópicos fundamentais de cibersegurança como phishing, gestão de palavras-passe e engenharia social. Também é ministrada formação específica para funcionários em cargos com responsabilidades de segurança

acrescidas.
A política inclui simulações regulares de phishing para testar e reforçar a capacidade dos funcionários de reconhecer ameaças. As campanhas contínuas de sensibilização para a segurança mantêm a cibersegurança no topo das atenções, enquanto as avaliações regulares da eficácia da formação garantem uma melhoria contínua.
Eis alguns passos para o construir:

- ***Desenvolver módulos de formação :***
  Criar ou obter conteúdos de formação adaptados às necessidades da agência, incluindo conteúdos gerais de sensibilização para a cibersegurança e conteúdos específicos para cada função.

- ***Implementar formação regular :***
  Estabelecer um calendário para as sessões obrigatórias de formação sobre cibersegurança, assegurando que todos os funcionários participam regularmente.

- ***Executar simulações :***
  Planear e executar simulações de phishing e outros ataques simulados para avaliar as respostas dos funcionários e reforçar a formação.

- ***Avaliar e melhorar :***
  Avaliar continuamente a eficácia dos programas de formação e introduzir melhorias com base no feedback e nos dados de incidentes.

• **Política de gestão de vulnerabilidades :**
A política de gestão das vulnerabilidades garante que a agência identifica e trata proativamente os pontos fracos da segurança. Inclui a análise regular das vulnerabilidades dos sistemas, redes e aplicações, utilizando ferramentas automatizadas. A gestão de correções é uma componente crítica, com processos estruturados para dar prioridade, testar e aplicar correções prontamente.

A política descreve a forma como as vulnerabilidades são avaliadas com base na gravidade e no impacto, orientando a prioridade dos esforços de correção. A documentação e os relatórios são enfatizados, assegurando que todas as vulnerabilidades identificadas e as ações de atenuação são cuidadosamente registadas.
Eis os elementos-chave desta política:

- **Análise regular de vulnerabilidades :**
  A análise regular permite à organização identificar proativamente as vulnerabilidades antes de estas poderem ser exploradas pelos atacantes. Esta deteção precoce é fundamental para manter um ambiente seguro.

- **Gestão de Patches :**
  Um processo de gestão de patches bem definido garante que os patches de segurança são aplicados prontamente, reduzindo o período de tempo durante o qual os sistemas são vulneráveis a ataques.

  Esta política define passos claros para testar e implementar correções, o que minimiza o risco de introdução de novos problemas durante o processo de correção e garante que os sistemas permanecem estáveis e seguros.

- **Avaliação da vulnerabilidade e definição de prioridades :**
  Esta secção garante que a organização concentra os seus recursos nas vulnerabilidades mais críticas em primeiro lugar, reduzindo o risco global de forma mais eficaz. A definição de prioridades com base na gravidade e no impacto potencial permite que a agência trate rapidamente das vulnerabilidades mais perigosas.

Nem todas as vulnerabilidades podem ser corrigidas imediatamente, pelo que a definição de prioridades permite à organização afetar recursos de forma mais eficiente, resolvendo primeiro os problemas de alto risco e gerindo as vulnerabilidades de menor risco ao longo do tempo.

- **Remediação e atenuação :**
  Passos claros de correção e tratamento garantem que as vulnerabilidades não são apenas identificadas, mas também devidamente tratadas. Isto reduz a probabilidade de exploração. Quando a correção imediata não é possível, as estratégias de atenuação ajudam a reduzir o risco até que possa ser implementada uma solução permanente. Isto garante uma proteção contínua, mesmo quando as correções são adiadas.
  Isto garante uma proteção contínua mesmo quando as correções são atrasadas.

- **Relatórios e documentação :**
  A documentação pormenorizada do processo de gestão da vulnerabilidade assegura a responsabilização dentro da agência. Permite que as partes interessadas compreendam quais as ações que foram tomadas e o que falta fazer.

  A elaboração regular de relatórios e a documentação exaustiva ajudam a cumprir os requisitos regulamentares e a passar nas auditorias de segurança. Esta transparência é também fundamental para a melhoria contínua, uma vez que fornece um registo do que tem sido eficaz e do que precisa de ser melhorado.

- **Melhoria contínua :**
  Com uma melhoria contínua, garantimos que o processo de gestão de vulnerabilidades evolui com o cenário de ameaças. Esta secção promove a utilização de novas ferramentas, técnicas e melhores práticas no âambito da estrutura existente. A documentação das lições aprendidas com vulnerabilidades e incidentes passados garante que a abordagem da organização à gestão de vulnerabilidades melhora ao longo do tempo, reduz a probabilidade de repetição de problemas e aumenta a segurança geral.

- **Política de recuperação de desastres e de continuidade das atividades**

Esta política garante a resiliência da agência face a perturbações. Inclui um Plano de Recuperação de Catástrofes (DRP) pormenorizado para restaurar os sistemas e dados informáticos, bem como um Plano de Continuidade da Atividade (BCP) para manter as operações críticas durante uma catástrofe. A política descreve os procedimentos de cópia de segurança e restauro para garantir que os dados possam ser rapidamente recuperados com um tempo de inatividade mínimo. Está também incluído um plano de comunicação de emergência para orientar a forma como a agência irá comunicar com os funcionários, as partes interessadas e o público durante uma crise. A realização de testes e simulacros regulares é essencial para validar a eficácia destes planos e assegurar a preparação.

A Política de Utilização Aceitável (PUA)
rege a utilização adequada dos recursos informáticos da agência. Define as atividades permitidas e proibidas, garantindo que os recursos são utilizados principalmente para fins profissionais e não para atividades ilegais ou inadequadas. A política permite uma utilização pessoal limitada dos recursos informáticos, desde que não interfira com as responsabilidades profissionais ou com a segurança. As medidas de controlo e conformidade são pormenorizadas, informando os utilizadores de que as suas atividades podem ser monitorizadas

para garantir o cumprimento da política. As consequências de uma utilização incorrecta estão claramente definidas, variando desde avisos até rescisões, dependendo da gravidade da violação.

j. Políticas/orientações em matéria de confidencialidade e proteção de dados

As políticas de confidencialidade e proteção de dados são fundamentais para uma Agência Nacional de Proteção de Dados, uma vez que constituem a espinha dorsal dos esforços do país para salvaguardar dados sensíveis e pessoais. Estas políticas garantem que todos os dados dentro da agência, bem como os dados tratados por várias partes interessadas, incluindo entidades governamentais, organizações privadas e o público em geral, são geridos de forma segura e em estrita conformidade com os requisitos legais e regulamentares.

Ao impor normas rigorosas para o tratamento, armazenamento e acesso aos dados, estas políticas protegem a integridade, confidencialidade e disponibilidade da informação, minimizando assim o risco de violações de dados, acesso não autorizado e utilização indevida. Para uma Agência Nacional de Proteção de Dados, estas políticas não se referem apenas à conformidade, mas também à definição de um padrão de referência para as melhores práticas na Guiné-Bissau. Elas fornecem um quadro que orienta todas as partes interessadas nos seus esforços para proteger os dados, assegurando que todas as atividades de processamento de dados sejam consistentes com as normas nacionais e internacionais.

Além disso, ao manter um ambiente de dados seguro e transparente, a agência promove a confiança entre cidadãos, empresas e parceiros internacionais, o que é essencial para o bom funcionamento dos serviços digitais e para a proteção da privacidade pessoal à escala nacional. A agência estabelecerá, implementará e manterá procedimentos relacionados a estas políticas para garantir a conformidade com os requisitos dos regulamentos nacionais e internacionais em matéria de proteção de dados.

A política aplica-se a todos os funcionários, contratantes, voluntários e outros indivíduos que trabalham para ou em nome da agência nacional de proteção de dados. Esta inclusão garante que todas as pessoas envolvidas no tratamento de dados sensíveis estão cientes das suas responsabilidades e são obrigadas a respeitar as mesmas normas de confidencialidade e proteção de dados.

Será aplicável a todas as áreas da agência e a adesão deve ser incluída em todos os contratos de serviços subcontratados ou partilhados. Não existem exclusões.
As apólices abrangerão:

- **Cobertura da informação**

As políticas abrangem todos os tipos de informação dentro da organização, incluindo dados pessoais, informação comercial sensível, entre outros. Ao abordar dados estruturados e não estruturados, bem como vários formatos de media (por exemplo, papel, digital, vídeo), a política assegura uma proteção abrangente de todas as formas de informação.

As políticas devem detalhar os vários tipos de informação que abrangem, garantindo que todos os dados, independentemente do seu formato ou localização, estão sujeitos às mesmas medidas de proteção rigorosas. Esta abordagem holística é essencial para evitar violações de dados e acessos não autorizados.

- **Processamento de informações**

Temos de abranger todos os aspectos do processamento da informação, incluindo a criação, recuperação, armazenamento, divulgação e destruição, para garantir que os dados são geridos de forma segura ao longo do seu ciclo de vida, minimizando

o risco de acesso não autorizado ou perda.

As políticas oferecerão diretrizes claras sobre o tratamento seguro da informação em cada fase, quer se trate de armazenamento, utilização ou eliminação, em conformidade com a legislação relevante. Abrangendo atividades como a divulgação e a destruição, estas políticas ajudam a garantir que a agência cumpra os regulamentos nacionais e internacionais de gestão de dados, evitando assim consequências legais.

- **Responsabilidades dos responsáveis pelo tratamento de dados**

A política deixa claro que os responsáveis pelo tratamento dos dados, como os contratantes independentes, são responsáveis pela gestão da confidencialidade e da proteção dos dados nas suas instalações. Esta delimitação de responsabilidades ajuda a evitar confusões e garante que todas as partes compreendem as suas obrigações.

Salienta igualmente o empenho da agência em apoiar os contratantes na gestão do risco de informação, prestando aconselhamento e partilhando as melhores práticas. Este apoio ajuda os contratantes a manter elevados padrões de proteção de dados, beneficiando o ecossistema global de segurança.

A política deve definir claramente as responsabilidades dos responsáveis pelo tratamento de dados, assegurando que estes compreendem o seu papel na proteção dos dados. Além disso, deve descrever a forma como a agência apoiará esses responsáveis pelo tratamento, promovendo uma abordagem colaborativa da segurança dos dados.

- Conformidade legal e regulamentar A política deve incluir disposições para a conformidade contínua com as alterações legais e regulamentares, assegurando que as práticas de proteção de dados da agência se mantêm atualizadas e eficazes. Isto ajuda a manter a confiança do público.

- A política também reconhece a importância de se adaptar às mudanças nas leis de gestão da informação, como as introduzidas pelas Leis da Saúde e da Assistência Social. Ao manter-se alinhada com os regulamentos atuais, a agência garante que as suas práticas de proteção de dados permanecem legalmente conformes e eficazes.

- Ao dar prioridade à colaboração com organizações e parceiros nacionais, a política reforça a capacidade da agência para garantir a utilização segura da informação e manter a conformidade com as normas jurídicas em evolução.

Execução e medidas disciplinares

Nesta secção, a política afirma claramente que o não cumprimento das regras pode resultar em ações disciplinares, incluindo o recurso a organismos reguladores e à aplicação da lei, o que funciona como um forte dissuasor contra o tratamento incorreto dos dados.
Devemos salientar na política que todos os funcionários e contratantes devem compreender as graves consequências de não protegerem os dados confidenciais, promovendo assim uma cultura de responsabilidade e vigilância na organização.

A política deve especificar as consequências do incumprimento, deixando claro que quaisquer violações da política serão levadas a sério. Isto ajuda a reforçar a importância da proteção de dados e incentiva todos os membros da organização a cumprirem rigorosamente as diretrizes.

3. Processos operacionais

A. Descrição dos procedimentos operacionais normalizados (SOP)

Os Procedimentos Operacionais Normalizados (SOPs) são instruções formalizadas e documentadas

1 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

que descrevem os passos específicos necessários para realizar operações ou tarefas de rotina numa organização. Estes procedimentos são concebidos para fornecer orientações claras e concisas aos funcionários sobre como desempenhar as suas funções de forma correta e consistente. Os SOPs são essenciais para o bom funcionamento de qualquer organização, especialmente nos sectores em que a precisão, o rigor e a conformidade com os regulamentos são fundamentais. Os SOPs são muito cruciais para a criação da agência. O estabelecimento de SOPs para cada atividade-chave dentro da agência é, portanto, fundamental para garantir que todas as tarefas são executadas de forma consistente e em conformidade com os requisitos regulamentares e as políticas internas. Ao definirem claramente os elementos-chave destes procedimentos, as organizações podem aumentar a eficiência, reduzir os erros e garantir que todos os membros do pessoal estão alinhados com os objetivos da agência. Eis uma visão geral concisa da sua importância:

- Os SOPs fornecem instruções claras e passo-a-passo que ajudam a garantir que as tarefas são realizadas de forma consistente, reduzindo a variabilidade e melhorando a eficiência.
- Os SOPs são um recurso fundamental para a formação de novos funcionários, assegurando que estes ficam rapidamente a par dos procedimentos estabelecidos.
- Os SOPs ajudam as organizações a cumprir as normas do sector, os requisitos legais e as políticas internas, documentando a forma como os processos específicos devem ser executados.
- Ao normalizar os procedimentos, os SOPs ajudam a reduzir os riscos associados a erros humanos, assegurando que as tarefas críticas são executadas corretamente e em segurança.

É também essencial compreender os elementos-chave que constituem estes procedimentos, que são a base para o bom funcionamento da empresa, proporcionando uma estrutura clara para o tratamento das tarefas e responsabilidades em toda a organização.

- Título e objetivo: Cada SOPs deve ter um título claro e uma declaração concisa do seu objetivo.
- ambito de aplicação : Definir a aplicabilidade do SOPs, incluindo a quem se aplica e em que condições.
- Procedimento : Instruções passo a passo para a realização de uma tarefa ou processo.
- Funções e responsabilidades : Esclarece quem é responsável por cada parte do processo.
- Documentação e manutenção de registos: Especifica quais os registos que devem ser mantidos e como devem ser documentados.
- Análise e revisão: Informações sobre a frequência com que o SOPs deve ser analisado e atualizado, e quem é responsável por este processo.

i. Processos para a agência de cibersegurança

A Agência Nacional de Cibersegurança da Guiné-Bissau será responsável pela proteção das infraestruturas críticas, dos dados sensíveis e dos ativos digitais contra as ciberameaças cada vez mais sofisticadas. Para gerir eficazmente estas responsabilidades, a agência deve implementar uma série de processos operacionais que garantam uma vigilância constante, uma resposta rápida a incidentes e o cumprimento das normas do sector.

Seguem-se os principais processos essenciais para uma agência de cibersegurança:

- **Resposta e gestão de incidentes :**
Procedimentos pormenorizados para detetar, investigar e responder a incidentes de cibersegurança. Isto inclui a formação de uma Equipa de Resposta a Incidentes (IRT) e a utilização de

ferramentas como os sistemas de Gestão de Informações e Eventos de Segurança (SIEM) para monitorizar as ameaças em tempo real.

Eis o SOPs proposto:

- ***Objetivos :*** Fornecer uma abordagem estruturada para detetar, investigar e responder a incidentes de cibersegurança para minimizar o impacto e garantir uma recuperação rápida.
- ***Aambito de aplicação :*** O presente SOPs aplica-se a todos os funcionários, contratantes e prestadores de serviços terceiros da Agência Nacional de Cibersegurança. Abrange todos os tipos de incidentes de cibersegurança, incluindo violações de dados, infecções por malware e ataques de negação de serviço
- ***Procedimento :***
  - Deteção de incidentes: monitorizar continuamente sistemas e redes utilizando ferramentas de gestão de informações e eventos de segurança (SIEM). Identificar potenciais incidentes através de alertas automáticos, relatórios de utilizadores, relatórios da empresa ou de outras agências e feeds de informações sobre ameaças.
  - Classificação do incidente: classificar o incidente com base na sua gravidade e impacto (baixo, médio, elevado).
  - Resposta inicial: A Equipa de Resposta a Incidentes (IRT) é notificada imediatamente após a identificação de um potencial incidente. A equipa analisa o caso e executa manuais. A equipa contém o incidente para evitar mais danos (por exemplo, isolar os sistemas afetados, bloquear endereços IP maliciosos)
  - Investigação: Realizar uma investigação exaustiva para determinar a causa e a extensão do incidente Recolher e preservar provas para eventuais ações judiciais.
  - Mitigação: Implementar medidas para mitigar o impacto do incidente (por exemplo, remover malware, aplicar patches). Comunicar com as partes interessadas afectadas e fornecer orientações sobre medidas de proteção.
  - Recuperação: Restaurar o funcionamento normal dos sistemas e serviços afetados. Verificar a integridade dos sistemas e dados restaurados.
  - Revisão pós-incidente: Efetuar uma revisão pós-incidente para identificar as lições aprendidas e as áreas a melhorar. Atualizar o plano de resposta a incidentes e os SOPs com base nas conclusões.
  - Colaboração com outros organismos : Coordenar com outros organismos governamentais, como a ARN, as autoridades policiais e os serviços de informação, a partilha de informações e recursos. Estabelecer uma cooperação internacional com agências de cibersegurança de outros países para partilhar informações sobre ameaças, melhores práticas e coordenar respostas a ciberameaças transfronteiriças.
- ***Funções e responsabilidades***
  - Equipa de Resposta a Incidentes (IRT) : Lideram os esforços de resposta a incidentes e coordenam com outras equipas. Asseguram a documentação e a comunicação adequadas do incidente.
  - Departamento de TI: Ajudam na investigação técnica e na atenuação do incidente. Implementam medidas de recuperação e verificam a integridade do sistema.
  - Equipa Jurídica e de Conformidade: fornece orientações sobre os requisitos legais e regulamentares. Asseguram a conformidade com as leis de proteção de dados e as obrigações de comunicação.
  - Coordenador da colaboração: Facilita a comunicação e a coordenação com outras agências governamentais.
- ***Documentação e manutenção de registos:***

A IRT deve manter registos detalhados de todos os incidentes, incluindo a identificação, a classificação, as ações de resposta e as revisões pós-incidente. Os registos devem ser armazenados de forma segura e devem estar acessíveis para efeitos de auditoria e revisão.

- ***Análise e revisão:*** A IRT deve analisar este SOPs anualmente ou após qualquer incidente grave.

• ***Procedimentos de comunicação com os parceiros*** Num modelo de governação híbrido, em que as responsabilidades são partilhadas entre a autoridade centralizada e várias entidades descentralizadas, a comunicação eficaz é crucial. Uma agência de cibersegurança deve estabelecer procedimentos claros para coordenar e partilhar informações com os seus parceiros, incluindo agências governamentais, organizações do sector privado e organismos internacionais.

Por exemplo, devemos estabelecer canais de comunicação formais, tais como reuniões regulares, trocas de correio eletrónico seguras e plataformas de comunicação encriptadas para partilhar informações sobre ciberameaças, vulnerabilidades e incidentes. E também implementar acordos ou memorandos de entendimento (MOU) com parceiros para formalizar a partilha de informações sobre ameaças e melhores práticas, assegurando simultaneamente a conformidade com os requisitos legais e regulamentares. Por exemplo, no caso de um ciberataque a nível nacional, a agência de cibersegurança pode comunicar rapidamente com os operadores de infraestruturas críticas e outros organismos governamentais através de uma rede de comunicação segura pré-estabelecida, assegurando uma resposta unificada e rápida.

Abaixo o SOP proposto :

• aambito de aplicação : Este procedimento aplica-se a todos os funcionários da agência de cibersegurança envolvidos na comunicação com parceiros externos. Abrange o estabelecimento de canais de comunicação, a utilização de métodos seguros para a troca de informações e a implementação de acordos, como os memorandos de entendimento, para formalizar a colaboração.

• ***Procedimento :***

- Estabelecer canais de comunicação :

  Identificar parceiros : Compilar uma lista dos principais parceiros, incluindo agências governamentais, organizações do sector privado, operadores de infraestruturas críticas e organismos internacionais que fazem parte integrante dos esforços de cibersegurança. Selecionar métodos de comunicação : Escolher os métodos de comunicação adequados para os diferentes tipos de partilha de informações. As opções podem incluir reuniões regulares, trocas de correio eletrónico seguras, plataforma de comunicação encriptada. ***Implementar a infraestrutura de comunicação:*** criar e manter a infraestrutura técnica necessária para uma comunicação segura, incluindo servidores de correio eletrónico encriptados, plataformas de mensagens seguras e ferramentas de videoconferência com encriptação de ponta a ponta.

- Desenvolver e formalizar acordos :

  Redação de Memorandos de Entendimento (MOU) : Trabalhar com o Departamento Jurídico para redigir os MOU que definem os termos da colaboração, incluindo protocolos de partilha de dados, acordos de confidencialidade e conformidade com os requisitos legais e regulamentares. Rever e assinar acordos : Envolver-se com os parceiros para rever, negociar e finalizar os MOU. Certifique-se de que todas as partes compreendem e concordam com os termos, especialmente no que diz respeito à partilha de informações sensíveis.

- Protocolo de comunicação de incidentes :

Configuração da comunicação pré-incidente: Antes da ocorrência de qualquer incidente, deve-se estabelecer um protocolo de comunicação seguro que defina a forma como a informação será partilhada durante um incidente cibernético. Este protocolo deve incluir funções predefinidas, listas de contactos e vias de escalonamento.

Comunicação durante um incidente: Na eventualidade de um ciberataque a nível nacional, ativar a rede de comunicação segura pré-estabelecida. Divulgue rapidamente informações críticas aos parceiros, incluindo a natureza da ameaça, os sistemas afectados e as ações iniciais de resposta. Comunicação pós-incidente: Após a contenção do incidente, continuar a comunicação com os parceiros para partilhar as lições aprendidas, discutir estratégias de recuperação e atualizar quaisquer acordos ou protocolos com base na análise do incidente.

- Melhoria contínua e formação :

  Revisão e atualizações regulares : Rever regularmente os procedimentos de comunicação para garantir que estão atualizados com as tecnologias atuais, ameaças e necessidades dos parceiros. Atualizar o SOPs conforme necessário para refletir quaisquer alterações. Formação: Realizar sessões de formação regulares e exercícios de comunicação com o pessoal e os parceiros para garantir que todos estão familiarizados com os procedimentos e podem executá-los eficazmente durante um incidente.

- Funções e responsabilidades:

  Especialista em segurança informática / Coordenador de incidentes: O especialista em segurança informática será responsável pela implementação e manutenção da infraestrutura técnica necessária para recolher, analisar e partilhar informações sobre ameaças.

  Esta função deve ser combinada com a de coordenador de incidentes. Envolve a gestão do processo geral de resposta a incidentes e o fornecimento dos conhecimentos técnicos necessários.

- Informações e análise das ameaças: Recolha, análise e partilha de informações sobre ciberameaças para antecipar e atenuar as potenciais ciberameaças. Este processo implica a colaboração com outros organismos nacionais e internacionais de cibersegurança. Eis o SOPs proposto:
  - ambito de aplicação: Este procedimento aplica-se a todo o pessoal envolvido em atividades de informação sobre ameaças na agência de cibersegurança, incluindo analistas, especialistas em segurança informática e responsáveis de comunicação. Inclui também processos de colaboração com parceiros externos, tais como agências governamentais, organizações do sector privado e organismos internacionais de cibersegurança.

  - Procedimento:
    - ***Recolha de informações sobre ameaças :*** Identificar as fontes de informação : Identificar e documentar uma lista de fontes fiáveis de informações sobre ameaças, tanto internas como externas. Estas fontes podem incluir: Registos de sistemas internos e relatórios de incidentes para fontes internas. Para fontes externas, a agência deve consultar informações de fonte aberta (OSINT), feeds de informações sobre ameaças (por exemplo, de fornecedores ou agências governamentais), centros de partilha e análise de informações (ISAC) e informações de organismos internacionais de cibersegurança. Recolha automatizada

de dados sobre ameaças: implementar ferramentas e plataformas automatizadas para recolher dados de informações sobre ameaças. As ferramentas podem incluir sistemas de gestão de informações e eventos de segurança (SIEM), plataformas de informações sobre ameaças (TIPs) e ferramentas de recolha automática de dados para OSINT. Inteligência humana (HUMINT) ***Recolha:*** Participar em comunidades, fóruns e redes de cibersegurança para recolher informações humanas sobre ameaças emergentes. Isto pode implicar assistir a conferências, participar em webinars e manter relações com peritos em cibersegurança.

- Análise da informação sobre ameaças : ***Correlação de dados e contextualização:*** Correlacionar os dados de informações sobre ameaças recolhidas para identificar padrões, tendências e potenciais indicadores de comprometimento (IOCs). Utilizar informações contextuais para avaliar a relevância e o potencial impacto das ameaças. Avaliação dos riscos: Avaliar o risco associado às ameaças identificadas com base na sua probabilidade e potencial impacto nas infraestruturas críticas e na segurança nacional. Classificar as ameaças de acordo com a sua gravidade (alta, média, baixa). Validação das informações: validar a exatidão e a fiabilidade das informações recolhidas antes da sua divulgação. Verificar as informações com múltiplas fontes e, sempre que possível, corroborá-las com dados históricos.

- Partilha e colaboração de informações : ***Desenvolver acordos de partilha de informações:*** Estabelecer acordos formais (MOU) com parceiros nacionais e internacionais, incluindo agências governamentais, entidades do sector privado e organismos internacionais de cibersegurança. Estes acordos devem definir protocolos para a partilha de informações, garantindo a conformidade com os requisitos legais e regulamentares Canais de comunicação seguros : Implementar canais de comunicação seguros para a partilha de informações sobre ameaças, tais como correio eletrónico encriptado, plataformas de mensagens seguras ou portais dedicados à partilha de informações. Assegurar que estes canais são acessíveis a todos os intervenientes relevantes. Partilha de informações sobre ameaças: Divulgar informações acionáveis sobre ameaças às partes interessadas internas e externas relevantes. Estas podem incluir agências governamentais, parceiros do sector privado e organismos internacionais. Adaptar os relatórios de informações às necessidades de cada parte interessada, garantindo clareza e relevância.
- Melhoria: ***Monitorização contínua das ameaças :*** Monitorizar continuamente as fontes de informação sobre ameaças para detetar ameaças novas e emergentes Rever e atualizar os procedimentos : Rever e atualizar regularmente os procedimentos de análise e informação sobre ameaças para refletir as alterações no panorama das ameaças, os avanços tecnológicos e o feedback das partes interessadas.

- ***Funções e responsabilidades :***
  - Especialista em segurança informática: O especialista em segurança informática será responsável pela implementação e manutenção da infraestrutura técnica necessária para recolher, analisar e partilhar informações sobre ameaças.

Esta função deve ser combinada com a de coordenador de incidentes. Envolve a gestão do processo geral de resposta a incidentes e o fornecimento dos conhecimentos técnicos necessários.

- Analista de informações sobre ameaças: O analista de informações sobre ameaças é responsável pela recolha, análise e validação de informações sobre ameaças cibernéticas provenientes de várias fontes. Esta função envolve a identificação de potenciais ameaças, a avaliação da sua relevância e impacto e a divulgação de informações acionáveis às partes interessadas relevantes.

• **Gestão de vulnerabilidades:** Pesquisa regular de vulnerabilidades na infraestrutura nacional de TI, atribuindo-lhes prioridade com base no risco, e aplicação de correções ou outras medidas de atenuação para reduzir o potencial de exploração.

Eis o SOPs proposto:

- **ambito de aplicação:** Este procedimento aplica-se a todos os sistemas e redes de TI sob a jurisdição da agência nacional de cibersegurança, incluindo os geridos por entidades governamentais, operadores de infraestruturas críticas e parceiros do sector privado. O SOPs abrange a análise de vulnerabilidades, a avaliação de riscos, a gestão de correções e a aplicação de medidas de atenuação.
- ***Procedimento :***
  - Análise de vulnerabilidades :

    Programar análises regulares: Estabeleça um calendário para análises regulares de vulnerabilidade de todos os sistemas e redes de TI críticos. As análises devem ser realizadas pelo menos mensalmente, com análises adicionais realizadas após alterações significativas na infraestrutura ou em resposta a ameaças emergentes. ***Selecionar e configurar ferramentas de análise:*** Utilizar ferramentas de análise de vulnerabilidades padrão da indústria (por exemplo, Nessus, OpenVAS, Qualys) para identificar potenciais vulnerabilidades. Configure as ferramentas para efetuar análises autenticadas e não autenticadas para fornecer uma avaliação abrangente.

    Conduzir análises: efetuar as análises de vulnerabilidades de acordo com o calendário estabelecido. Assegurar que os controlos são completos e abrangem todos os sistemas relevantes, incluindo servidores, estações de trabalho, dispositivos de rede e aplicações.
  - Avaliação da vulnerabilidade e definição de prioridades:

    Analisar os resultados das análises: Analisar os resultados das análises de vulnerabilidades para determinar a natureza e a gravidade das vulnerabilidades identificadas. Esta análise deve incluir uma avaliação do impacto potencial, da facilidade de exploração e da probabilidade de ocorrência. Priorização com base no risco : Priorizar as vulnerabilidades com base no risco que representam para a infraestrutura nacional de TI. As vulnerabilidades críticas e de alta gravidade devem ser tratadas imediatamente, enquanto as vulnerabilidades de média e baixa gravidade podem ser programadas para correção de acordo com os recursos disponíveis. Avaliar o impacto potencial de cada vulnerabilidade nas operações da organização, incluindo as possíveis consequências da exploração, como violações de dados, interrupções de serviço ou danos à reputação.
  - Remediação e atenuação:

    Gestão de patches : Aplicar patches ou atualizações de segurança para resolver as vulnerabilidades identificadas. Para

sistemas críticos, dê prioridade aos patches que resolvem as vulnerabilidades mais graves. Assegure-se de que os patches são testados num ambiente controlado antes da implementação para evitar interrupções não intencionais.
Implementar mitigações: Se uma correção não estiver imediatamente disponível ou não for aplicável, devemos implementar atenuações alternativas para reduzir o risco de exploração. Isto pode incluir alterações de configuração, ajustes no controlo de acesso ou segmentação da rede.
Verificação e validação: Após a aplicação de correções ou atenuações, verificar se as vulnerabilidades foram efetivamente resolvidas. Efetuar análises de acompanhamento ou testes manuais para confirmar que os riscos foram atenuados.

- Comunicação e apresentação de relatórios:
  Relatórios internos e externos: Preparar um relatório sumário abrangente das atividades de gestão de vulnerabilidades, incluindo as vulnerabilidades identificadas, priorizadas e corrigidas. Este relatório deve ser partilhado com os quadros superiores e as partes interessadas relevantes da agência (relatório interno), bem como com os parceiros externos se forem identificadas vulnerabilidades nos sistemas que gerem (relatório externo). Ao comunicar com parceiros externos, forneça prontamente as conclusões, juntamente com as medidas de correção recomendadas, oferecendo orientação e apoio, conforme necessário, para resolver as vulnerabilidades.

  Notificação de incidentes : Se uma vulnerabilidade for explorada e resultar num incidente de segurança, siga o protocolo de resposta a incidentes para notificar as partes afectadas, incluindo os organismos reguladores e o público, se necessário.

- Melhoria:
  Monitorização contínua de ameaças: Monitorizar continuamente a existência de novas vulnerabilidades, mantendo-se atualizado com feeds de informações sobre ameaças, avisos de fornecedores e boletins de segurança. Assegurar que o processo de gestão de vulnerabilidades se adapta a ameaças novas e emergentes. Rever e atualizar os procedimentos : Rever e atualizar regularmente o SOPs de gestão de vulnerabilidades para refletir as alterações tecnológicas, o panorama de ameaças e as necessidades organizacionais. Incorporar o feedback das auditorias internas e as lições aprendidas com atividades anteriores de gestão de vulnerabilidades.

- ***Funções e responsabilidades :***
  - ***Especialista em segurança informática / Coordenador de incidentes :*** O especialista em segurança informática será responsável pela implementação e manutenção da infraestrutura técnica necessária para recolher, analisar e partilhar informações sobre ameaças.
    Esta função deve ser combinada com a de coordenador de incidentes. Envolve a gestão do processo global de resposta a incidentes e a disponibilização dos conhecimentos técnicos necessários.

  - Responsável pela comunicação: O responsável pela comunicação é responsável pela gestão das comunicações externas relacionadas com a gestão das vulnerabilidades, em especial com os parceiros externos que possam ser afectados pelas vulnerabilidades identificadas.

- Gestão do Centro de Operações de Segurança (SOC) : Monitorização contínua do tráfego de rede, alertas de segurança e potenciais ameaças através de um SOC centralizado para garantir a rápida deteção e resposta a incidentes de segurança.

Eis o SOPs proposto:

- ambito: Este procedimento aplica-se a todo o pessoal envolvido nas operações do SOC, incluindo analistas do SOC, especialistas em segurança de TI, equipas de resposta a incidentes e gestão do SOC.

  Abrange os processos de monitorização, deteção, resposta a incidentes e relatórios.

- ***Procedimento:***
  - **Estrutura e funções do SOC:**
    Definir funções e responsabilidades do SOC : Definir claramente as funções e responsabilidades de todo o pessoal do SOC, incluindo analistas do SOC, chefes de turno, especialistas em segurança de TI e responsáveis pela resposta a incidentes. Gestão de pessoal e turnos : Estabeleça um horário de pessoal 24/7 para garantir uma monitorização contínua. Implementar um horário de rotação para evitar a fadiga dos analistas e garantir novas perspectivas no turno.
  - Monitorização contínua:
    Ferramentas e sistemas de monitorização: Implementar e configurar ferramentas e sistemas de monitorização, tais como sistemas de Gestão de Informações e Eventos de Segurança (SIEM), sistemas de deteção/prevenção de intrusões (IDS/IPS), firewalls e analisadores de tráfego de rede. Monitorização em tempo real: os analistas SOC devem monitorizar o tráfego de rede, os registos do sistema e os alertas de segurança em tempo real. Isto inclui a identificação de anomalias, tentativas de acesso não autorizado e potenciais indicadores de comprometimento (IOCs).
    Integração da informação sobre ameaças: Integrar a informação sobre ameaças nos sistemas de monitorização para melhorar a deteção de ameaças conhecidas e de padrões de ataque emergentes.
  - Deteção e análise de incidentes:
    Triagem e priorização de alertas: os analistas do SOC devem fazer a triagem dos alertas com base na gravidade, no impacto e na criticidade dos sistemas afetados. Priorizar os alertas de alta gravidade que representam o maior risco para a organização.
    Análise inicial de incidentes : Efetuar uma análise inicial do alerta para determinar se representa um verdadeiro positivo (incidente confirmado) ou um falso positivo (evento benigno). Isto inclui o exame de registos, a correlação de dados entre sistemas e a utilização de informações sobre ameaças. Procedimentos de escalonamento : Se for determinado que um alerta é um incidente de segurança confirmado, encaminhar o incidente para a equipa de resposta adequada com base na gravidade e no âambito do incidente.
  - Coordenação da resposta a incidentes:
    Envolver a Equipa de Resposta a Incidentes: Assim que um incidente for escalado, coordene com a Equipa de Resposta a Incidentes (IRT) para iniciar o processo de resposta. Forneça à IRT todas as informações relevantes, incluindo registos, análise inicial e quaisquer ações já tomadas.
    Contenção e atenuação : Trabalhe com a IRT para implementar estratégias de contenção para evitar que o incidente se espalhe. Isto pode envolver o isolamento dos sistemas afetados, o bloqueio de IPs maliciosos ou a desativação de contas comprometidas.

3 https://www.sans.org/

Recuperação e restauro: Ajudar a IRT na recuperação e restauro dos sistemas afetados. Isso inclui a restauração de backups, a aplicação de patches e a verificação de que o incidente foi totalmente resolvido.

- Relatórios e comunicação:
  Relatório de incidente: Depois de o incidente ter sido resolvido, preparar um relatório de incidente detalhado que inclua a cronologia dos eventos, as ações tomadas e o impacto do incidente. Este relatório deve ser partilhado com a gestão de topo e com as partes interessadas relevantes.
  Relatórios diários e semanais do SOC: Gerar relatórios diários e semanais que resumem as atividades do SOC, incluindo o número de alertas recebidos, incidentes tratados e quaisquer tendências observadas. Partilhe estes relatórios com a gestão de topo e outros departamentos relevantes.
  Comunicação com entidades externas : Se um incidente envolver entidades externas (parceiros, clientes, organismos reguladores), assegurar que são efetuadas as notificações adequadas em tempo útil. Coordenar com o responsável pelas comunicações a gestão das comunicações externas.

- Melhoria:
  Revisão pós-incidente: Conduzir uma revisão pós-incidente (PIR) após cada incidente significativo para identificar o que correu bem e o que poderia ser melhorado. Utilizar as conclusões para atualizar os procedimentos SOC e melhorar as capacidades da equipa.
  Atualização dos processos e formação : Rever e atualizar regularmente as ferramentas, tecnologias e processos utilizados pelo SOC para garantir que permaneçam eficazes contra ameaças em evolução. Isto inclui a atualização dos sistemas SIEM, das configurações IDS/IPS e das integrações de informações sobre ameaças. Efetuar sessões de formação regulares e exercícios de simulação para o pessoal do SOC, de modo a garantir que são competentes nas ferramentas, técnicas e procedimentos mais recentes. Os exercícios devem simular cenários do mundo real para testar as capacidades de resposta da equipa.

- Funções e responsabilidades :
  - Gestor do SOC: O Gestor do SOC é responsável pela gestão e funcionamento geral do Centro de Operações de Segurança. Isto inclui a supervisão da equipa do SOC, a garantia de uma monitorização eficaz dos eventos de segurança, a coordenação das respostas a incidentes e a manutenção da infraestrutura e dos processos do SOC.
  - Analistas SOC: Os analistas SOC são responsáveis pela monitorização em tempo real do tráfego de rede, dos alertas de segurança e dos registos do sistema. São os defensores da linha da frente que detectam e analisam potenciais ameaças à segurança e tomam as medidas iniciais para mitigar os riscos.
  - Coordenador de incidentes: O coordenador de incidentes é responsável pela gestão da resposta a incidentes de segurança. Trabalhará em estreita colaboração com a equipa SOC
  - Responsável pela comunicação: O responsável pela comunicação é responsável pela gestão das comunicações externas relacionadas com a gestão das vulnerabilidades, em especial com os parceiros externos que possam ser afectados pelas vulnerabilidades identificadas.

- Conformidade e auditoria : Garantir que as práticas de cibersegurança em todo o país cumprem

os regulamentos relevantes, como o GDPR ou as leis nacionais de cibersegurança, e realizam auditorias regulares para avaliar e melhorar a postura de segurança. Os objectivos destes processos são avaliar as práticas de cibersegurança das empresas públicas e das empresas do sector privado que gerem infraestruturas críticas ou tratam dados governamentais sensíveis, garantindo que cumprem as normas e regulamentos nacionais de cibersegurança. Podem ser realizados muitos tipos de auditoria:

Auditorias internas : Auditorias internas regulares para avaliar a conformidade da agência com as suas próprias políticas e procedimentos, incluindo SOPs, práticas de tratamento de dados e protocolos de resposta a incidentes.

Auditorias externas : Contratar auditores independentes para analisar a postura de cibersegurança da agência, garantindo que esta cumpre as normas internacionais e as melhores práticas. As auditorias externas fornecem uma avaliação objetiva e ajudam a identificar as áreas a melhorar.

Auditorias de parceiros : Num modelo de governação híbrido, a auditoria das práticas de cibersegurança das organizações parceiras é crucial para garantir que todas as partes interessadas cumprem as normas exigidas. Isto pode incluir auditorias a entidades do sector privado que gerem infraestruturas críticas ou lidam com dados governamentais sensíveis.

Auditorias de conformidade : Realizar auditorias para garantir o cumprimento da legislação relevante em matéria de cibersegurança, como o GDPR ou os regulamentos nacionais de cibersegurança, e para verificar se todas as ações tomadas estão em conformidade com estes requisitos.

Eis o SOPs proposto:

- **ambito de aplicação:** Este procedimento aplica-se a todas as entidades sujeitas a normas e regulamentos nacionais de cibersegurança, incluindo agências governamentais, empresas públicas, empresas do sector privado e organizações parceiras envolvidas na gestão de infraestruturas críticas ou de dados sensíveis. Abrange auditorias internas, externas, de parceiros e de conformidade.
- ***Procedimento :***
  - Planeamento e preparação de auditorias:

    Identificar o âambito e os objectivos da auditoria : Determinar o âambito e os objectivos da auditoria. Isto inclui a identificação das entidades a auditar, as práticas específicas de cibersegurança a avaliar e os regulamentos ou normas em relação aos quais a conformidade será avaliada.

    Reunir a equipa de auditoria : Reunir uma equipa de auditores qualificados para realizar a auditoria. Para auditorias internas, esta equipa pode incluir responsáveis pela conformidade interna e especialistas em segurança de TI. Para auditorias externas ou de parceiros, contrate auditores independentes ou empresas de auditoria especializadas.

    Desenvolver uma lista de controlo de auditoria : Desenvolver uma lista de verificação de auditoria abrangente com base nos regulamentos, normas e políticas internas relevantes para as entidades que estão a ser auditadas. Esta lista de verificação deve abranger todas as áreas-chave, como práticas de tratamento de dados, protocolos de resposta a incidentes e conformidade com leis específicas como o GDPR.

  - Realização de auditorias:

    Auditorias internas: Realizar auditorias internas regulares para avaliar a conformidade da agência com as suas próprias políticas e procedimentos.

    Auditorias externas: Contratar auditores independentes para efetuar uma análise exaustiva das práticas de cibersegurança

da agência.

Auditorias de parceiros: No modelo de governação híbrido da Guiné-Bissau, realizar auditorias a organizações parceiras, incluindo entidades do sector privado que gerem infraestruturas críticas ou tratam dados governamentais sensíveis. A auditoria deve avaliar se estes parceiros cumprem as normas nacionais de cibersegurança exigidas.

- Relatórios:

  Relatórios de auditoria: Realizar auditorias internas regulares para avaliar a conformidade da agência com as suas próprias políticas e procedimentos.

  Desenvolvimento de um plano de ação: Com base nas conclusões da auditoria, desenvolver um plano de ação para resolver quaisquer lacunas identificadas ou problemas de não conformidade.

  Verificação das ações corretivas: Verificar se as ações corretivas identificadas no plano de ação foram implementadas e se a conformidade foi alcançada.
- Melhoria: Utilizar os resultados das auditorias para informar os esforços de melhoria contínua na organização. Isto pode envolver a atualização dos SOPs, a revisão das estratégias de conformidade ou a prestação de formação adicional ao pessoal.

- Funções e responsabilidades:
  - Gestor de auditoria: O gestor de auditoria é responsável pela gestão de todo o processo de auditoria, desde o planeamento e preparação até à execução e acompanhamento. Isto inclui a supervisão de auditorias internas, externas, de parceiros e de conformidade, bem como a garantia de que as conclusões da auditoria são tratadas atempadamente ou normas em relação às quais a conformidade será avaliada.
  - Consultor jurídico: O consultor jurídico fornece orientações sobre os aspectos jurídicos da conformidade e da auditoria, assegurando que todas as práticas e auditorias de cibersegurança respeitam a legislação e os regulamentos relevantes. Desempenha um papel fundamental para garantir que a organização se mantém em conformidade com os requisitos legais, tanto nacionais como internacionais.

- Sensibilização e formação do público : Desenvolver e apresentar programas de sensibilização em matéria de cibersegurança para educar os funcionários públicos, os parceiros do sector privado e o público em geral sobre as melhores práticas e as ciberameaças emergentes.

- Eis o SOPs proposto:
  - ***ambito de aplicação:*** Este procedimento aplica-se a todas as agências governamentais, parceiros do sector privado e entidades públicas envolvidas na realização de programas de sensibilização e formação em matéria de cibersegurança. Abrange a criação, implementação, entrega, avaliação e melhoria contínua destes programas.
  - ***Procedimento***:
    - Planeamento e avaliação das necessidades:
      - Identificar públicos-alvo
      - Avaliar as necessidades específicas de sensibilização para a cibersegurança de cada público-alvo através de inquéritos, entrevistas e análise de incidentes anteriores.
      - Definir objetivos e metas para os programas de sensibilização e formação.
      - Desenvolver um plano anual de sensibilização e formação

- Desenvolvimento de programas e materiais:
  - Criar conteúdo
  - Criar materiais suplementares, tais como cartazes, infografias, brochuras e módulos de aprendizagem eletrónica/conteúdos digitais para campanhas públicas.
  - Plano de formação

- Entrega do programa:
  - Selecionar os métodos de entrega
  - Programar e realizar as campanhas de sensibilização
  - Implementar módulos de aprendizagem eletrónica

- Feedback e melhoria contínua:
  - Avaliar a eficácia da formação
  - recolher as reações dos participantes
  - Analisar métricas de desempenho
  - Rever e atualizar regularmente o conteúdo do programa

- ***Funções e responsabilidades :***
  - Programadores de conteúdos: Desenvolvem materiais didáticos e suplementares para programas de formação e sensibilização.
  - Gestor de formação: Promove programas de formação e sensibilização através de vários canais para garantir o máximo alcance e envolvimento.
  - Equipa de comunicação: Promovem programas de formação e sensibilização através de vários canais para garantir o máximo alcance e envolvimento.

j. Processos para a Agência de Proteção de Dados

Os processos operacionais da agência nacional de proteção de dados centram-se na salvaguarda de dados pessoais e sensíveis, garantindo a conformidade com os regulamentos de proteção de dados e defendendo os direitos de privacidade dos indivíduos. Estes processos são vitais para manter a confiança do público e garantir que as atividades de processamento de dados são conduzidas de forma legal e ética. É essencial estabelecer e implementar um conjunto de processos operacionais fundamentais:

- Avaliações de impacto sobre a proteção de dados (DPIA) :

Procedimentos para avaliar os riscos associados às atividades de tratamento de dados e aplicar medidas para atenuar esses riscos. As DPIA são essenciais para garantir que os novos projectos cumprem a legislação em matéria de proteção de dados. Por exemplo, ao introduzir um novo sistema de reconhecimento facial para vigilância pública, a agência realizará uma DPIA para avaliar as implicações em termos de privacidade e implementará medidas rigorosas de retenção de dados e de controlo do acesso para proteger a privacidade dos cidadãos:

- ***Identificação das atividades de tratamento:*** Identificar e documentar as atividades específicas de tratamento de dados que exigem uma DPIA. Isto inclui normalmente atividades que envolvem o tratamento em grande escala de dados sensíveis, a monitorização sistemática de áreas públicas ou o tratamento que possa afetar significativamente a privacidade das pessoas.
- ***Avaliação dos riscos:*** Analisar os potenciais riscos para a privacidade e os direitos de proteção de dados dos titulares dos dados. Isto inclui a avaliação da probabilidade e gravidade dos potenciais danos.
- ***Conduzir a DPIA:*** Criar um mapa detalhado do fluxo de dados para compreender como os dados são recolhidos, processados, armazenados e partilhados.
- ***Medidas de atenuação:*** Desenvolver e implementar medidas para atenuar os riscos identificados, como a minimização de dados, a

pseudonimização ou controlos de acesso melhorados.

- ***Documentação e revisão:*** Documentar o processo de AIPD, incluindo os riscos identificados, as medidas de atenuação escolhidas e a fundamentação dessas decisões. Rever e atualizar regularmente as DPIA à medida que as atividades de tratamento ou as tecnologias evoluem.

• Gerir autorizações para processar e tratar dados pessoais:

Este processo destina-se a conceder, gerir e revogar autorizações a organizações públicas e privadas para o tratamento e processamento de dados pessoais.

Também ajudará a monitorizar e a avaliar estas organizações para garantir a conformidade com a legislação em matéria de proteção de dados. Abaixo estão as principais etapas do processo:

- ***Identificação de dados sensíveis:*** Identificar os tipos de dados pessoais considerados sensíveis e que exigem autorizações específicas para o seu tratamento e processamento.
- ***Apresentação do pedido de autorização:*** As organizações devem enviar um pedido formal à agência, solicitando autorização para processar dados pessoais. O formulário de pedido padronizado deve incluir pelo menos as seguintes informações:
  - Uma descrição das atividades de tratamento de dados
  - Categorias de dados pessoais envolvidos (por exemplo, dados de saúde, financeiros ou biométricos).
  - Medidas de segurança aplicadas para proteger os dados.
  - Objetivo e duração do tratamento dos dados.
- ***Avaliação das medidas de segurança e da conformidade:*** o DPO e a equipa de auditoria efetuam uma avaliação da segurança e uma verificação da conformidade, a fim de avaliar as medidas de proteção e segurança dos dados da organização e garantir que cumprem as normas exigidas (nesta fase, iremos executar o SOPs de auditoria)
- ***Decisão e notificação:*** Dependendo dos resultados da Auditoria, temos duas opções aqui: conceder autorizações temporárias com dados de validade específicos ou negar a autorização
- ***Monitorização e auditorias periódicas :*** As organizações autorizadas são sujeitas a auditorias periódicas para garantir a conformidade contínua com as leis de proteção de dados e as medidas de segurança.
  (Podemos executar o SOPs de auditoria aqui)
- ***Revogação da autorização:*** A agência pode revogar a autorização se uma organização for considerada não conforme ou não mantiver medidas de segurança adequadas. A organização é formalmente notificada e o processamento de dados deve cessar imediatamente, podendo apresentar documentação e novas provas de conformidade.
- ***Processo de autorização após a revogação:*** As organizações cuja autorização tenha sido revogada podem voltar a candidatar-se depois de resolverem os problemas identificados
- ***Documentação e revisão:*** Manter um registo das autorizações concedidas, incluindo os detalhes do pedido, as decisões do comité e as datas de expiração. Rever este SOPs anualmente ou após qualquer incidente grave que envolva dados pessoais

• *Tratamento dos pedidos de acesso dos titulares dos dados (DSAR):* Processos de gestão dos pedidos de pessoas que pretendem aceder, corrigir ou apagar os seus dados pessoais. Isto inclui :

- Verificar a identidade do requerente,
- Recuperação das informações solicitadas,
- Garantir que as respostas são dadas dentro

dos prazos legais
- A formação regular e as atualizações do procedimento asseguram a melhoria contínua e a conformidade.

Processos sólidos para tratar estes pedidos de forma eficiente, garantindo a conformidade com as leis de proteção de dados, como o GDPR. Por exemplo, se uma empresa da Guiné-Bissau comercializar produtos ou serviços, mesmo que sejam gratuitos, a indivíduos na UE, o GDPR aplica-se às suas atividades de processamento de dados.
As principais funções incluem :
- O coordenador do DSAR, que gere todo o processo;
- O responsável pela proteção de dados (GDPR), que assegura a conformidade legal;
- A equipa informática, responsável pela recuperação de dados;
- O conselheiro jurídico, que presta orientação jurídica.

• **Gestão de violações de dados:** O SOPs para a gestão de violações de dados descreve um processo abrangente para identificar, comunicar e responder a violações de dados. Envolve :
- Detetar violações,
- Realização de uma avaliação inicial,
- Informar prontamente as partes interessadas internas, as autoridades reguladoras e as pessoas afectadas.
- Esforços imediatos de contenção e atenuação,
- Uma investigação exaustiva para determinar a causa principal.

Depois de a violação ter sido gerida, o PON exige uma análise pós-violação para aprender com o incidente e melhorar as respostas futuras. Eis as principais funções que incluem :
- O Responsável pela Proteção de Dados (DPO) : responsável pela supervisão de todo o processo de gestão da violação de dados, garantindo que todas as ações cumprem a legislação e os regulamentos relevantes em matéria de proteção de dados.
- A equipa de resposta a incidentes: responsável pela gestão da resposta à violação de dados, incluindo a contenção, a atenuação, a investigação e os esforços de recuperação. As duas equipas IRT devem desenvolver planos conjuntos de resposta a incidentes com funções e responsabilidades claras.
- O Consultor Jurídico: Responsável por fornecer orientação jurídica durante todo o processo de gestão da violação de dados, garantindo que todas as ações estão em conformidade com as leis e regulamentos relevantes.
- Responsável pelas comunicações: É responsável pela gestão de todas as comunicações internas e externas relacionadas com a violação de dados. Isto inclui a notificação das pessoas afectadas, a gestão das relações públicas e a coordenação com os meios de comunicação social, se necessário.

• **Retenção e eliminação de dados:** Este SOPs estabelece diretrizes abrangentes para a gestão de dados ao longo do seu ciclo de vida, garantindo que são retidos apenas durante o tempo necessário para cumprir os requisitos legais, regulamentares e operacionais, e eliminados de forma segura quando já não são necessários.
O processo inclui as seguintes etapas principais:
- Categorização de dados: Os dados são classificados por tipo e sensibilidade, permitindo a determinação de períodos de retenção adequados com base em obrigações legais e necessidades organizacionais.
- Definição de períodos de retenção: São estabelecidos períodos de retenção específicos para cada categoria de dados, em conformidade com as leis, regulamentos e requisitos

operacionais atuais. Estes períodos são revistos regularmente para se manterem alinhados com quaisquer alterações nas normas legais ou organizacionais.

- Armazenamento seguro e controlo de acesso: Durante o período de retenção, os dados são armazenados de forma segura com controlos de acesso rigorosos para evitar o acesso não autorizado, utilizando métodos como a encriptação e as permissões baseadas em funções.
- Procedimentos de eliminação segura: Quando os dados atingem o fim do seu período de retenção, são eliminados de forma segura de acordo com o seu tipo e sensibilidade, por exemplo, através da destruição de documentos físicos ou da eliminação segura de dados digitais. Todas as ações de eliminação são meticulosamente documentadas para criar uma pista de auditoria.
- Conformidade legal e revisão contínua: O SOPs garante que as práticas de retenção e eliminação de dados cumprem as leis de proteção de dados, como o GDPR. São efectuadas revisões e auditorias regulares para garantir que as práticas permanecem em conformidade e são eficazes.

Para garantir a aplicação efectiva destes procedimentos, várias funções-chave são responsáveis pela supervisão e gestão de diferentes aspectos do processo de conservação e eliminação de dados. Estes incluem :

- Responsável pela proteção de dados (DPO): Supervisiona todo o processo, assegura a conformidade legal e coordena a revisão das políticas de retenção e eliminação de dados.
- Equipa de TI/Segurança: Responsável pela proteção dos dados durante o seu período de retenção e pela execução de procedimentos de eliminação segura.
- Auditor interno: Realiza auditorias regulares para garantir que as políticas de retenção e eliminação são corretamente aplicadas e cumprem as normas relevantes.

• **Monitorização e auditoria da conformidade:** trata-se de procedimentos para realizar auditorias e avaliações regulares para garantir que as práticas de proteção de dados na organização cumprem os requisitos legais, como o Regulamento Geral sobre a Proteção de Dados (GDPR), e as políticas internas de proteção de dados. Este processo envolve os seguintes passos:

- Planeamento e programação de auditorias: O SOP começa com o desenvolvimento de um plano de auditoria, que inclui um calendário para auditorias e avaliações regulares. Este plano foi concebido para abranger todas as áreas de proteção de dados, assegurando que tanto os requisitos legais como as políticas internas são cuidadosamente analisados.
- Realização de auditorias: As auditorias são realizadas de acordo com o plano estabelecido, centrando-se em áreas-chave como as práticas de tratamento de dados, os controlos de acesso e os protocolos de resposta a incidentes. As auditorias avaliam a conformidade com o GDPR e outras leis relevantes, bem como a adesão às políticas internas de proteção de dados.
- Identificação de problemas de não-conformidade: Durante as auditorias, quaisquer áreas de não conformidade são identificadas, documentadas e comunicadas. Isto inclui lacunas nas práticas de proteção de dados, falhas no cumprimento de obrigações legais ou desvios das políticas internas.
- ações corretivas e acompanhamento: Uma vez identificados os problemas de não conformidade, são desenvolvidas e aplicadas medidas corretivas para os resolver. São programadas auditorias de acompanhamento para garantir que as medidas corretivas foram aplicadas com êxito e que a

conformidade foi restabelecida.

- Documentação e relatórios: Todo o processo de auditoria, incluindo as conclusões, as ações corretivas e os resultados do acompanhamento, é cuidadosamente documentado. Os relatórios são preparados e apresentados à gestão de topo, garantindo transparência e responsabilidade nos esforços de proteção de dados da organização.

As funções do DPO e do auditor interno para realizar as auditorias e do responsável pela conformidade para supervisionar todo o processo de controlo da conformidade são importantes para este SOPs.

- Programas de formação e sensibilização : O SOPs para Programas de Formação e Sensibilização fornece uma abordagem estruturada para educar os funcionários, parceiros e partes interessadas relevantes sobre as melhores práticas de proteção de dados e cibersegurança. O objetivo é garantir que todos os envolvidos no tratamento de dados compreendam as suas responsabilidades e a importância do cumprimento das leis de proteção de dados. Uma boa formação sobre os princípios da proteção de dados, as obrigações legais e as melhores práticas para o tratamento de dados pessoais.

  Estes programas ajudarão a criar uma cultura de proteção de dados na organização.

  Por exemplo, os processos recomendam uma série de workshops centrados nos novos regulamentos de proteção de dados. Os funcionários receberão formação sobre as implicações dos regulamentos para o seu trabalho quotidiano e a importância de salvaguardar os dados pessoais. O feedback destas sessões será utilizado para aperfeiçoar futuros programas de formação.

  Seguem-se as principais etapas deste SOPs:

  - Avaliação das necessidades e desenvolvimento de programas: O processo começa com a avaliação das necessidades de formação específicas dos diferentes grupos da organização. Com base nesta avaliação, são desenvolvidos programas de formação personalizados para colmatar as lacunas de conhecimento e reforçar os conceitos-chave relacionados com a proteção de dados e a cibersegurança.
  - Apresentação do programa: Os programas de formação e sensibilização são apresentados através de uma variedade de métodos, incluindo workshops, módulos de e-learning, webinars e campanhas de sensibilização contínuas. Estes programas são concebidos para serem cativantes e acessíveis, assegurando que todos os participantes possam efetivamente absorver o material.
  - Monitorização e avaliação: A eficácia dos programas de formação é avaliada regularmente através de avaliações, inquéritos de feedback e métricas de participação. Esta etapa garante que os programas estão a atingir os seus objectivos e fornece informações para uma melhoria contínua.
  - Campanhas de sensibilização contínuas: Para além da formação formal, o SOPs inclui a implementação de campanhas de sensibilização contínuas que mantêm a proteção de dados e a cibersegurança no topo das atenções. Estas campanhas podem incluir atualizações regulares, lembretes e a divulgação das melhores práticas.
  - Documentação e relatórios: Todas as atividades de formação, incluindo a participação, os conteúdos ministrados e os resultados da avaliação, são cuidadosamente documentados. Os relatórios sobre a eficácia dos programas são elaborados e partilhados com os quadros superiores para garantir a transparência e o apoio contínuo a estas iniciativas.

Eis os principais papéis para garantir a implementação e gestão eficaz destes programas:

- Coordenador de formação: Gere o desenvolvimento, a calendarização e a realização de

programas de formação, assegurando que estes satisfazem as necessidades identificadas da organização.

- Programador de conteúdos/designer instrucional: Cria materiais de formação cativantes e eficazes que são adaptados às necessidades específicas de diferentes públicos dentro da organização.
- Responsável pela proteção de dados (DPO): Assegura que o conteúdo dos programas de formação está em conformidade com as leis de proteção de dados, como o GDPR, e as políticas internas. O DPO também ajuda a monitorizar a eficácia da formação.

B. Protocolos de resposta a incidentes

Os protocolos de resposta a incidentes são fundamentais para qualquer organização, em especial para uma Agência Nacional de Proteção de Dados (ANPD) ou uma Agência de Cibersegurança, para gerir e atenuar eficazmente o impacto de incidentes de segurança, como violações de dados, ciberataques ou falhas do sistema.

Estes protocolos não só asseguram que a agência pode responder rápida e eficazmente, minimizando os danos e restaurando as operações normais, como também servirão de padrão de base para todas as outras entidades governamentais e organizações do sector privado.

Ao estabelecer estes protocolos como referência, a ANPD ou Agência de Cibersegurança ajuda a garantir a aplicação de medidas coerentes e sólidas de resposta a incidentes em todo o ecossistema nacional, promovendo uma abordagem unificada da cibersegurança e da proteção de dados.

Teremos muitas partes de um protocolo de resposta a incidentes:

- **Parte 1: Deteção e comunicação de incidentes:** A fase inicial da resposta a incidentes envolve a deteção e comunicação atempadas de incidentes. Este processo, que inclui a monitorização dos sistemas em busca de atividades suspeitas e a criação de canais de comunicação, servirá como uma prática normalizada que outras entidades governamentais e organizações privadas podem adotar. O estabelecimento de uma abordagem uniforme para a deteção de incidentes em todos os sectores ajuda a garantir uma resposta rápida e coordenada a potenciais ameaças. Os principais passos desta fase são os seguintes
  - Implementar ferramentas de monitorização como o SIEM
  - Estabelecimento de canais de comunicação claros para os funcionários, parceiros e partes interessadas comunicarem suspeitas de incidentes
  - Após a deteção de um potencial incidente, efetuar uma avaliação inicial para determinar a sua gravidade e âmbito

- **Parte 2: Participação da equipa de resposta a incidentes** a equipa de resposta a incidentes é responsável pela gestão do processo de resposta a incidentes. Para a APDN ou a Agência de Cibersegurança, a estrutura e as operações da IRT podem servir de modelo para outras organizações. Ao promover um quadro consistente de IRT, a agência pode ajudar a garantir que as respostas a incidentes sejam tratadas com eficiência e perícia semelhantes em todos os sectores. No contexto da Guiné-Bissau, onde os recursos financeiros são limitados, devemos conceber um quadro de Equipa de Resposta a Incidentes (IRT) que seja simultaneamente rentável e eficiente. A tónica deve ser colocada na maximização da utilização dos recursos disponíveis, no aproveitamento de parcerias e na definição de prioridades para as funções essenciais, de modo a garantir que o país possa responder eficazmente a incidentes de cibersegurança. Eis um exemplo de um quadro:
  - Estrutura e funções da equipa: Tendo em conta os condicionalismos, a equipa de

investigação deve ser simples mas funcional, com funções claramente definidas que podem ser combinadas quando necessário. Abaixo as principais funções :

- Coordenador de incidentes: O coordenador liderará o processo de resposta a incidentes, supervisionando todas as atividades e servindo como ponto de contacto principal. No contexto da Guiné-Bissau, esta função pode também assumir outras responsabilidades, como as comunicações.
- *Analista forense/especialista em segurança informática: O analista será responsável pela investigação de incidentes, pela contenção de ameaças e pelo restabelecimento dos sistemas afectados.*
- Responsável jurídico/conformidade: esta função pode ser exercida a pedido ou a tempo parcial. Fornece orientações sobre a conformidade regulamentar, especialmente no que respeita a violações de dados e notificações de incidentes.

- *Fases de resposta a incidentes*
- Comunicação e notificação de incidentes

• Parte 3: Contenção e Erradicação

Uma vez confirmado um incidente, o passo seguinte é conter e erradicar a ameaça para evitar mais danos. As estratégias de contenção e erradicação utilizadas pela ANPD ou pela Agência de Cibersegurança servirão como melhores práticas que outras entidades podem adotar, garantindo uma abordagem consistente e eficaz para gerir e neutralizar as ameaças em todo o país.

• Parte 4: Plano de recuperação de desastres (DRP) O plano de recuperação de desastres é crucial para a recuperação de incidentes graves que perturbem as operações. O DRP da ANPD ou da Agência de Cibersegurança abrirá um precedente para que outras entidades desenvolvam os seus próprios planos, garantindo uma abordagem coerente e eficaz da recuperação em todos os sectores.

• Parte 5: Plano de Continuidade da Atividade (PCN) O Plano de Continuidade da Atividade assegura que as operações críticas podem continuar durante e após um incidente. O BCP da ANPD ou da Agência de Cibersegurança servirá de modelo para outras organizações, ajudando a garantir que as funções essenciais em todo o país sejam mantidas mesmo em caso de interrupções. Abaixo estão os principais elementos do BCP:

- Funções comerciais críticas: Identificar e dar prioridade às funções críticas que devem ser mantidas durante uma perturbação. Incentivar outras entidades a adotar uma priorização semelhante garante a estabilidade operacional nacional.
- Estratégias de continuidade: Desenvolver estratégias para manter as operações, como o teletrabalho ou a utilização de fornecedores alternativos. A partilha destas estratégias ajuda outras entidades a criar resiliência.
- Atribuição de recursos: Assegurar que os recursos necessários são afetados para apoiar os esforços de continuidade, fornecendo um modelo a seguir por outras organizações.
- Teste e manutenção: Testar regularmente o PCN para garantir a sua eficácia, uma prática que deve ser incentivada em todos os sectores para garantir a preparação.

• Parte 6: Análise e comunicação pós-incidente

Após a resolução de um incidente, é essencial efetuar uma análise exaustiva para compreender o que aconteceu e como a resposta pode ser melhorada. O processo de revisão pós-incidente da ANPD ou da Agência de Cibersegurança deve ser partilhado com outras entidades para promover uma abordagem consistente à aprendizagem e à melhoria dos incidentes a nível nacional. Os

4 https://www.rivermate.com/fr/guides/guinee-bissau/accords
5 https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/4325/GNB4325.pdf

seguintes passos fundamentais descrevem a forma como esta revisão deve ser efectuada para garantir a melhoria contínua e a preparação.

- Debrief do incidente : Realizar uma sessão de debriefing com todas as partes interessadas relevantes para discutir o incidente e as ações de resposta. Incentivar outras entidades a adotar esta prática ajuda a criar uma cultura de melhoria contínua.
- Análise da causa principal: Efetuar uma análise detalhada para identificar a causa principal do incidente, fornecendo uma estrutura que outras organizações podem utilizar para reforçar as suas medidas de segurança.
- Lições aprendidas: Documentar as lições aprendidas com o incidente, concentrando-se nas melhorias que podem ser efectuadas. A partilha destes conhecimentos entre sectores garante que todas as entidades possam beneficiar da experiência.
- Relatórios : Preparar um relatório exaustivo do incidente, que pode servir de modelo a outras entidades para garantir uma documentação exaustiva e transparência.

4. Gestão de recursos

A gestão dos recursos inclui todos os procedimentos relacionados com os recursos humanos e os recursos não humanos, como o computador portátil, o software, etc.

A. Gestão dos recursos humanos

É da responsabilidade de todos os empregados de cada agência manter um bom ambiente de trabalho. Especificamente para os funcionários com poder, como gestores, diretores, diretores-gerais, etc., estes têm a responsabilidade adicional de liderar de forma a promover um ambiente de respeito por cada indivíduo.

Para atingir este objetivo, é da responsabilidade de todos os trabalhadores:

- Promover a cooperação e a comunicação leal entre colegas, com respeito e dignidade.
- Evitar conflitos no local de trabalho e, caso surjam, reagir de forma justa e rápida para facilitar a sua resolução.
- Aplicar todas as políticas de forma justa e equitativa, reconhecendo que os postos de trabalho são diferentes, mas que cada um é importante; que o desempenho individual deve ser reconhecido e medido em função de normas de avaliação pré-determinadas, conhecidas e compreendidas por todos.
- Ter em consideração as opiniões dos trabalhadores e apoiá-los no seu planeamento de carreira, a fim de criar um sentimento de pertença.
- Promover a harmonia e o espírito de equipa em todas as relações.

Para apoiar a implementação de um ambiente deste tipo, devem ser implementadas políticas e procedimentos apoiados pela direção. Estas políticas e procedimentos incluem, mas não se limitam a, o seguinte:

- Equidade no emprego
  - Cada agência deve respeitar o princípio da igualdade de acesso ao emprego. O pessoal deve ser contratado independentemente do local de origem, raça, origem étnica, ascendência, língua, credo, género, orientação sexual, idade, estado civil, religião, deficiência física e/ou mental ou capacidade financeira.
- Recrutamento e seleção
  - Todas as ofertas de emprego devem ser publicadas durante um período mínimo de cinco (5) dias úteis. Podem ser publicadas no sítio Web de cada agência e/ou em quaisquer outros painéis de emprego e/ou agências de emprego. Os funcionários internos são incentivados a candidatar-se, mas serão considerados da mesma forma que os candidatos externos.
  - Os candidatos são convidados a apresentar

6 https://www.rivermate.com/fr/guides/guinee-bissau/salaire

a sua candidatura, juntamente com um curriculum vitae atualizado, demonstrando que preenchem os critérios mínimos para o cargo em questão. Na data-limite, todos os candidatos são convidados a efetuar uma prova escrita para avaliar as suas competências técnicas e capacidades interpessoais. Os dossiers dos 3 ou 5 melhores candidatos com uma classificação positiva, consoante o nível do cargo, serão examinados e convidados para uma entrevista. Será atribuída uma nota a cada candidato com base no seu desempenho durante a entrevista. A média da nota escrita e da entrevista é a nota final. O candidato que sair em primeiro lugar deste processo com, pelo menos, uma nota de aprovação será submetido a uma verificação de ecrã, validando certificados e referências. Após resultados satisfatórios, este candidato receberá o seu contrato. Para mais pormenores, ver os diagramas do processo de contratação no Entregável 2.

- Nepotismo
  - Nenhum candidato pode ser contratado para um cargo em que seja suscetível de responder ou supervisionar um membro da sua família direta. Por família direta entende-se: pai(s), padrasto(s), pai(s) adotivo(s), irmão(s), avô(s), cônjuge (casado ou solteiro), enteado(s) ou pupilo do membro do pessoal, sogro ou sogra. As relações pessoais com outros empregados ou membros do conselho de administração ou dos comités da agência em questão devem ser reveladas antes da aceitação de qualquer oferta do empregador.
- Orientação
  - Todos os novos funcionários receberão uma sessão de orientação que inclui uma visão geral das políticas, procedimentos e operações gerais. Esta sessão permitirá também que os novos funcionários de um cargo ou da agência conheçam as expectativas de desempenho da direção para o cargo em questão. Terão acesso ao manual de políticas, assinarão um aviso de receção e tomarão conhecimento do seu conteúdo.
- Classificações dos empregados
  - Cada cargo é classificado como administrativo ou de gestão, conforme determinado pelo Diretor Executivo. Esta decisão baseia-se nas tarefas atribuídas e nas qualificações exigidas para cada cargo. Eis um exemplo de nível de classificação que pode ser utilizado:
    - Nível C1 para técnicos
    - Nível C2 para especialistas
    - Nível C3 para peritos
    - Nível B1 para gestores
    - Nível B2 para quadros superiores
    - Nível B3 para diretor
    - Nível A para Diretor Geral
- Deveres dos trabalhadores
  - O contrato de trabalho é acompanhado de uma descrição das funções e das responsabilidades associadas, bem como de quaisquer tarefas adicionais que possam ser necessárias. Este documento, juntamente com um plano de trabalho, será utilizado para avaliar o desempenho durante e após o período de estágio. Se um trabalhador não tiver a certeza do seu conteúdo, não deve hesitar em pedir esclarecimentos ao seu superior hierárquico.
  - Ocasionalmente, pode ser necessário alterar a descrição das funções de um funcionário. Estas alterações serão previamente discutidas com o trabalhador, mas a decisão final sobre a sua aplicação será tomada pela direção.
- Designação de emprego
  - As normas laborais da Guiné-Bissau reconhecem dois tipos de contratos de trabalho. São eles o contrato a termo certo e o contrato a termo indeterminado. De acordo com a legislação da Guiné-Bissau, os contratos a termo

são limitados a uma duração máxima de dois anos. Se a relação de trabalho se prolongar para além deste período, o contrato é automaticamente transformado num contrato permanente. Nas agências, os dois tipos de contrato podem assumir várias formas:

- Período a tempo inteiro: emprego como assalariado durante um período fixo e, no final desse período, o trabalhador deixa de ser assalariado.
- A tempo inteiro Indeterminado : Emprego assalariado numa base contínua, sem data de fim especificada.
- Trabalho a tempo parcial: Trabalho assalariado por um período fixo, por menos horas do que o dia de trabalho normal, a semana ou o mês e, no final do período fixo, o trabalhador deixa de ser trabalhador.
- Tempo parcial indeterminado: Emprego assalariado numa base contínua por um número de horas inferior ao dia de trabalho normal, à semana ou ao mês.
- Trabalhadores eventuais: Os trabalhadores eventuais são pagos à hora para trabalharem numa base eventual, conforme necessário. Os benefícios e as deduções serão efetuados em conformidade com a legislação em vigor na Guiné-Bissau.
- Empreiteiro : Os empreiteiros efectuam trabalhos geralmente não recorrentes, temporários e de natureza especializada. A maior parte do trabalho é efectuada fora do local. Esta pessoa não deve ser considerada como um empregado e não serão efectuadas quaisquer deduções em seu nome. O indivíduo deve faturar os serviços profissionais prestados de acordo com os termos do acordo contratual. A pessoa deve igualmente fornecer o seu próprio equipamento e ferramentas e suportar os custos relacionados com a sua utilização. O empregador pode pagar as despesas de deslocação e as despesas negociadas no contrato.

- Ficheiro pessoal
  - Cada agência recolhe informações pessoais para inclusão nos ficheiros do pessoal. Esta informação é acessível ao empregado, ao diretor geral e ao supervisor do empregado. Estas informações são mantidas num local seguro e não são partilhadas com os membros do conselho de administração ou financiadores. A informação contida no ficheiro pessoal de um funcionário inclui: curriculum vitae, carta de oferta, avaliações de desempenho, alterações às descrições de funções, reconhecimento e aceitação assinados do manual de política de recursos humanos, avisos disciplinares, formulários de impostos, quando aplicável, cópias de formulários de inscrição em benefícios e pedidos de licença aprovados.
- Liberdade condicional
  - O período experimental dura os primeiros três meses de emprego para o nível C e os primeiros seis meses para os níveis B e A. Durante este período, ambas as partes podem avaliar a sua aptidão para o trabalho. Recomenda-se vivamente que ambas as partes comuniquem à outra quaisquer situações que necessitem de ser melhoradas, se necessário, antes do final do período de estágio, para que a colaboração tenha mais hipóteses de ser bem sucedida. Este período também permite que a direção avalie os níveis de competências e aborde quaisquer áreas de potencial preocupação. Durante o período de estágio, o contrato de trabalho pode ser rescindido por qualquer das partes por qualquer motivo, com ou sem justa causa, e sem aviso prévio ou indemnização em vez de aviso prévio, com exceção das disposições mínimas estabelecidas na Lei de Emprego/Normas de Trabalho das nossas respectivas jurisdições na Guiné-Bissau, tal como pode ser alterada

periodicamente. No final do período experimental, o trabalhador e a entidade patronal reúnem-se para fazer o ponto da situação. Nesta altura, uma de três coisas acontecerá:
  - A liberdade condicional terminará
  - A liberdade condicional será prorrogada
  - O emprego terminará
- Salário
  - Os salários são determinados pelo diretor executivo, com base em considerações orçamentais e nas qualificações do candidato selecionado. A organização pagará aos empregados mensalmente, deduzidas as deduções legais e outras deduções habituais e necessárias, de acordo com as práticas normais de pagamento de salários do empregador. Estas práticas podem ser alteradas periodicamente, segundo o critério exclusivo da entidade patronal.
- Objectivos e avaliação
  - Cada supervisor deve estabelecer objetivos para o ano, para cada um dos seus recursos, com base nos objetivos globais da agência. As avaliações são efectuadas em janeiro e são determinados os objectivos do trabalhador para o ano seguinte. Os resultados e todos os elementos de prova relativos à avaliação devem ser colocados no dossier do assalariado.
- Profissionalismo
  - Ao representar a agência, os funcionários devem vestir-se e comportar-se de forma adequada. Os funcionários devem optar por vestir-se de uma forma que apresente uma imagem profissional ao público e respeite os outros. O uso excessivo de palavrões não é profissional nem respeitador dos colegas e não será tolerado.
- Horas de trabalho
  - O horário normal de expediente é das 8:00 às 12:00 e das 14:00 às 18:00, de segunda a sexta-feira inclusive (exceto feriados). Todos os funcionários devem trabalhar 8 horas por dia. Os intervalos para refeições não são remunerados. Os empregados podem também ser obrigados a trabalhar horas adicionais se solicitado ou exigido de tempos a tempos. As horas extraordinárias não devem exceder 10 horas por semana e 100 horas por ano. Os horários dos empregados contratados a tempo parcial serão determinados caso a caso.
  - Os funcionários são obrigados a informar o seu diretor/supervisor com antecedência dos dias em que planeiam ausentar-se do escritório. As ausências não planeadas do escritório devem ser comunicadas ao gestor/supervisor do empregado logo que sejam razoavelmente previsíveis. Segundo o critério do diretor executivo e dependendo das circunstâncias, os empregados podem ser autorizados a trabalhar a partir de casa durante períodos específicos, se as condições o permitirem.
- Feriados públicos/estatutários
  - Os trabalhadores com direito a subsídio de férias têm direito aos seguintes nove (9) feriados públicos/legais remunerados:
    - Feriados de data fixa :

      Dia de Ano Novo (1 de janeiro): Este dia marca o início do ano civil.

      Dia dos Heróis Nacionais (20 de janeiro): Este dia comemora o assassinato de Amílcar Cabral, uma figura-chave do movimento de independência.

      Dia Internacional da Mulher (8 de março): Este dia é dedicado à celebração das mulheres em todo o mundo.

      Dia do Trabalhador (1 de maio): Este dia celebra as contribuições dos trabalhadores de todo o mundo.

Dia da Independência (24 de setembro): Celebra a declaração de independência da Guiné-Bissau de Portugal em 1973.

Dia das Forças Armadas (14 de novembro) : Este dia homenageia as forças militares da Guiné-Bissau.

Dia de Natal (25 de dezembro): Um feriado cristão que celebra o nascimento de Jesus Cristo.

- Feriados públicos com datas variáveis :

Aïd el-Fitr (Fim do Ramadão) : Este dia marca o fim do mês sagrado muçulmano do Ramadão. A data exacta varia de ano para ano.

Aïd el-Adha / Tabaski (Festa do Sacrifício) : Este dia comemora a vontade de Ibrahim (Abraão) de sacrificar o seu filho. A data exacta varia de ano para ano.

- Horas extraordinárias
  - Todas as horas extraordinárias devem ser autorizadas pelo seu diretor/supervisor antes de serem efectuadas. A legislação laboral da Guiné-Bissau limita o número máximo de horas de trabalho por dia a 10. As horas extraordinárias são definidas como qualquer hora que exceda o dia normal de trabalho. Na Guiné-Bissau, as horas extraordinárias devem ser pagas a uma taxa pelo menos 50% superior à taxa horária normal. Além disso, o número total de horas extraordinárias é limitado a 10 horas por semana e a 100 horas por ano, dependendo do contrato.
  - As horas extraordinárias efectuadas e não compensadas serão pagas se o trabalhador se demitir ou for despedido.
- Rescisão por justa causa
  - Um contrato de trabalho pode ser rescindido pelo empregador a qualquer momento por justa causa, sem aviso prévio ou compensação por aviso de despedimento, com exceção do pagamento de salários, horas extraordinárias e férias devidas até à data da rescisão. A justa causa inclui, entre outros, qualquer ato de desonestidade, conflito de interesses, violação de confidencialidade, assédio, insubordinação, imprudência, negligência ou mau desempenho profissional documentado.
- Rescisão sem justa causa
  - O contrato de trabalho pode ser rescindido pela entidade patronal a todo o tempo e por qualquer motivo, sem justa causa, mediante aviso prévio ou pagamento de indemnização compensatória e, se for caso disso, de indemnização por despedimento, nos termos mínimos exigidos pela legislação laboral da Guiné-Bissau. Para os trabalhadores com menos de 3 anos de serviço, o período de pré-aviso é de um mês e 30 dias. Para os trabalhadores com 3 ou mais anos de serviço, o período de pré-aviso é de dois meses e 60 dias. A entidade patronal pagará uma indemnização de acordo com a legislação laboral em vigor.
- Demissão
  - O trabalhador deve notificar a entidade patronal da sua demissão com um pré-aviso de um (1) mês, se tiver menos de três (3) anos de serviço na agência, ou com um pré-aviso de dois (2) meses, se tiver mais de três (3) anos de serviço na agência. A entidade patronal pode, em qualquer altura, renunciar total ou parcialmente ao prazo de pré-aviso, mediante o pagamento do salário normal correspondente ao período assim renunciado.
- Entrevistas de saída
  - Os trabalhadores demissionários devem ser encorajados a participar numa entrevista

de saída. Será utilizado um formulário de entrevista de saída para completar cada entrevista. Este formulário garantirá que as informações sejam recolhidas de forma justa e coerente e identificará:

- O que fazemos bem
- Áreas em que podemos melhorar
- Obstáculos ao sucesso
- Feedback sobre o desempenho
- Compreender os motivos de saída dos trabalhadores

- Propriedade do empregador
  - Após a cessação do contrato de trabalho por qualquer motivo, todos os itens de qualquer tipo criados ou utilizados de acordo com o serviço do empregado ou fornecidos pelo Empregador, incluindo, mas não se limitando a computadores, relatórios, ficheiros, disquetes, manuais, literatura, informações confidenciais ou outros materiais, devem permanecer e ser considerados propriedade exclusiva do Empregador em todos os momentos, e devem ser entregues ao Diretor Executivo, em boas condições, prontamente e sem serem solicitados a fazê-lo.
- Licença de férias
  - A licença de férias será acumulada com base em:
    - Os trabalhadores acumulam férias anuais remuneradas à razão de 2,5 dias por cada mês trabalhado, ou seja, 21 dias por ano. Este valor pode variar consoante a antiguidade ou o grau profissional.
  - Estes valores serão rateados para o pessoal a tempo parcial. Uma vez que as férias se destinam a dar aos trabalhadores a oportunidade de descansar e rejuvenescer, a entidade patronal incentiva o gozo das mesmas. Os trabalhadores não podem transferir dias de férias de um ano para o outro. É da responsabilidade conjunta da direção e dos trabalhadores gerir a utilização das férias ao longo do ano. Os trabalhadores, em conjunto com as suas chefias, controlam as suas férias através do sistema RH.
- Licença por doença
  - Os trabalhadores podem beneficiar de um período máximo de 26 semanas de licença por doença remunerada, cujos pormenores são determinados pelos contratos de trabalho.
  - A licença por doença pode ser utilizada para doenças pessoais, consultas médicas pessoais e visitas a especialistas.
  - O empregador reserva-se igualmente o direito de solicitar um atestado médico para as ausências de três (3) dias ou mais.
- Licença por luto
  - A agência concederá até três (3) dias de trabalho remunerados por evento em caso de morte na família imediata do empregado. Por família direta entende-se: pai(s), padrasto(s), pai(s) adotivo(s), irmão(s), avô(s), cônjuge (incluindo a coabitação), enteado(s) ou pupilo do membro do pessoal, sogro ou sogra (incluindo o progenitor de um parceiro do mesmo sexo).
  - Podem ser concedidas licenças adicionais adicionais, à discrição do diretor executivo, por razões não abrangidas pelo presente manual. Esses pedidos devem ser discutidos com o Diretor Executivo e apresentados por escrito.
- Licença de maternidade, parental e de adoção
  - A agência respeitará as disposições da Lei das Normas de Trabalho da Guiné-Bissau em matéria de licença de gravidez e licença parental. As trabalhadoras têm direito a 14 semanas de licença de maternidade remunerada. A licença de paternidade é igualmente prevista por lei e a sua duração fica a critério da direção.
- Licença não remunerada protegida
  - A licença sem vencimento protegida inclui:

- Licença de gravidez
- Licença parental
- Licença médica familiar
- Licença de dador de órgãos
- Licença de emergência pessoal
- Licença de emergência, emergências declaradas
- Licença de cuidador familiar
- Licença para assistência a filho com doença grave
- Licença por morte ou desaparecimento de criança relacionada com o crime

- Licença sem vencimento não protegida
  - Os funcionários podem gozar uma licença sem vencimento com o consentimento escrito do Diretor Executivo. Durante os períodos de licença sem vencimento, a cobertura médica, dentária, de vida e outras são suspensas, a acumulação de licenças cessa e a antiguidade no serviço é interrompida. Muitas prestações podem ser suspensas durante o período de ausência. Serão envidados todos os esforços para reintegrar os funcionários num cargo de igual responsabilidade após o regresso da licença, mas não há garantia de que o cargo deixado esteja disponível aquando do seu regresso.
- Licença de voto
  - Em caso de votação num dia útil para os trabalhadores, a agência deve conceder-lhes o tempo necessário para se deslocarem e cumprirem a sua obrigação cívica.
- Médico, dentário, LTD, vida e AD&D
  - Todas as agências devem oferecer planos de seguro a todos os seus empregados. Estes planos devem incluir seguros de saúde, dentários, oftalmológicos, de incapacidade a longo e curto prazo, de acidentes e de vida. Estas prestações são inteiramente pagas pela entidade patronal (com exceção da cobertura familiar).
- Responsabilidade limitada na concessão de prestações
  - O direito de um trabalhador à cobertura de prestações estará sempre sujeito aos termos dos planos e das apólices, uma vez que estes podem ser reavaliados ocasionalmente, segundo o critério exclusivo de cada agência. A responsabilidade de cada agência está estritamente limitada ao estabelecimento dos planos e ao pagamento dos prémios aplicáveis. A agência não é especificamente responsável por qualquer falha ou recusa de cobertura por terceiros, por qualquer motivo, e não é responsável pela prestação dos próprios benefícios.
- Desenvolvimento profissional
  - Segundo o critério do diretor executivo, os funcionários podem participar em conferências, cursos, seminários e reuniões, identificados nos planos de trabalho anuais e nas avaliações de desempenho, que possam ser benéficos para o seu desenvolvimento profissional. Se estas oportunidades estiverem diretamente relacionadas com o cargo do funcionário ou forem sugeridas pelo diretor executivo, algumas ou todas as taxas de inscrição, materiais do curso e despesas de viagem podem ser cobertas.
  - Se a agência concordar em pagar um curso, a taxa será paga mediante prova de conclusão com êxito. Se a agência pagar um curso (ou cursos) e o funcionário deixar a agência no prazo de um ano após a conclusão do curso, a taxa do curso tornar-se-á totalmente reembolsável.
- Informações confidenciais
  - Ocasionalmente, os funcionários da Agência podem tomar conhecimento de informações confidenciais, incluindo informações sobre segredos governamentais, fornecedores, finanças e afins. Os funcionários são obrigados a manter a confidencialidade de qualquer informação que lhes seja revelada ou que

lhes seja dada a conhecer. Para além disso, qualquer informação confidencial obtida no decurso do trabalho não deve ser utilizada por um funcionário para ganho pessoal ou para promover um negócio externo.

- Propriedade intelectual
  - Toda a propriedade intelectual, como marcas registadas, direitos de autor e patentes, e qualquer trabalho criado por um funcionário no decurso do seu emprego na Agência são propriedade da Agência e considera-se que o funcionário renunciou a todos os direitos a favor da Agência. Para efeitos da presente Política, o termo "trabalho" significa trabalhos escritos, criativos ou mediáticos. Todas as fontes utilizadas em apresentações ou materiais escritos devem ser reconhecidas.
- Armazenamento e segurança da informação informática
  - Todos os dispositivos de armazenamento (CDs, pen drives, nuvem, discos rígidos) utilizados pelos funcionários da agência devem ser reconhecidos como propriedade da agência. Além disso, os funcionários devem compreender que o equipamento da empresa só deve ser utilizado para assuntos da empresa durante o horário normal de expediente. O descarregamento de documentos pessoais para o equipamento da empresa pode ser prejudicial para esse equipamento e não deve ser efectuado.
- Consumo de álcool e drogas
  - O consumo de álcool ou de drogas ilícitas não é permitido nas instalações. Ocasionalmente, com a autorização do Diretor-Geral, o álcool pode ser utilizado para celebrar uma ocasião ou um evento.
- Ambiente livre de fumo
  - É proibido fumar em todas as instalações da agência e isto aplica-se a todos os empregados, hóspedes, contratantes e visitantes. Esta política também se aplica aos veículos da empresa e a quaisquer quartos de hotel ou carros alugados reservados para fins profissionais.
- Assédio/Discriminação:
  - A Agência procura proporcionar aos seus empregados um ambiente livre de assédio e discriminação. O respeito mútuo, a cooperação e a compreensão devem ser a base das interações entre os membros e o pessoal. A Agência não tolerará nem aceitará comportamentos susceptíveis de pôr em causa a dignidade ou a autoestima de uma pessoa ou de criar um ambiente intimidante, hostil ou ofensivo.
- Procedimento de denúncia: Discriminação, assédio e violência no local de trabalho
  - Se considerar que foi pessoalmente assediado, discriminado ou sujeito a violência no seu local de trabalho, pode apresentar uma queixa por escrito. Contacte o seu departamento de recursos humanos para conhecer o procedimento de apresentação de queixa.
- Resolução de conflitos/disputas:
  - Infelizmente, podem surgir conflitos em qualquer ambiente de trabalho. A fim de resolver os conflitos de forma rápida e justa, a agência recomenda o seguinte processo de resolução de conflitos ou litígios:
    - Fale com a pessoa com quem tem um litígio. Os litígios surgem frequentemente devido a mal-entendidos e falhas de comunicação.
    - Se não for possível falar com a pessoa em causa, fale com o seu superior hierárquico. O diretor marcará uma reunião entre as pessoas envolvidas no litígio para encontrar uma solução.
    - Se o diretor não conseguir resolver um litígio no local de trabalho, as partes podem ser encaminhadas para os Recursos Humanos. A resolução do litígio pelos RH é vinculativa para ambas as partes.

- Atividade política
  - Os funcionários são livres de se envolverem em atividades políticas, incluindo a adesão a um partido político, o apoio a um candidato a eleições e a procura ativa de eleições. No entanto, as atividades políticas dos trabalhadores devem ser claramente separadas das suas atividades relacionadas com o emprego. Se participarem em atividades políticas, os funcionários devem ser capazes de manter uma perceção de imparcialidade em relação aos seus deveres e responsabilidades para com a agência.
  - Os trabalhadores não devem participar em atividades políticas durante o horário de trabalho e a política partidária não deve ser introduzida no local de trabalho. Isto não se aplica a discussões informais privadas entre colegas de trabalho.

B. Gestão dos recursos materiais e tecnológicos

Há também recursos não humanos que temos de gerir. Sem querer ser exaustivo, estes incluem :

- Utilização aceitável de telemóveis
  - Os funcionários da agência devem utilizar os seus telemóveis pessoais ou emitidos pela empresa para fins profissionais apenas durante o horário normal de expediente. Espera-se o cumprimento das seguintes regras e regulamentos:
    - Espera-se que os funcionários usem os seus telemóveis pessoais com a mesma discrição que usariam os telemóveis da empresa.
    - Os funcionários devem evitar fazer ou receber chamadas pessoais durante o horário de trabalho e utilizar os seus telemóveis pessoais apenas durante as pausas programadas ou pausas para almoço em áreas não operacionais.
    - As chamadas pessoais devem ser efectuadas fora do horário de trabalho e os funcionários devem garantir que os seus amigos e familiares são informados desta política.
    - A agência não é responsável pela perda de telemóveis pessoais trazidos para o local de trabalho.
    - Os funcionários estão estritamente proibidos de utilizar telemóveis ou dispositivos semelhantes em qualquer local de trabalho onde a utilização de tal dispositivo possa distrair o utilizador e/ou criar um ambiente de trabalho inseguro.
    - Os funcionários estão estritamente proibidos de utilizar telemóveis ou dispositivos semelhantes para qualquer outro fim (ou seja, utilização pessoal da Internet, jogos, mensagens de texto, música) durante o horário de trabalho. Estas funções podem ser utilizadas durante as pausas programadas ou períodos de refeição em áreas não operacionais.
    - Por razões de privacidade, os funcionários da Agência estão proibidos de tirar fotografias das instalações ou do pessoal da Empresa utilizando as funções de câmara dos seus telemóveis sem primeiro obterem uma autorização expressa por escrito.
- Utilização de telemóveis durante a condução:
  - É estritamente proibida a utilização manual de telemóveis durante a condução de veículos da Agência ou durante a condução de um veículo ao serviço da Agência. Para efetuar ou receber chamadas:
    - Encostar e parar
    - Utilizar um dispositivo mãos-livres ou as funcionalidades aplicáveis
    - Permitir que um passageiro utilize o telemóvel
    - Utilizar o correio de voz e atender a chamada numa altura mais segura
    - Deixe que outra pessoa conduza, permitindo-lhe fazer ou receber chamadas.

- Os funcionários são os únicos responsáveis por quaisquer multas e/ou acusações apresentadas pelas autoridades por utilização ilegal de um telemóvel durante a condução de um veículo no exercício das suas funções. Os funcionários que violem esta política podem ser sujeitos a ações disciplinares, incluindo despedimento, ou responsabilidade legal se, no exercício das suas funções, estiverem envolvidos num acidente de viação e houver provas de que estavam a utilizar o telemóvel enquanto conduziam, e o empregador for processado.

• Utilização aceitável do computador/Internet

- A tecnologia informática e os sistemas de Internet devem ser utilizados apenas para as atividades comerciais adequadas da Empresa. Todas as informações e correspondência da Agência, incluindo mensagens de correio eletrónico, transmitidas/recebidas através da nossa tecnologia informática são consideradas propriedade comercial da Empresa e devem ser geridas em conformidade para os assuntos apropriados.
- Proteção por palavra-passe:
  - O acesso à Internet é gerido através de contas de utilizador individuais e de palavras-passe confidenciais.
  - No caso de um funcionário perder, esquecer ou acreditar que a sua palavra-passe está comprometida, o funcionário deve notificar imediatamente o seu chefe. O gestor deve confirmar o nome do utilizador, repor a palavra-passe e notificar o empregado das alterações.
- Segurança:
  - Todas as palavras-passe não podem ser divulgadas ou partilhadas com outros utilizadores ou terceiros. As contas de Internet só devem ser acessíveis a utilizadores designados para fins legítimos. Os funcionários não estão autorizados a obter a palavra-passe da conta de outra pessoa. Se um utilizador tiver motivos para acreditar que a sua palavra-passe foi comprometida, deve notificar imediatamente o seu gestor.
  - Os utilizadores da Internet devem cumprir as seguintes orientações, regras e regulamentos de segurança:
  - Os ficheiros ou dados pessoais descarregados da Internet não podem ser armazenados nos discos rígidos dos computadores da Agência, nos servidores de ficheiros da rede ou nos sistemas de armazenamento de ficheiros na nuvem.
  - Os ficheiros de vídeo e áudio não podem ser descarregados da Internet, a menos que a sua utilização tenha sido autorizada para efeitos de realização de atividades da Agência.
  - Os utilizadores devem abster-se de quaisquer práticas ou procedimentos em linha que possam expor a rede ou os recursos a ataques de vírus, spyware, adware, malware ou hackers.
  - Os utilizadores são responsáveis por se familiarizarem com os procedimentos para descarregar e proteger as informações de forma segura e por identificarem e evitarem qualquer material em linha que seja considerado sensível, privado ou protegido por direitos de autor.
  - Os funcionários que utilizam a Internet devem comportar-se sempre de forma profissional, especialmente quando participam em atividades de colaboração, e não devem divulgar informações da agência ou propriedade intelectual a terceiros não autorizados.
- Utilização adequada da Internet: Os funcionários só podem utilizar a Internet para desempenhar as suas funções, de acordo com os objectivos comerciais da Agência. As atividades comerciais permitidas, aceitáveis

e adequadas relacionadas com a Internet incluem:

- Procurar, acumular e divulgar qualquer informação relacionada com o desempenho das responsabilidades atribuídas ao Utilizador, durante o horário de trabalho ou horas extraordinárias.
- Colaborar e comunicar com outros funcionários, parceiros e clientes da Agência, conforme adequado às funções e responsabilidades atribuídas ao indivíduo.
- Realização de atividades de desenvolvimento profissional (ou seja, grupos de discussão, sessões de conversação, grupos de notícias, publicações em quadros de avisos, webinars, etc.) relacionadas com as necessidades de trabalho do Utilizador.

- Utilização inadequada da Internet: A utilização inadequada e inaceitável da Internet inclui, mas não se limita a:
  - Utilização para fins ilegais, tais como roubo, fraude, calunia, difamação, assédio (sexual e não sexual), perseguição, roubo de identidade, jogos de azar em linha, propagação de vírus, envio de spam, falsificação de identidade, intimidação e plágio/violação de direitos de autor.
  - Qualquer utilização que entre em conflito com a missão, os objetivos e a reputação da Agência.
  - Copiar, destruir, modificar quaisquer dados, documentação ou outras informações pertencentes à Agência ou a qualquer outra entidade empresarial sem autorização.
  - Descarregar ficheiros excessivamente grandes pode afetar negativamente o desempenho da rede. Todos os utilizadores devem utilizar a Internet de uma forma que não interfira com a utilização de outros.
  - Aceder, descarregar ou imprimir qualquer conteúdo que viole qualquer uma das normas existentes na agência
  - políticas, ou seja, material sexualmente explícito.
  - Envolver-se em qualquer outra atividade que possa de alguma forma desacreditar ou prejudicar a agência.
  - Envolver-se em atividades comerciais pessoais online, incluindo a oferta de serviços ou produtos para venda ou a solicitação de serviços ou produtos a vendedores online.
  - Não se envolver em qualquer atividade que possa comprometer a segurança dos servidores da agência ou dos computadores anfitriões. As palavras-passe não podem ser divulgadas ou partilhadas com outros utilizadores.
  - Permitir que terceiros ou pessoas não autorizadas acedam à rede e aos recursos da agência.
- Correio eletrónico: As comunicações por correio eletrónico devem ser conduzidas com respeito e respeitar o Código de Conduta e Ética da agência. Todas as comunicações por correio eletrónico devem ser criadas com profissionalismo e atenção aos pormenores.
- Acesso e monitorização da utilização do computador/Internet: A Agência reserva-se o direito de aceder e monitorizar a utilização do correio eletrónico, computador e sistemas de Internet da Empresa pelo pessoal. Apenas o pessoal autorizado pode analisar essa utilização/registos para assuntos relacionados com a Empresa. A Agência enviará os seus melhores esforços para proteger a privacidade dos funcionários, ao mesmo tempo que exerce a devida diligência e rigor na condução de investigações relativas à utilização do correio eletrónico, computador e Internet da Empresa.

- Redes sociais Utilização pessoal
  - Redes sociais : Uma forma de comunicação eletrónica através da qual os utilizadores criam comunidades em linha para partilhar

informações, ideias, mensagens pessoais e outros conteúdos. Estas incluem, mas não estão limitadas a: Facebook, Twitter(X), LinkedIn, Pinterest, Snapchat, Tumblr, YouTube, Google Plus+ e Instagram.

- Os funcionários que mantêm páginas ou contas pessoais nas redes sociais devem cumprir as seguintes diretrizes relativamente à sua associação com a Agência. Os funcionários serão responsabilizados pelo que escreverem ou publicarem nas redes sociais ou páginas Web. Comentários inflamatórios, comentários não profissionais ou comentários depreciativos sobre a organização, os seus funcionários, clientes, fornecedores ou concorrentes podem resultar em ações disciplinares, até e incluindo a rescisão.
- Os funcionários devem seguir as diretrizes abaixo indicadas quando publicam mensagens ou comentários em qualquer sítio de redes sociais, quer seja público ou privado:
  - Os funcionários devem comportar-se de forma profissional, tanto durante como fora do trabalho. Quando um membro do pessoal se associa publicamente à agência, todos os materiais associados à sua página podem refletir a agência. Deve evitar-se comentários, fotografias, ligações, etc. inadequados.
  - As publicações que envolvam os seguintes elementos não serão toleradas e sujeitarão o empregado a ações disciplinares:
    - Informações confidenciais e exclusivas da agência
    - Declarações discriminatórias ou insinuações sexuais relativamente a colegas de trabalho, gestores, clientes ou fornecedores
    - Declarações difamatórias relativas à agência, aos seus empregados, clientes ou vendedores
- Quando um trabalhador menciona a agência, deve incluir uma declaração de exoneração de responsabilidade em que afirma que os pontos de vista expressos são da sua responsabilidade e não representam as posições, estratégias ou opiniões da empresa.
- Os funcionários que utilizam estes sítios estão proibidos de divulgar informações organizacionais privadas ou comentários negativos sobre a organização.
- Os funcionários estão proibidos de falar em nome da organização, revelar informações confidenciais, divulgar notícias ou comunicar como representante da organização sem autorização prévia para atuar como representante designado da agência.
- Os funcionários estão proibidos de utilizar as redes sociais durante o horário normal de expediente. Os funcionários devem limitar a sua utilização às pausas oficiais (ou seja, pausas para refeições). Uma vez que o acesso à Internet dentro da agência é monitorizado, tenha em atenção que a utilização excessiva das redes sociais para fins pessoais constitui um desvio do tempo e dos recursos da empresa e pode resultar em ações disciplinares.
- Os funcionários estão proibidos de utilizar materiais protegidos por direitos de autor da agência (materiais protegidos por direitos de autor, marca e/ou logótipo(s)) sem autorização prévia expressa por escrito.

5. Comunicação interna e externa

A. Canais de comunicação

Em cada agência, os canais de comunicação são essenciais para garantir que todas as comunicações sejam claras, coerentes e conformes às exigências regulamentares. Eis os tipos de canais de comunicação identificados e os seus responsáveis:

- Comunicações públicas: Todas as comunicações públicas, incluindo comunicados de imprensa, discursos e artigos, devem ser coordenadas com o responsável pelas comunicações

para garantir a coerência e a conformidade com as diretrizes regulamentares. As comunicações públicas devem ser sempre aprovadas pelo Diretor-Geral antes de se tornarem públicas. Nenhum funcionário tem o direito de partilhar informações com o público sem passar pelo processo de aprovação, sob pena de ação disciplinar, incluindo processo judicial e despedimento.

• Comunicações internas: Atualizações regulares e canais de comunicação claros dentro da organização são cruciais. Isto inclui e-mails, boletins informativos internos e reuniões para manter todos informados sobre as alterações regulamentares e os requisitos de conformidade. Outras formas de comunicação, menos supervisionadas, podem ter lugar entre os funcionários. Estas incluem discussões orais, mensagens, chamadas e afins. Em todas estas formas de configuração, a diretriz continua a ser a mesma: ser claro na mensagem a transmitir.

• Comunicações Externas : Ao comunicar-se com as partes interessadas externas, tais como agências de outros países, órgãos de soberania da Guiné-Bissau ou outras entidades, é importante utilizar modelos padronizados e garantir que toda a informação é exacta e actualizada. As pessoas autorizadas a comunicar com as partes interessadas externas estão claramente identificadas e receberam formação adequada. Conhecem as diretrizes para a partilha de informação em todas as formas de colaboração.

• Documentação: Todas as comunicações oficiais devem ser documentadas e armazenadas corretamente para referência futura e auditorias de conformidade. Isto inclui a manutenção de registos de e-mails, actas de reuniões e quaisquer outras comunicações relevantes

B. Protocolos de comunicação

Em cada agência, os protocolos de comunicação são os mesmos.

Para as comunicações oficiais, eis a lista dos protocolos de comunicação aprovados em função das necessidades:

- Boletim informativo
- Comunicado de imprensa
- Entrevista pública
- Publicação nas redes sociais
- Artigos
- Reuniões

Para as comunicações não oficiais, eis os protocolos recomendados em função das necessidades:

- Correio eletrónico
- Conversa
- Qualquer outro método de comunicação disponível permitido pela agência, desde que a mensagem a comunicar seja clara

6. Formação contínua e sensibilização

A. Oportunidades de desenvolvimento profissional

Encorajamo-lo a ter também um plano de construção de transportadoras. Isto pode aumentar a motivação dos recursos. Por exemplo, podem ser definidos vários níveis. Eis um exemplo de nível

- Nível C1 para técnicos
- Nível C2 para especialistas
- Nível C3 para peritos
- Nível B1 para gestores
- Nível B2 para quadros superiores
- Nível B3 para diretor
- Nível A para Diretor Geral

B. Programas de formação

Todo o pessoal deve receber formação e ser avaliado frequentemente para garantir que compreende, tem acesso e pode interpretar facilmente os requisitos da legislação em matéria de proteção de dados e os seus princípios para os recursos de proteção de dados e pode recomendar as melhores práticas de

cibersegurança para a Agência de Cibersegurança. O programa de formação deve ser aplicado aos novos funcionários e aos atuais. Sem ser exaustiva, esta formação deve abranger os seguintes tópicos

- Para o programa de formação sobre proteção de dados :
  - Convenção de Malabo Workshop e sessões de formação
  - Ato da CEDEAO Workshop e sessões de formação
  - Workshops e sessões de formação sobre o GDPR
- Para o programa de formação em cibersegurança :
  - Formações em cibersegurança do ISC2
  - Formações ISACA
  - Conselho da CE
  - InfoSec
- Para ambas as agências, os recursos :
  - Testes de avaliação
  - Coaching e Mentoring
  - Sessões de apoio 1:1
  - Scripts e auxiliares de lembrete

Os pormenores da formação farão parte de um relatório do resultado 4 que abrangerá o reforço das capacidades. O resultado 5, relacionado com a plataforma de e-learning, mostrará flexibilidade para os administradores acrescentarem algumas destas ações de formação, se necessário.

7. Gestão de projectos

A. Metodologia de gestão de projectos

A gestão do projeto deve ser feita, tanto quanto possível, segundo uma metodologia ágil. Este método dá mais flexibilidade e uma oportunidade de corrigir as coisas durante o processo. Existem muitos programas ágeis como o scrum.org ou outros. Todos eles partilham alguns conceitos comuns como :

- O ideal é que a equipa de desenvolvimento não exceda 8 pessoas
- A função de proprietário do produto deve ser imposta
- A função de scrum master deve ser aplicada
- A equipa de desenvolvimento deve ter reuniões scrum frequentes, que não excedam 15 minutos, idealmente todos os dias úteis.
- A sessão de preparação é importante para rever o atraso e ajustar
- O planeamento do sprint ajudará a planear a tarefa a realizar no sprint seguinte
- A retrospetiva ajudará a corrigir os aspectos negativos e a realçar os aspectos positivos.

A gestão do projeto não se resume à entrega, mas também à gestão do orçamento em conformidade com os resultados. Esta é da responsabilidade do gestor de projeto. Na ausência do gestor de projeto, o scrum master deve assumir esta responsabilidade.

B. Ferramentas e recursos de gestão de projectos

Para a metodologia ágil, são necessárias algumas ferramentas que facilitem o trabalho. Na lista, temos:

- Jira, trello ou outros para gerir a evolução das tarefas
- Ferramenta de planeamento de póquer incluída no Jira ou disponível diretamente a partir de outro fornecedor
- Sítio Confluence para documentação Wiki interna
- Sharepoint para documentos
- Excel ou SAP para gerir o orçamento do projeto

8. atividades de acompanhamento

Isto incluirá o mecanismo para validar que os processos são corretamente seguidos. O controlo envolve várias etapas fundamentais para garantir a conformidade, a eficácia e a melhoria contínua. Eis alguns componentes essenciais:

- Estabelecer normas e diretrizes: É crucial ter normas e diretrizes claras. Documentos como o Roteiro de Normas de Auditoria fornecem uma estrutura abrangente para o controlo de qualidade,

requisitos éticos e documentação de auditoria.

- Atividades de monitorização da qualidade: As principais atividades de controlo de qualidade incluem o teste do sistema de controlo de qualidade da agência, a realização de análises antes da emissão, análises de conformidade pós-emissão, apoio a análises por pares e realização de análises de causas profundas. Estas atividades estão descritas no Questionário do compromisso de revisão não pública.
- Avaliação e análise de riscos: As avaliações de risco regulares ajudam a identificar e a classificar os riscos relacionados com a confidencialidade, integridade, disponibilidade do sistema, conformidade, fiabilidade dos dados, etc.
- Documentação e manutenção de registos: É essencial a documentação adequada de todos os procedimentos de auditoria, provas obtidas e resultados da auditoria. Isto inclui a manutenção de registos de e-mails, actas de reuniões e outras comunicações relevantes.
- Auditorias e revisões regulares: A realização de auditorias e análises regulares e aleatórias garante que os processos estão a ser seguidos corretamente e ajuda a identificar áreas de melhoria. Isto inclui auditorias internas e externas para manter a transparência e a responsabilidade. Seguindo estes passos, cada agência pode monitorizar e auditar eficazmente os seus processos, garantindo a conformidade com os requisitos regulamentares e a melhoria contínua.

9. Qualidade e segurança

A. Normas de qualidade

Em cada agência, a manutenção de normas de elevada qualidade para todas as operações é essencial para garantir a conformidade, a transparência e a eficiência. Eis algumas das principais normas de qualidade que devem ser respeitadas:

- Conformidade com as leis, regulamentos e normas : Todas as operações devem respeitar as leis, os regulamentos e as normas regionais e internacionais locais. Isto inclui a implementação e manutenção de procedimentos definidos pelos proprietários da informação e a garantia de proteção e manutenção adequadas dos activos de informação
- Sistemas de gestão da qualidade: cada agência deve implementar sistemas de gestão da qualidade que cumpram os processos internos, a legislação ou requisitos locais, textos regionais como a CEDEAO e normas internacionais, como o GDPR internacional. Isto garante que todos os trabalhos de auditoria são efectuados com um elevado nível de qualidade e coerência.
- Avaliação e gestão de riscos: As avaliações devem ser efectuadas regularmente para identificar e avaliar os riscos relacionados com a confidencialidade, integridade, disponibilidade do sistema, conformidade e fiabilidade dos dados. Isto ajuda a implementar medidas de segurança eficazes e a atenuar os riscos potenciais.
- Documentação e conservação de registos: É fundamental uma boa comunicação e documentação de todos os processos e procedimentos. Para tal, cada agência deve manter registos de e-mails, atas de reuniões e outros documentos relevantes para referência futura e auditorias de conformidade
- Melhoria contínua: cada agência deve esforçar-se por obter uma melhoria contínua, revendo e atualizando regularmente os seus sistemas, políticas e procedimentos de gestão da qualidade. Isto inclui a realização de auditorias e análises regulares para identificar áreas a melhorar e implementar as alterações necessárias.

Se uma agência respeitar os critérios anteriores, deverá dispor de normas de elevada qualidade para todas as operações.

B. Norma de serviço ao cliente

No que diz respeito às normas de serviço ao cliente

em cada agência, é crucial garantir que todas as interações sejam profissionais, eficientes e estejam em conformidade com as diretrizes regulamentares. Eis alguns pontos-chave a considerar:

- Comunicação clara: Todas as comunicações, quer internas quer externas, devem ser claras, concisas e isentas de jargão. Isto garante que todas as partes interessadas, incluindo o sector público e privado, compreendem a informação que está a ser transmitida.
- Respostas atempadas: As agências reguladoras devem ter como objetivo responder prontamente aos inquéritos e pedidos. Isto ajuda a criar confiança e garante que as partes interessadas se sintam valorizadas e ouvidas.
- Documentação e manutenção de registos: É essencial a documentação adequada de todas as comunicações e interações. Isto inclui a manutenção de registos de e-mails, atas de reuniões e outros documentos relevantes para referência futura e auditorias de conformidade.
- Conformidade com os regulamentos : Todas as interações de serviço ao cliente devem cumprir os regulamentos e orientações relevantes. Isto inclui garantir que todas as informações fornecidas são exactas e atualizadas.
- Melhoria contínua : A revisão e atualização regulares dos protocolos e normas de serviço ao cliente ajudam a garantir que a agência continua a responder eficazmente às necessidades dos seus intervenientes.

Os critérios anteriores são a chave de um bom serviço ao cliente. Devem fazer parte dos valores transmitidos por cada um dos colaboradores da agência.

C. Medidas de segurança e higiene

É essencial garantir que todas as diretrizes sejam claras, abrangentes e estejam em conformidade com os regulamentos relevantes. A recente pandemia ter-nos-á lembrado de muitas coisas básicas. Cada agência deve considerar as seguintes medidas :

- Higiene pessoal: Os trabalhadores devem manter elevados padrões de higiene pessoal, incluindo a lavagem regular das mãos, a utilização de desinfectantes para as mãos e o cumprimento de práticas adequadas de higiene respiratória. O toto sobre vestuário adequado, asseio e higiene pessoal no local de trabalho.
- Limpeza do local de trabalho: A limpeza e a desinfeção regulares do local de trabalho, incluindo as áreas comuns, as casas de banho e as superfícies de contacto frequente, devem ser realizadas para manter um ambiente limpo e seguro. Isto é crucial para evitar a propagação de infecções e garantir um local de trabalho saudável.
- Formação em saúde e segurança: Os funcionários devem receber formação regular sobre protocolos de saúde e segurança, incluindo procedimentos de emergência, utilização adequada de equipamento de proteção individual (EPI) e primeiros socorros. Isto assegura que todos estão conscientes das medidas de segurança e sabem como reagir em caso de emergência.
- Comunicação e gestão de incidentes: Deve ser estabelecido um protocolo claro para a comunicação e gestão de incidentes, tais como acidentes ou questões relacionadas com a saúde. Isto inclui a manutenção de registos de incidentes e a realização de revisões regulares para identificar áreas a melhorar.
- Conformidade com os regulamentos: Todas as medidas de segurança e higiene devem estar em conformidade com os regulamentos locais e com as melhores práticas padrão. Isto inclui a implementação e manutenção de procedimentos de segurança definidos pelos proprietários da informação e a garantia de uma proteção e manutenção adequadas dos bens de informação.

Estas medidas ajudarão cada agência a garantir um ambiente de trabalho seguro e saudável para os seus empregados.

10. Documentação suplementar da agência

Seguem-se alguns modelos ou documentação adicional que podem ser úteis para documentar ou apoiar o manual de operações pormenorizado.

- Estratégia nacional de cibersegurança: cria um quadro que orienta o Governo da Guiné-Bissau para ajudar a proteger os cidadãos e as organizações das ciberameaças. Há um projeto WARDIP a trabalhar neste documento. Eis um exemplo de um ponto que se espera que seja abordado no documento:

Amostra de elementos a incluir na estratégia nacional de cibersegurança
Resumo executivo ■ O lugar da Guiné-Bissau num mundo digital ■ A importância da cibersegurança ■ A visão da Estratégia Nacional de Cibersegurança: Segurança e prosperidade na era digital ■ mbito de aplicação da estratégia ■ Implementação da estratégia Introdução ■ Tirar partido dos pontos fortes da Guiné-Bissau num cenário cibernético dinâmico Segurança e resiliência ■ Contexto estratégico: A evolução da ciberameaça ■ Cibercriminalidade e ciberameaças avançadas ■ O impacto crescente ■ Consulta pública sobre cibersegurança ■ Segurança e resiliência dos sistemas da Guiné-Bissau Inovação cibernética ■ Contexto estratégico: Expansão das fronteiras da cibersegurança ■ Novos Horizontes de Tecnologia e Desenvolvimento Empresarial ■ Tirar partido das vantagens da tecnologia digital ■ Promoção das competências e conhecimentos do século XXI ■ Consulta pública sobre cibersegurança ■ Um ecossistema cibernético inovador e adaptável Liderança e colaboração ■ Contexto estratégico: Colaborar para concretizar os benefícios da vida digital ■ Aumentar a segurança cibernética de base na Guiné-Bissau ■ Liderança nacional em matéria de cibersegurança num ambiente dinâmico ■ Consulta pública sobre cibersegurança ■ Liderança, governação e colaboração eficazes Glossário do livro de exercícios

Quadro 03: Exemplo de conteúdo para a estratégia nacional de cibersegurança

- **Modelo de plano de continuidade das atividades:**

Equipa de planeamento para a continuidade das atividades

Papel	Nome	Posição atual/ Função	E-mail	Telefone	Emergência #
Coordenador do plano de continuidade das atividades			Autocarro: Casa:	Autocarro: Casa: Célula	
Coordenador de apoio			Autocarro: Casa:	Autocarro: Casa: Célula	
Membros da equipa de planeamento			Autocarro: Casa:	Autocarro: Casa: Célula	
			Autocarro: Casa:	Autocarro: Casa: Célula	
Membros da equipa de apoio			Autocarro: Casa:	Autocarro: Casa: Célula	
			Autocarro: Casa:	Autocarro: Casa: Célula	
Gestores de sítios locais			Autocarro: Casa:	Autocarro: Casa: Célula	
			Autocarro: Casa:	Autocarro: Casa: Célula	
Equipa de cibersegurança			Autocarro: Casa:	Autocarro: Casa: Célula	

Quadro 04: Modelo de plano de continuidade das atividades

- **EssClassificação dos serviços/funções essenciais:**

Serviço/unidade de negócio: _____

Áreas afetadas e grau de influência

Nome do serviço	Serviço 1	Serviço 2	Serviço 3	Serviço 4	Serviço 5	Serviço 6
Nível de importância do serviço essencial						
Finanças						
Empregados						
Clientes						
Tecnologia / Cibersegurança						
Fornecedores / parceiros comerciais						
Jurídico/regulamentar						
Público / comunidade						
Outros						
Pontuação total (estabelecer prioridades e elaborar a lista de serviços)						

Pontuação baixa = fraca influência negativa *Pontuação alta = forte influência negativa*

Quadro 05 : Modelo Áreas afetadas e grau de influência

- **Fator de criticidade dos serviços essenciais**

Identificação das funções e serviços essenciais por nível de importância

Unidade de serviço/negócio:_____

Nível de importância do serviço essencial	**A.**			**B.**			**C.**		
Nome do serviço									
Número atual de empregados que prestam serviços									
Número restante de trabalhadores se for aplicada uma taxa de absentismo de 35%									
Grau de risco (elevado, médio, baixo)									
Possibilidade de trabalhar a partir de casa (Sim ou não?)									
Tecnologia utilizada									
Plano de ação implementado para o serviço essencial (Sim ou não?)									

Quadro 06: Modelo de serviços essenciais

Legenda do nível de importância :

A. *Serviço crucial. Não pode ser interrompido ou suspenso.*

B. *Serviços/funções que podem ser suspensos por um curto período de tempo (por exemplo, um mês).*

C. *Serviços/funções que podem ser suspensos por um longo período de tempo.*

- **Plano de ação para manter o serviço/atividade essencial**

Modelo de plano de ação para manter um serviço/atividade essencial

Departamento/unidade económica:			
Serviço essencial (Identificar e fornecer uma breve descrição)			
Indivíduo/posição responsável pela execução plano de ação específico	(Nome)	(Números de telefone)	(Endereços de correio eletrónico)
Pessoa/posição de apoio responsável pela execução plano de ação específico			
Questões relacionadas com o impacto nas empresas (enumerar todas)			
Plano de ação (Enumerar o plano de ação, incluindo, plano de notificação, comunicações estratégia, plano de reafectação do pessoal, utilização de outros serviços do sector, qualquer alteração do âmbito da prestação de serviços, necessidades de controlo e informação, etc.)			
Necessidades de recursos (Enumerar as necessidades e os contactos dos recursos necessários - pessoal, equipamento, contratação de serviços, tecnologia)			

Quadro 07: Modelo de plano de ação para manter um serviço/atividade essencial

- **Principais clientes, fornecedores, prestadores de serviços ou parceiros**

Modelo de plano de ação para manter o serviço/atividade essencial: principais clientes

Produto/serviço:	
Nome do cliente/fornecedor/parceiro:	
Endereço de rua:	
Cidade/área/caixa postal:	
Pessoa de contacto: Contacto alternativo:	Número de telefone: 24 horas N.º: Fax n.º: Outro n.º: Correio eletrónico: E-mail:
Comentários:	

Quadro 08 : Modelo de formulário de contacto dos recursos-chave externos

- **Modelo de cartão de informação de contacto**

CARTÃO DE INFORMAÇÃO DE CONTACTO DA PESSOA	
Título da função (por exemplo, diretor-geral)	
Nome próprio :	
Apelido :	
Endereço de correio eletrónico do escritório :	
Número de telefone do escritório :	
Horário de expediente	

Quadro 09: modelo de cartão de informação de contacto para uma pessoa

CARTÃO DE CONTACTO PARA O SERVIÇO	
Nome do serviço (por exemplo, serviço de apoio informático)	
Serviço Endereço de correio eletrónico :	
Número de telefone de serviço :	
Horário de atendimento	

Quadro 10: modelo de cartão de informação de contacto para o serviço

- **Modelo de SOP**

SOP : Nome do SOP	
Versão e data de criação/atualização :	
Descrição e objetivo :	
O âmbito de aplicação :	
Procedimento	
Funções e responsabilidades :	
Documentação e manutenção de registos	
Análise e revisão	

Quadro 11 : Modelo de SOP

IV. CONCLUSÃO

Neste relatório, temos o manual de funcionamento da Agência para a Proteção de Dados e da Agência para a Cibersegurança. Começámos por identificar as orientações a respeitar. Em seguida, foram identificadas e documentadas as principais atividades de cada agência. Sem serem exaustivos, estes procedimentos permitirão o bom desempenho das atividades e uma boa continuidade das atividades. A fim de garantir e controlar o cumprimento correto dos procedimentos, recomendamos a realização de auditorias internas e externas com regularidade.

A maioria destes procedimentos exige competências técnicas. Para tal, propusemos um plano de formação de alto nível. No próximo entregável 4, o plano de formação será pormenorizado. O entregável 5, que diz respeito à criação da plataforma de e-learning, apoiará determinados cursos de formação.

Este manual operacional deve ter o apoio dos quadros superiores para ser adotado pela maioria dos empregadores.

Powered by :
BS Innovations & GoSecure
09/2024