



Modelo de Política de Segurança da Redação

Guiné-Bissau



Financiado pela
União Europeia



REPORTERES
SEM FRONTEIRAS



Agradecimentos

O presente documento foi elaborado no âmbito do projeto de apoio ao sector dos media, com duração de 18 meses, intitulado « *Promover e proteger a democracia ao salvaguardar a liberdade de opinião e de expressão e combater a mis/desinformação na Guiné-Bissau* ».

O projeto é financiado pela União Europeia e implementado pela Fundação dos Media para a África Ocidental (MFWA), em colaboração com Repórteres Sem Fronteiras (RSF) e Fondation Hirondelle (FH).

Isenção de Responsabilidade

O conteúdo deste documento é da exclusiva responsabilidade da Fundação dos Media para a África Ocidental (MFWA) e não pode, em circunstância alguma, ser considerado como refletindo a posição da União Europeia.

Índice

Introdução	1
1. Declaração de Política	2
2. Segurança Integrada	3
3. Âmbito de Aplicação	3
4. Estrutura de Responsabilidades	4
5. Avaliação de Riscos	5
6. Segurança Física	5
7. Segurança Digital	5
8. Proteção de Fontes	6
9. Segurança Jurídica	6
10. Segurança Editorial	6
11. Apoio Psicossocial	7
12. Gestão de Incidentes	7
13. Cooperação Institucional	8
14. Formação	8
15. Revisão e Responsabilização	8
16. Anexos Operacionais	9
Anexo A: Lista de Verificação para Avaliação de Riscos	10
Anexo B: Ficha de Contatos de Emergência	13
Anexo C: Orientações de Segurança Digital	14
Anexo C (2): Checklist Digital para Reportagens	15
Anexo D: Registo de Incidentes de Segurança	16
Anexo E: Checklist de Segurança para Publicações Sensíveis	18

Introdução

A presente Política de Segurança da Redação foi elaborada no âmbito do projeto financiado pela União Europeia, implementado pela Fundação dos Media para a África Ocidental (MFWA), em coordenação com Repórteres Sem Fronteiras (RSF) e Fondation Hironnelle (FH), tendo sido revista e consolidada após processo participativo de validação envolvendo organizações de media e profissionais da comunicação social da Guiné-Bissau.

A política surge num contexto marcado por riscos multidimensionais para jornalistas e trabalhadores da comunicação social, incluindo ameaças, agressões físicas, assédio, intimidação jurídica, ataques digitais, pressões políticas, interferências editoriais e desgaste psicossocial.

O documento baseia-se no UN Plan of Action on the Safety of Journalists (UNESCO/ONU), nos UNESCO Safety Indicators e nas diretrizes da RSF, CPIJ, IFJ e IMS, bem como na Constituição da República da Guiné-Bissau e na legislação nacional aplicável à comunicação social.

O seu objetivo é estabelecer um sistema integrado de proteção dos jornalistas e das redações, reforçando a segurança, a resiliência institucional e a liberdade de imprensa.

A eficácia desta política depende da sua aplicação contínua, monitorização regular e integração efetiva no funcionamento quotidiano das redações.

1. Declaração de Política

Esta Política de Segurança constitui parte integrante da cultura institucional da redação e aplica-se a todos os seus membros, colaboradores e parceiros.

A redação compromete-se a:

- Priorizar a segurança humana acima da urgência editorial ou da publicação;
- Adotar tolerância zero contra violência, assédio, intimidação, discriminação ou ameaças;
- Implementar medidas específicas de prevenção e resposta a assédio, intimidação e violência contra mulheres jornalistas e outros grupos vulneráveis;
- Integrar a Segurança Integrada (física, digital, jurídica, editorial, psicossocial e proteção de fontes) em todas as fases do trabalho jornalístico;
- Promover uma cultura de prevenção, solidariedade e responsabilidade coletiva;
- Garantir que nenhum jornalista será prejudicado, sancionado ou retaliado por reportar incidentes de segurança.

2. Segurança Integrada

A Segurança Integrada combina seis dimensões interdependentes:

1. Segurança Física;
2. Segurança Digital e da Informação;
3. Segurança Jurídica;
4. Segurança Psicossocial;
5. Segurança Editorial e Ética;
6. Proteção de Fontes e Denunciantes.

Estas dimensões devem ser tratadas de forma articulada, reconhecendo que fragilidades numa área podem comprometer a segurança global da redação.

3. Âmbito de Aplicação

A política aplica-se a:

- Jornalistas permanentes, *freelancers* e colaboradores;
- Editores, direção e pessoal técnico;
- Estagiários e estudantes em prática profissional;
- Missões nacionais e internacionais relacionadas com a atividade jornalística.

A redação reconhece que *freelancers*, jovens jornalistas e estagiários podem enfrentar vulnerabilidades acrescidas, devendo beneficiar de mecanismos adequados de proteção e acompanhamento.

4. Estrutura de Responsabilidades

Função	Responsabilidades
<i>Direção / Editores-Chefes</i>	Garantir recursos, aprovar missões, fornecer equipamentos, supervisionar protocolos, assegurar apoio jurídico e médico
<i>Pessoa Responsável pela Segurança (Ponto Focal)</i>	Atualizar protocolos, monitorizar riscos, gerir incidentes, realizar briefings, manter contactos de emergência
<i>Jornalistas e Pessoal</i>	Cumprir protocolos, reportar ameaças, proteger fontes e utilizar corretamente ferramentas de segurança

O Ponto Focal de Segurança deverá possuir acesso direto à direção editorial e capacidade de ativação imediata dos mecanismos de resposta a incidentes.

A atribuição de responsabilidades específicas não exime a redação da responsabilidade coletiva pela segurança de todos os seus membros.

5. Avaliação de Riscos

- Toda missão em ambiente sensível requer avaliação prévia de riscos;
- Missões classificadas como de risco elevado exigem aprovação superior e medidas reforçadas;
- Jornalistas mulheres, jovens repórteres e *freelancers* recebem atenção adicional devido a vulnerabilidades específicas;
- Os formulários e autorizações devem ser arquivados digitalmente durante, pelo menos, 12 meses após a missão.

6. Segurança Física

- Identificação profissional visível quando apropriado;
- Equipamentos de proteção adequados;
- Transporte seguro e comunicação contínua;
- Protocolos específicos para protestos, comícios e operações policiais;
- Planos de evacuação e retirada rápida.

7. Segurança Digital

- Palavras-passe fortes e autenticação de dois fatores;
- Encriptação de dispositivos e dados sensíveis;
- Utilização de redes seguras;
- Formação contínua em cibersegurança;
- Protocolos de resposta a assédio e ataques digitais.

8. Proteção de Fontes

A redação garante:

- Confidencialidade;
- Canais seguros de comunicação;
- Proteção reforçada em investigações sensíveis;
- Armazenamento seguro de dados;
- Proibição de divulgação não autorizada.

9. Segurança Jurídica

- Acesso imediato a apoio jurídico;
- Informação sobre direitos legais dos jornalistas;
- Procedimentos em caso de detenção, confisco de material ou processos;
- Verificação editorial reforçada para evitar alegações infundadas.

Todas as medidas devem respeitar a Constituição da República da Guiné-Bissau, a Lei de Imprensa e as normas internacionais de direitos humanos ratificadas pelo Estado.

10. Segurança Editorial

- As decisões editoriais devem considerar impactos na segurança;
- Devem ser registadas interferências externas;
- É proibida autocensura forçada ou pressão editorial indevida;
- Devem existir orientações específicas para coberturas sensíveis.

11. Apoio Psicossocial

- *Debriefings* após missões de risco;
- Encaminhamento para apoio psicológico;
- Prevenção de stress traumático e *burnout*;
- Mecanismos contra assédio e *bullying*.

A redação compromete-se a promover ambiente inclusivo, seguro e solidário.

12. Gestão de Incidentes

- Sistema confidencial de reporte sem risco de retaliação;
- Registo atualizado de incidentes;
- Produção de relatórios periódicos para análise interna;
- Cooperação com entidades de proteção.

Os incidentes graves devem ser avaliados no prazo máximo de 24 horas, com definição imediata de medidas de proteção sempre que necessário.

A redação deverá promover revisões periódicas dos incidentes reportados, visando identificar padrões de risco, melhorar protocolos e reforçar medidas preventivas.

13. Cooperação Institucional

Em caso de detenção, agressão, desaparecimento, ameaça grave ou confisco ilegal:

1. Notificação imediata às autoridades competentes;
2. Contacto com advogados e organizações de proteção;
3. Avaliação da necessidade de apoio institucional adicional;
4. Solicitação formal de investigação.

14. Formação

- Formação regular para toda a redação;
- Inclusão de freelancers e estagiários;
- Simulações de situações de risco;
- Atualização periódica sobre segurança digital, jurídica e operacional.

15. Revisão e Responsabilização

- A política será revista anualmente;
- O *feedback* da redação será integrado;
- O incumprimento grave dos protocolos poderá implicar medidas disciplinares;
- A implementação da política deverá ser objeto de acompanhamento periódico.

16. Revisão e Responsabilização

Anexo	Finalidade
A	Lista de Verificação e Avaliação de Riscos
B	Ficha de Contactos de Emergência
C	Orientações de Segurança Digital
C (2)	Checklist Digital para Reportagens
D	Registo de Incidentes de Segurança
E	Checklist para Publicações Sensíveis

Mensagem Final

A segurança dos jornalistas não depende apenas da existência formal de políticas e protocolos.

Constrói-se através de prática contínua, responsabilidade institucional, solidariedade profissional e compromisso coletivo com a liberdade de imprensa.

Anexo A: Lista de Verificação para Avaliação de Riscos

A preencher antes de missões de risco (eleições, protestos, investigações, áreas remotas, conflitos).

1. Dados da Missão

Título da missão: _____

Data e local: _____

Jornalista(s): _____

Editor/Supervisor: _____

2. Como Utilizar a Checklist

- Cada item assinalado (✓) = 1 ponto
- Some os totais por secção

Classificação Final:

- **0–6 = Risco Baixo** (avançar com precauções normais)
- **7–12 = Risco Médio** (reforçar medidas de segurança)
- **13–22 = Risco Elevado** (exige medidas reforçadas ou reconsideração da missão)

3. Avaliação

A) Contexto e Ambiente (0-4)

- ☐ Missão politicamente sensível
- ☐ Envolve protestos/violência
- ☐ Área com ameaças recentes à imprensa
- ☐ Presença provável de grupos hostis

Subtotal: ___ /4

B) Segurança Física (0-4)

- ☐ Missão politicamente sensível
- ☐ Envolve protestos/violência
- ☐ Área com ameaças recentes à imprensa
- ☐ Presença provável de grupos hostis

Subtotal: ___ /4

C) Segurança Digital e da Informação (0-4)

- ☐ Dispositivos sem encriptação/password forte
- ☐ Dados sensíveis ou fontes em risco
- ☐ VPN indisponível / internet insegura prevista
- ☐ Falta plano de proteção de fontes

Subtotal: ___ /4

D) Riscos Jurídicos e Políticos (0–3)

- ☐ Risco de detenção / intimidação
- ☐ Legislação relevante não revista
- ☐ Contacto jurídico indisponível

Subtotal: ____/3

E) Saúde e Bem-Estar (0–3)

- ☐ Riscos de saúde conhecidos no local
- ☐ Sem seguro médico
- ☐ Apoio psicossocial não previsto

Subtotal: ____/3

F) Comunicação e Emergência (0–4)

- ☐ Ponto Focal de Segurança não designado
- ☐ Sem plano de “*check-in*”
- ☐ Contactos de emergência não partilhados
- ☐ Rota de evacuação não identificada

Subtotal: ____/4

Pontuação Total: ____/22

- ☐ Aprovada
- ☐ Aprovada com condições
- ☐ Não aprovada

Editor/Supervisor: _____

Assinatura: _____ **Data:** / _____

Anexo B: Ficha de Contatos de Emergência

Atualização obrigatória pela Pessoa Responsável pela Segurança.

I. Números de Emergência (Guiné-Bissau)

- **Emergência geral:** 112
- **Polícia da Ordem Pública:** 117 | 1414 (MTN) | 1515 (Orange)
- **Polícia Judiciária:** 121
- **Bombeiros:** 118 | 1212 (MTN) | 1313 (Orange)
- **Ambulância / Hospital:** 119
- **Linha Saúde:** 1919 (MTN) | 2020 (Orange)

II. Apoio Jurídico

- **Liga Guineense dos Direitos Humanos (LGDH):**
+245 95 333 222 | liga.guinebissau@gmail.com
- **WANAMDEL – Rede Oeste-Africana da MFWA:**
+233 302 555 327 | +233 302 955 213 | info@mfw.org

(Recomenda-se que cada redação inclua os seus próprios advogados ou contactos locais adicionais.)

Anexo C: Orientações de Segurança Digital

1. Dispositivos e Contas

- Usar **Palavras-passe fortes** (≥ 12 caracteres);
- Ativar **2FA** no e-mail e redes sociais;
- Manter dispositivos atualizados;
- Encriptar telemóveis e portáteis;
- Não partilhar dispositivos sem verificação.

2. Comunicação Segura

- Usar **Signal** ou **WhatsApp** para conteúdos sensíveis;
- Evitar Wi-Fi público sem **VPN**;
- Fazer *backups* regulares;
- Verificar identidade de contactos.

3. Proteção de Fontes

- Encriptar dados sensíveis;
- Usar pseudónimos para fontes vulneráveis;
- Evitar guardar dados desnecessários;
- Eliminar ficheiros sensíveis quando já não forem necessários.

4. Redes Sociais

- Evitar partilhar dados pessoais;
- Separar contas pessoais e profissionais;
- Não entrar em confrontos online;
- Reportar assédio de imediato ao Ponto Focal.

5. Em Caso de Incidente Digital

- Desligar o dispositivo da internet;
- Guardar provas (capturas de ecrã, mensagens);
- Informar o Ponto Focal e apoio técnico;
- Notificar entidades de proteção.

Anexo C (2): Checklist Digital para Reportagens

1. Antes da saída

- ☐ Dispositivos carregados e atualizados
- ☐ Palavras-passe fortes e 2FA ativo
- ☐ VPN instalada e testada
- ☐ Aplicações encriptadas prontas
- ☐ Dados sensíveis encriptados
- ☐ *Backup* feito
- ☐ Fontes anónimas
- ☐ Redes sociais revistas
- ☐ Contactos de emergência guardados

2. Durante a reportagem

- ☐ Evitar Wi-Fi público sem VPN
- ☐ Não partilhar dispositivos
- ☐ Cautela com links/anexos desconhecidos
- ☐ Contacto regular com o Ponto Focal

3. Em caso de incidente

- ☐ Desligar internet
- ☐ Guardar provas
- ☐ Reportar ao Ponto Focal
- ☐ Escalar para entidades de proteção

Anexo D: Registo de Incidentes de Segurança

Data: _____ Hora: _____

Local: _____

Jornalista: _____

Função: _____

Testemunhas / envolvidos: _____

Tipo de incidente:

- ☐ Ameaça verbal
- ☐ Assédio online
- ☐ Agressão física
- ☐ Detenção / intimidação policial
- ☐ Confisco / destruição de equipamento
- ☐ Violação de dados
- ☐ Tentativa de aceder a fontes
- ☐ Outro: _____

Consequências imediatas:

- ☐ Danos físicos
- ☐ Danos emocionais
- ☐ Perda de equipamento
- ☐ Violação de dados
- ☐ Interferência no trabalho
- ☐ Outro: _____

Descrição factual do incidente:

Ações tomadas – Internas:

- ☐ Comunicação ao editor
- ☐ Recolha de provas
- ☐ Reforço de proteção
- ☐ Apoio psicológico
- ☐ Outro: _____

Ações tomadas – Externas:

- ☐ Queixa à polícia
- ☐ Contacto MFWA/UNESCO/LGDH
- ☐ Apoio jurídico
- ☐ Outro: _____

Recomendações: _____

Assinaturas:

Jornalista: _____

Ponto Focal: _____

Data: ____ / ____ / _____

Anexo E: Checklist de Segurança para Publicações Sensíveis

1. Verificação Editorial

- ☐ Informação verificada com ≥ 2 fontes
- ☐ Fontes confidenciais protegidas
- ☐ Documentos autenticados
- ☐ Sem dados pessoais desnecessários

2. Avaliação de Risco

- ☐ Possível retaliação contra jornalista?
- ☐ Risco para fonte/informante?
- ☐ Risco de incitamento ao ódio?
- ☐ Consultado editor e Ponto Focal?

3. Linguagem e Ética

- ☐ Linguagem neutra
- ☐ Sem difamação ou acusações sem prova
- ☐ Sem estereótipos
- ☐ Separação clara entre factos e opinião

4. Segurança Digital

- ☐ Documento protegido e encriptado
- ☐ Ficheiros sensíveis seguros
- ☐ Comunicação com fontes via canais seguros
- ☐ Metadados verificados/limpos

5. Revisão Legal

- ☐ Cumprimento da Lei de Imprensa
- ☐ Sem violação de segredo judicial
- ☐ Sem elementos difamatórios
- ☐ Parecer jurídico (quando necessário)

6. Aprovação Final

- ☐ Editor responsável – aprovado
- ☐ Ponto Focal – validado
- ☐ Direção (alto risco) – validado

**Scanear para
baixar cópia digital**

