***Plantilla de Protocolo de Seguridad Física y Digital para Periodistas***

## Introducción

**Objetivo del protocolo:** Garantizar la seguridad del periodista durante sus actividades profesionales mediante medidas físicas y digitales.

**Alcance:** Aplicable a todas las etapas del trabajo periodístico (antes, durante y después de la cobertura).

## Información General

- Nombre del periodista:
- Contacto de emergencia:
    - Nombre:
    - Teléfono:
- Relación:
    - Organización o medio:
    - Nombre:
- Contacto:

## Evaluación de Riesgos

- Lugar de la cobertura:
- Tipo de cobertura:
    - ( ) Manifestación
    - ( ) Zonas de conflicto
    - ( ) Investigación
    - ( ) Otro:
- Actores identificados:
    - Aliados:
    - Potenciales amenazas:
- Análisis de entorno:

    - Riesgos físicos:
    - Riesgos digitales:
- Nivel de riesgo (1-5):
    - Probabilidad:
    - Impacto:
    - Resultado (probabilidad × impacto):

## Medidas de Seguridad Física

**Antes de la Cobertura:**

- Planificación de rutas seguras y puntos de evacuación.
- Información del itinerario compartida con contacto de confianza.
- Preparación del equipo:
    - ( ) Chaleco antibalas
    - ( ) Casco
    - ( ) Botiquín de primeros auxilios
    - ( ) Cargador portátil
- Verificación del contexto local (protestas, bloqueos, presencia de grupos armados).

**Durante la Cobertura:**

- Mantener un perfil bajo (ropa discreta, sin logos llamativos).
- Identificar puntos estratégicos para posicionarse.
- Comunicación constante con el contacto de confianza.
- Evitar enfrentamientos o confrontaciones.

**Después de la Cobertura:**

- Evaluación de incidentes.
- Verificación de posibles seguimientos físicos.
- Revisión de equipos y respaldo de datos.

## Medidas de Seguridad Digital

**Antes de la Cobertura:**

- Uso de herramientas seguras:
    - Aplicaciones de comunicación cifrada (e.g., Signal, Telegram).
    - VPN activada para navegación segura.
- Revisión de dispositivos:
    - Actualización de sistemas operativos y aplicaciones.
    - Cifrado de archivos sensibles.
- Contraseñas seguras:
    - Cambiadas antes de la cobertura.
    - Activación de autenticación en dos pasos.

**Durante la Cobertura:**

- Evitar conexiones a redes Wi-Fi públicas.
- Monitoreo constante de dispositivos por comportamientos inusuales.
- Envío regular de datos a respaldos seguros.

**Después de la Cobertura:**

- Análisis de posibles intentos de hackeo o accesos no autorizados.
- Cambio de contraseñas y revisión de configuraciones de seguridad.
- Respaldar y cifrar toda la información recopilada.

## Plan de Contingencia

**Escenarios Críticos y Acciones a Tomar:**

- Detención Arbitraria:
    - Acción: Mantener la calma, solicitar identificar a la autoridad y contactar al abogado o red de apoyo.
    - Contacto clave: Nombre: _____ Teléfono: _____
- Seguimiento o vigilancia detectada:

    - Acción: Cambiar de ruta, buscar refugio en un lugar seguro y notificar a un contacto de confianza.

- Confiscación de equipos:
    - Acción: Reportar el incidente a la organización y respaldar la información previamente cifrada.
- Emergencia médica:
    - Acción: Dirigirse al hospital más cercano o activar el plan de evacuación.
- Puntos médicos identificados:

## Contactos Clave y Recursos

- Contacto de confianza:
    - Nombre: _____
    - Teléfono: _____
- Abogado o asesor legal:
    - Nombre: _____
    - Teléfono: _____
- Organización de apoyo:
    - Nombre: _____
    - Teléfono: _____

## Seguimiento y Evaluación

- Fecha de revisión del protocolo: _____
- Lecciones aprendidas de la cobertura anterior: _____
- Ajustes realizados en el protocolo: _____

## Notas Finales:

Este protocolo debe ser revisado y ajustado antes de cada nueva cobertura. Mantén siempre actualizados tus contactos clave y las herramientas de seguridad utilizadas.