conectivas
TEJIENDO REDES DE INCLUSIÓN

POLÍTICA DE SEGURIDAD DIGITAL INTERSECCIONAL Y SISTEMA DE CUIDADO

Modelo integrado de protección y participación sostenible

Conectivas ONG
Organización de Mujeres con Discapacidad

POLÍTICA DE SEGURIDAD DIGITAL INTERSECCIONAL Y SISTEMA DE CUIDADO

MODELO INTEGRADO DE PROTECCIÓN Y PARTICIPACIÓN SOSTENIBLE

CONECTIVAS ONG

Organización de mujeres con discapacidad en Guatemala

2026

conectivas

TEJIENDO REDES DE INCLUSIÓN

ÍNDICE

1. SÍNTESIS EJECUTIVA

¿POR QUÉ ESTO ES UNA INVERSIÓN ESTRATÉGICA, NO UN COSTO ADMINISTRATIVO?

En contextos de incidencia política, la violencia digital contra mujeres con discapacidad no es un riesgo marginal o una externalidad manejable. Es un mecanismo sistemático de exclusión que debilita la calidad de la participación, erosiona la sostenibilidad de los procesos y desactiva actores estratégicos.

Esta política se construye a partir de la experiencia concreta de Conectivas: identificar patrones de ataque, comprender sus efectos políticos y diseñar respuestas que protejan sin paralizar, que visibilicen sin exponer.

1.1 Argumento central

- **Sin protección:** La carga de la exposición recae individualmente sobre participantes, causando retiro, autocensura y pérdida de legitimidad política.
- **Con sistema integrado:** La protección es colectiva y estructurada, permitiendo participación sostenida, incidencia de calidad y continuidad institucional.

1.2 Propuesta de valor para donantes

- **Protección del retorno de la inversión:** Asegura que los actores clave mantengan su participación a lo largo del ciclo del proyecto.
- **Mejora de resultados de incidencia:** Sin autocensura, la calidad del posicionamiento político y las propuestas es superior.
- **Prevención de crisis:** Evita costos emergentes de manejo de crisis, acompañamiento de emergencia y restitución de daño.
- **Modela buenas prácticas:** Genera conocimiento replicable sobre seguridad digital interseccional en espacios de incidencia.

1.3 Rango de inversión

5-10% del presupuesto total del proyecto, integrado como costo directo de implementación (no administrativo).

2. CONTEXTO Y FUNDAMENTOS

2.1 POSICIONAMIENTO POLÍTICO Y ÉTICO

Esta política se fundamenta en tres ejes conceptuales que no son decorativos sino operacionales:

Enfoque de derechos humanos y feminista

La seguridad digital se entiende como condición previa para el ejercicio de derechos de participación política, libertad de expresión y acceso a información. No se trata de proteger a individuos, sino de proteger procesos colectivos de incidencia.

Perspectiva anticapacitista

Se reconoce que la violencia digital contra mujeres con discapacidad no es idéntica a la violencia contra otros actores. Los ataques utilizan la discapacidad como mecanismo de deslegitimación, invalidación y exclusión. La estrategia de protección debe ser sensible a estas especificidades.

Interseccionalidad como método

Género, discapacidad y posicionamiento político no operan de forma aislada. Se refuerzan mutuamente, produciendo formas específicas de riesgo. El análisis y la respuesta deben considerar estas intersecciones de forma explícita.

2.2 TENSIÓN CENTRAL: VISIBILIDAD VS. SEGURIDAD

Esta política no pretende eliminar la visibilidad. La visibilidad es parte constitutiva del trabajo político de incidencia. El desafío es gestionar los riesgos de la exposición de forma colectiva, evitando que recaigan individualmente sobre quienes participan.

La paradoja resuelta: no se busca que las mujeres con discapacidad desaparezcan del espacio público. Se busca que su presencia no genere vulnerabilidades específicas.

2.3 MARCO DE CONOCIMIENTO SITUADO

Esta política no responde a estándares prediseñados de seguridad informática. Se construye desde la sistematización de experiencias concretas de Conectivas, que permite:

- Identificar patrones reales de ataque (no hipotéticos)
- Comprender sus efectos en la participación y la incidencia
- Diseñar respuestas que sean cultural y políticamente coherentes

3. ANÁLISIS DE RIESGOS SITUADOS

La experiencia de Conectivas ha permitido identificar patrones diferenciados de violencia digital que operan de forma sistemática, no como hechos aislados:

3.1 MATRIZ DE PATRONES DIFERENCIADOS

PATRÓN	MANIFESTACIÓN	EFECTO POLÍTICO
Deslegitimación política	Narrativas que posicionan a las defensoras como actores ocultos o funcionales a intereses políticos, utilizando su participación en espacios de derechos humanos como evidencia de un supuesto sesgo.	Debilita su legitimidad para opinar y participar en espacios de decisión política.
Capacitismo de invalidación	Comentarios y discursos que cuestionan la capacidad de las defensoras para opinar, decidir o incidir, desplazando el debate político hacia el cuerpo y la condición de discapacidad.	Excluye del debate político; funciona como despolitización.
Infantilización y condescendencia	Discursos que aparentan protección o empatía, pero niegan el reconocimiento como sujetas políticas con criterio propio.	Reduce su participación; limita la percepción de sus aportes en el espacio público.
Exposición de datos	Circulación de números de teléfono, direcciones y datos de contacto obtenidos de listados de asistencia, memorias de eventos y documentos difundidos en espacios de derechos humanos.	Llamadas dirigidas, manipulación, riesgos de extorsión. Incrementa vulnerabilidad y dependencia.

3.2 EFECTO MÁS CRÍTICO: RESTRICCIÓN DE LA PARTICIPACIÓN

En contextos donde las mujeres con discapacidad dependen de redes de cuidado, los ataques digitales pueden ser utilizados como argumento para limitar su presencia en espacios públicos, reforzando dinámicas de control. De esta manera, la violencia digital no solo afecta la integridad en línea. Reconfigura las condiciones materiales de participación.

4. ARQUITECTURA OPERATIVA DEL SISTEMA

El sistema se estructura en componentes interdependientes que operan simultáneamente:

4.1 MARCO POLÍTICO Y ÉTICO

Define el enfoque de derechos humanos, feminista y anticapacitista que orienta todas las decisiones. Explicita la tensión entre visibilidad y seguridad y proporciona criterios para resolverla en contextos específicos.

4.2 ARQUITECTURA DE INFORMACIÓN

- **Clasificación de información:** pública, sensible, crítica
- **Reglas de acceso:** quién puede acceder, según contexto
- **Protocolos de almacenamiento:** dónde se guardan, cómo se protegen
- **Gestión de circulación:** cómo se comparten datos sin exponer a participantes

4.3 EVALUACIÓN PREVIA DE RIESGOS

Antes de cualquier participación o visibilidad pública, se evalúa:

- Contexto político y nivel de polarización
- Historial de ataques contra la organización o actores similares
- Vulnerabilidades específicas de la persona (dependencias, visibilidad previa, estado actual)
- Capacidad de respuesta y acompañamiento disponible

4.4 PROTOCOLO DE RESPUESTA ESCALONADO

La respuesta se diferencia según nivel de riesgo:

NIVEL	INDICADORES	ACCIONES INMEDIATAS	ESCALAMIENTO
BAJO	Críticas menores, discrepancias sin coordinación, aisladas.	Documentación, monitoreo, comunicación con participante.	Análisis en reunión de equipo semanal.
MEDIO	Coordinación de cuentas, desinformación, campañas débiles de deslegitimación.	Activación de protocolo, respuesta coordinada, acompañamiento intenso.	Reunión de respuesta rápida, evaluación de respuesta pública.
ALTO	Violencia directa, campañas coordinadas, exposición de datos personales, amenazas.	Activación inmediata, acompañamiento 24/7, respuesta estratégica, asesoría legal.	Contacto con aliados, cooperación con autoridades, redes de protección.

4.5 ESTRATEGIA DE RESPUESTA PÚBLICA

- **Responder:** cuando la respuesta amplifica el mensaje político y debilita la narrativa del atacante
- **No responder:** cuando el silencio estratégico es más efectivo o cuando la respuesta podría incrementar vulnerabilidad
- **Escalar narrativamente:** conectar ataques específicos con patrones más amplios (capacitismo, violencia política de género)
- **Activar aliados:** movilizar a actores solidarios para amplificar el mensaje sin exponer más a la persona atacada

4.6 SISTEMA DE CUIDADO COMO COMPONENTE ESTRATÉGICO

El cuidado es parte de la arquitectura operativa, no un aspecto complementario:

- **Distribución de carga emocional:** los efectos psicológicos de los ataques no recaen individualmente
- **Retiro informado:** quien necesita pausar puede hacerlo sin culpa, con respaldo institucional
- **Acompañamiento continuo:** conexión con redes de apoyo emocional y material

5. EQUIPO Y CAPACIDADES REQUERIDAS

5.1 ESTRUCTURA MÍNIMA

1. **Responsable de Sostenimiento y Cumplimiento:** gestión de protocolos, monitoreo, coordinación de respuesta, acompañamiento
2. **Equipo de respuesta rápida:** rol de monitoreo, rol de comunicación estratégica, rol de cuidado y acompañamiento
3. **Asesoría técnica externa:** seguridad digital, protección de datos, herramientas
4. **Asesoría legal:** para escalamientos, denuncias, protección jurídica

5.2 CAPACIDADES CLAVE

- Análisis político de ataques (no técnico, sino de efectos políticos)
- Comunicación estratégica y gestión de narrativa
- Acompañamiento psicosocial y gestión de trauma
- Manejo de herramientas de seguridad digital básica
- Coordinación y gestión de protocolos
- Sensibilidad a interseccionalidad, género y discapacidad

5.3 FORMACIÓN CONTINUA

El sistema requiere actualización trimestral de conocimientos sobre nuevos patrones de ataque, herramientas emergentes y análisis de incidentes.

6. MODELO DE INVERSIÓN Y SOSTENIBILIDAD FINANCIERA

6.1 ARGUMENTACIÓN CENTRAL

La seguridad digital y el sistema de cuidado no son costos administrativos ni complementarios. Son condiciones operativas para garantizar que la participación de mujeres con discapacidad en procesos de incidencia ocurra sin generar daño, desgaste o distorsión de resultados.

La evidencia de Conectivas demuestra que en ausencia de esta inversión, los costos de la exposición —violencia digital, deslegitimación, sobrecarga y retiro— son absorbidos individualmente por las participantes, debilitando la sostenibilidad del proyecto.

6.2 RIESGOS DE NO IMPLEMENTAR

- Reducción de participación efectiva en espacios clave
- Retiro parcial o total de actores estratégicas
- Distorsión de resultados por autocensura y restricción de exposición
- Aumento de costos no planificados (crisis, manejo reactivo, acompañamiento emergente)
- Debilitamiento de legitimidad de la incidencia
- Pérdida de inversión en capacitación y desarrollo de actores

6.3 COMPONENTES FINANCIADOS

Componente 1: Gestión política de la exposición

- Evaluación previa de riesgos
- Decisiones estratégicas de visibilidad
- Acompañamiento estratégico a participantes
- Comunicación con aliados antes de participaciones públicas

Componente 2: Respuesta y protección

- Monitoreo de incidentes (herramientas, tiempo del equipo)
- Activación de protocolos escalonados
- Gestión de información crítica
- Coordinación de respuesta pública

Componente 3: Sostenimiento de la participación

- Distribución de carga emocional
- Acceso a acompañamiento psicosocial
- Sistema de retiro informado
- Conexión con redes de cuidado

6.4 ESTRUCTURA DE COSTOS

CONCEPTO	UNIDAD	COSTO ANUAL
Responsable de Sostenimiento y Cumplimiento	Salario	USD 15,000
Herramientas de seguridad digital	Anual	USD 2,000
Asesoría técnica en seguridad digital	Horas / año	USD 3,000
Asesoría legal	Casos / año	USD 2,000
Formación continua del equipo	Anual	USD 1,500
TOTAL ANUAL		**USD 23,500**

Estos costos varían según el contexto y la intensidad de la implementación. El modelo de inversión porcentual (5-10% del presupuesto del proyecto) es más flexible y se ajusta a la escala del financiamiento.

6.5 MODELO PORCENTUAL DE INVERSIÓN

1. **Rango recomendado:** 5-10% del presupuesto total del proyecto
2. **Integración:** como costo directo de implementación, no como administrativo
3. **Justificación:** la seguridad digital es condición operativa para la calidad de la incidencia

Ejemplos de aplicación:

- Proyecto de USD 200,000: inversión en seguridad = USD 10,000 - 20,000
- Proyecto de USD 500,000: inversión en seguridad = USD 25,000 - 50,000
- Proyecto de USD 1,000,000: inversión en seguridad = USD 50,000 - 100,000

6.6 ESCENARIOS DE IMPLEMENTACIÓN

Escenario mínimo (5% del presupuesto)

Capacidad básica de monitoreo y respuesta:

- Responsable part-time (0.25 FTE) de coordinación de protocolos
- Herramientas básicas de seguridad
- Asesoría técnica externa según necesidad
- Respuesta reactiva a incidentes

Escenario intermedio (7% del presupuesto)

Fortalecimiento significativo de capacidades:

- Responsable part-time (0.5 FTE) con dedicación específica
- Sistema completo de herramientas
- Asesoría técnica y legal regular
- Respuesta proactiva con evaluación previa de riesgos
- Sistema básico de cuidado integrado

Escenario robusto (10% del presupuesto)

Sistema completo con máxima capacidad:

- Responsable full-time (0.5 FTE + dedicaciones complementarias)
- Monitoreo 24/7 en momentos de riesgo alto
- Asesoría técnica y legal permanente
- Sistema completo de cuidado con acceso a especialistas
- Articulación con redes de protección externas

6.7 CONTRIBUCIÓN A RESULTADOS DEL PROYECTO

- **Sostiene la participación:** actores clave se mantienen activos a lo largo del ciclo del proyecto
- **Reduce deserción:** minimiza pérdida de recursos humanos por desgaste o retiro forzado
- **Mejora la calidad:** sin autocensura, el posicionamiento y las propuestas políticas son más sólidas
- **Protege la inversión:** previene costos emergentes de crisis y manejo reactivo
- **Genera conocimiento:** produce modelos replicables de seguridad digital interseccional

7. INDICADORES Y MONITOREO

7.1 INDICADORES DE PROCESO

- Evaluaciones de riesgo previas realizadas / participaciones públicas planificadas
- Incidentes identificados y documentados
- Protocolos activados según nivel de riesgo
- Tiempo de respuesta desde identificación del incidente
- Sesiones de formación del equipo realizadas

7.2 INDICADORES DE IMPACTO

- Tasa de permanencia de participantes estratégicas en espacios de incidencia
- Reducción de retiros por causas relacionadas a violencia digital
- Calidad y amplitud de intervenciones políticas (sin autocensura)
- Satisfacción de participantes con el sistema de acompañamiento
- Reportes de carga emocional distribuida (vs. carga individual)

7.3 MONITOREO TRIMESTRAL

Se realizarán análisis de:

- Patrones de ataque emergentes
- Efectividad de protocolos implementados
- Lecciones aprendidas
- Ajustes necesarios para la siguiente fase

8. SOSTENIBILIDAD INSTITUCIONAL

8.1 INTEGRACIÓN INSTITUCIONAL

La seguridad digital debe ser parte de la gobernanza institucional de Conectivas, no un proyecto paralelo. Esto significa:

- Rol definido en la estructura organizacional
- Presupuesto garantizado más allá de ciclos de proyectos específicos
- Procesos y protocolos documentados y accesibles
- Capacitación continua del equipo

8.2 ESTRATEGIA DE MOVILIZACIÓN DE FONDOS

Donantes de incidencia política

Fundaciones que financian incidencia y defensa de derechos son los más proclives a entender la lógica de inversión. Argumentación clave: la seguridad digital es condición operativa para que la incidencia sea efectiva y sostenible.

Donantes de derechos humanos

Fondos especializados en protección de defensores de derechos humanos entienden directamente la necesidad. Se puede conectar con programas regionales de seguridad de activistas.

Donantes de género y discapacidad

Existen fondos globales especializados en género y en derechos de personas con discapacidad que pueden co-financiar como reconocimiento de las intersecciones.

Cooperación bilateral

Agencias de cooperación internacional (especialmente de países con agendas fuertes en derechos digitales) pueden incluir este componente en acuerdos de cooperación más amplios.

8.3 ESTRATEGIA DE COSTOS COMPARTIDOS

- Cada proyecto de incidencia que usa el sistema contribuye proporcionalmente al costo base
- Fondos dedicados cubren asesoría especializada y herramientas centralizadas
- Presupuesto central de Conectivas cubre parte de la gestión y coordinación

8.4 ESCALABILIDAD

El modelo está diseñado para ser replicable:

- Procesos y protocolos documentados pueden adaptarse a otros contextos
- Formación de capacidades puede transferirse a otras organizaciones
- Herramientas y tecnología pueden compartirse o adaptarse

9. CONCLUSIÓN

La Política de Seguridad Digital Interseccional y Sistema de Cuidado de Conectivas no es una iniciativa defensiva o complementaria. Es una propuesta de transformación de cómo se gestiona la incidencia política cuando los actores son mujeres con discapacidad en contextos de violencia.

Su financiamiento representa una inversión en:

- **Protección real:** no teórica, sino operativa y verificable
- **Calidad política:** incidencia sin restricciones ni autocensura
- **Sostenibilidad:** participación que se mantiene a lo largo del tiempo
- **Conocimiento:** modelos replicables en otros contextos y geografías

En contextos de incidencia política, no financiar estas condiciones mínimas de seguridad implica asumir riesgos que afectan directamente los resultados del proyecto. Esto es una propuesta de buena administración del financiamiento internacional.