Documento Clasificado – Nivel IV
Asignación de Misión – Unidad de Ciberinteligencia
Referencia: OPS-CYB-INT/2025-0615
Destino: Agente Especial [BLACK 3301]

Resumen Ejecutivo:

En virtud de la alerta emitida por la División de Ciberdelincuencia de INTERPOL el pasado 12 de junio de 2025, se ha detectado una campaña coordinada de intrusión en sistemas críticos de seguridad digital en jurisdicciones pertenecientes a la Unión Europea, Norteamérica y Sudamérica. Dicha campaña ha sido atribuida preliminarmente a un actor APT de carácter transnacional, con patrones de ataque consistentes y objetivos estratégicos.

Designación Operativa:

Usted ha sido designado como enlace operativo entre nuestra unidad nacional de ciberinteligencia y el centro de coordinación de INTERPOL en Lyon. Su historial en operaciones de infiltración digital, nivel de acceso y acreditación de seguridad, lo convierten en el candidato designado para cumplir esta misión con la debida confidencialidad.

Objetivos de la Misión

1. Analizar los indicadores de compromiso (IoCs) y artefactos técnicos compartidos por los centros CSIRT internacionales.
2. Infiltrar las infraestructuras de comando y control (C2) sin comprometer la visibilidad del atacante.
3. Recolectar evidencia digital bajo estándares forenses certificados (cadena de custodia).
4. Cooperar en tiempo real con unidades espejo ubicadas en Berlín, Ottawa y Bogotá a través de nodos seguros habilitados para este fin.

Marco Legal y Normativo

Toda la operación estará regida por el *Convenio de Budapest sobre Ciberdelincuencia*, el *Reglamento Europeo de Ciberseguridad (EU 2019/881)*, y los acuerdos bilaterales de ciber-cooperación firmados por España con entidades aliadas. El más estricto cumplimiento normativo será condición indispensable para la validez de cualquier acción ejecutada o evidencia recolectada.

Consideraciones Finales:

Esta misión no contempla intervención armada. Su éxito dependerá de su capacidad de operar con precisión, discreción y plena conciencia del escenario diplomático que implica.

Dirija cualquier reporte, anomalía o validación directamente al nodo seguro LIN/INT-CB-041 y evite cualquier canal de comunicación no cifrado fuera del entorno operativo autorizado.