



OPERACIÓN RANSOM II

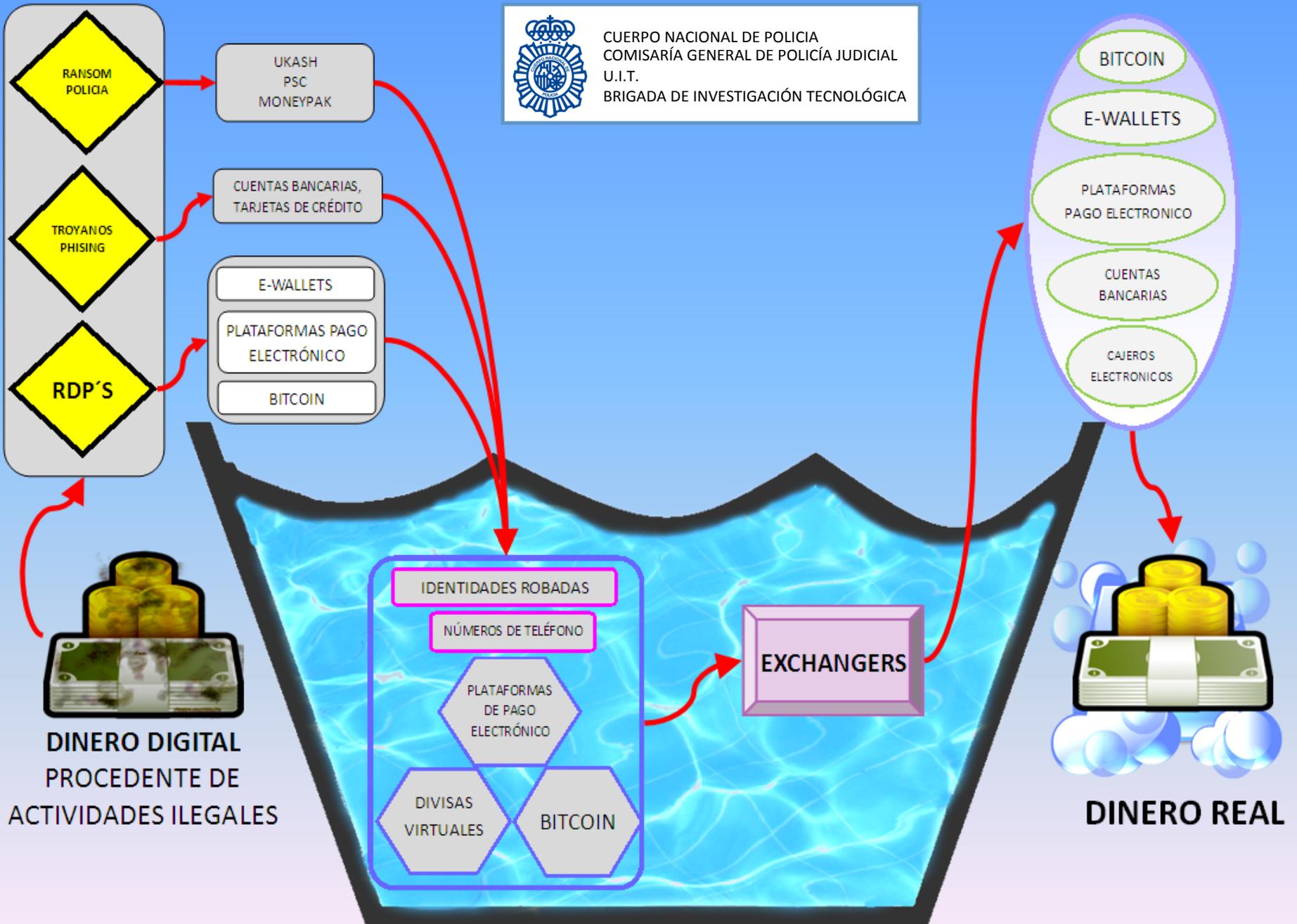
CUERPO NACIONAL DE POLICIA
COMISARÍA GENERAL DE POLICÍA JUDICIAL
U.I.T.
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA



BLANQUEO DE CAPITALES ELECTRÓNICO



CUERPO NACIONAL DE POLICIA
COMISARÍA GENERAL DE POLICÍA JUDICIAL
U.I.T.
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA



**DINERO DIGITAL
PROCEDENTE DE
ACTIVIDADES ILEGALES**

DINERO REAL

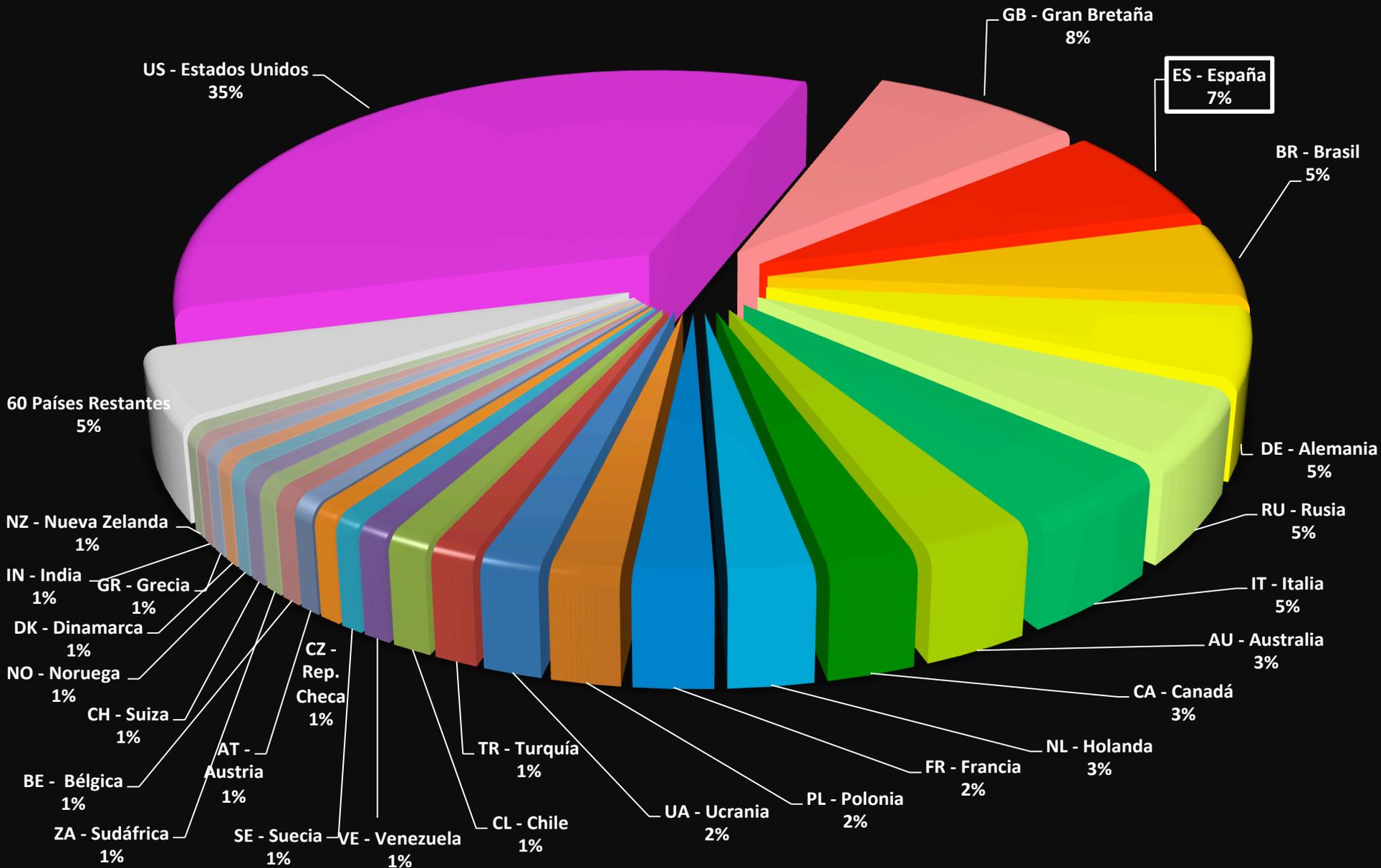


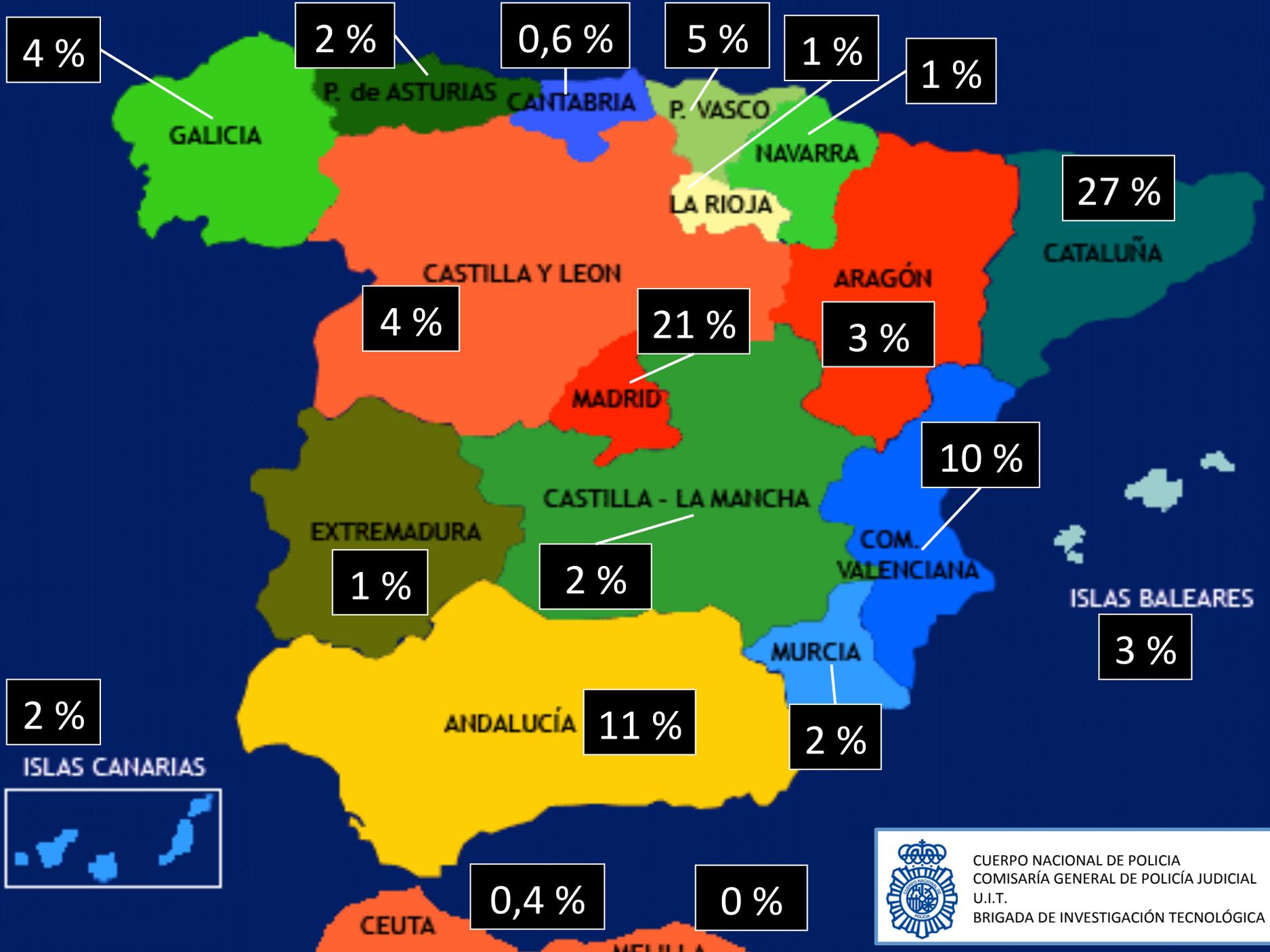
SERVIDORES
COMPROMETIDOS



CUERPO NACIONAL DE POLICIA
COMISARÍA GENERAL DE POLICÍA JUDICIAL
U.I.T.
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA

ORDENADORES COMPROMETIDOS

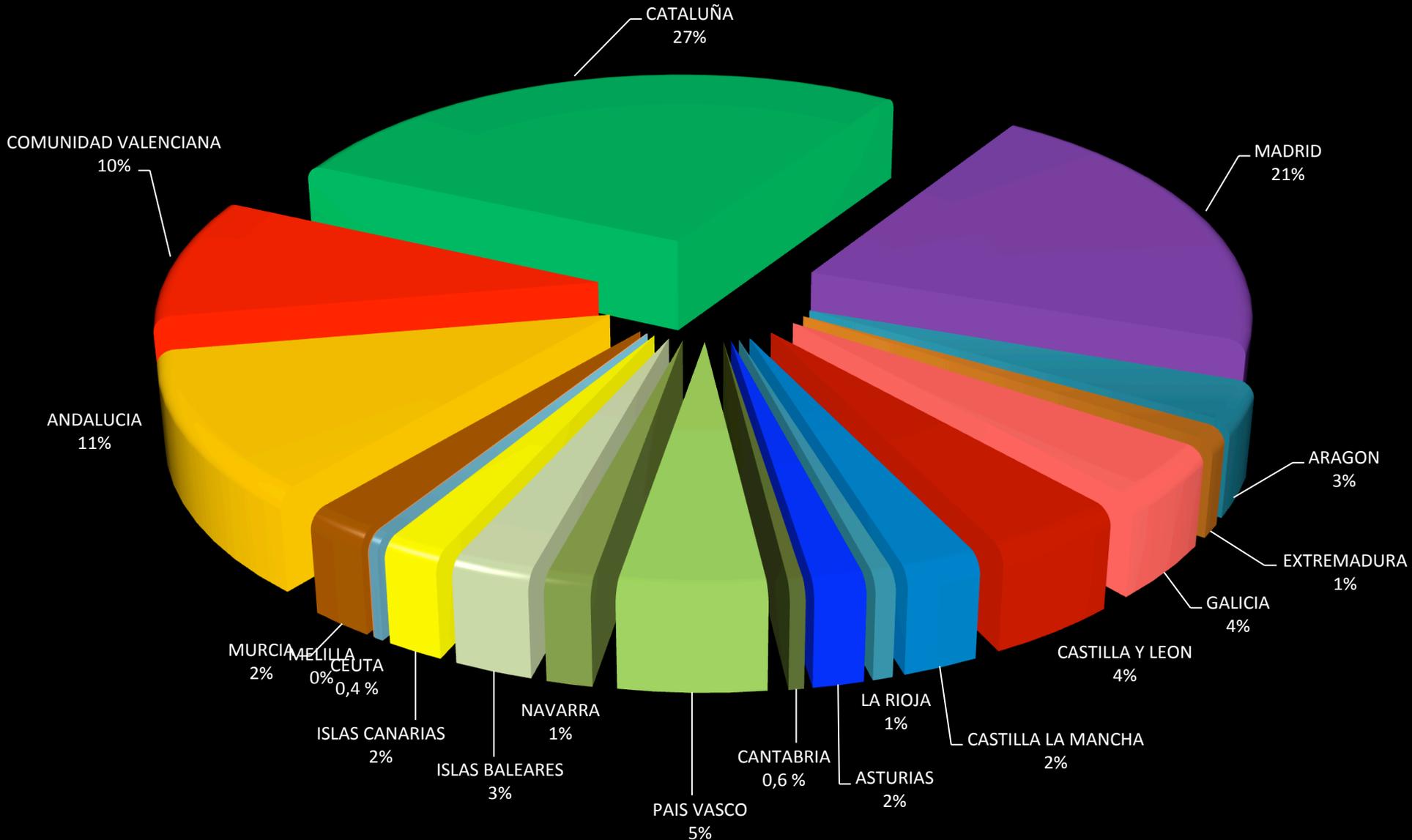






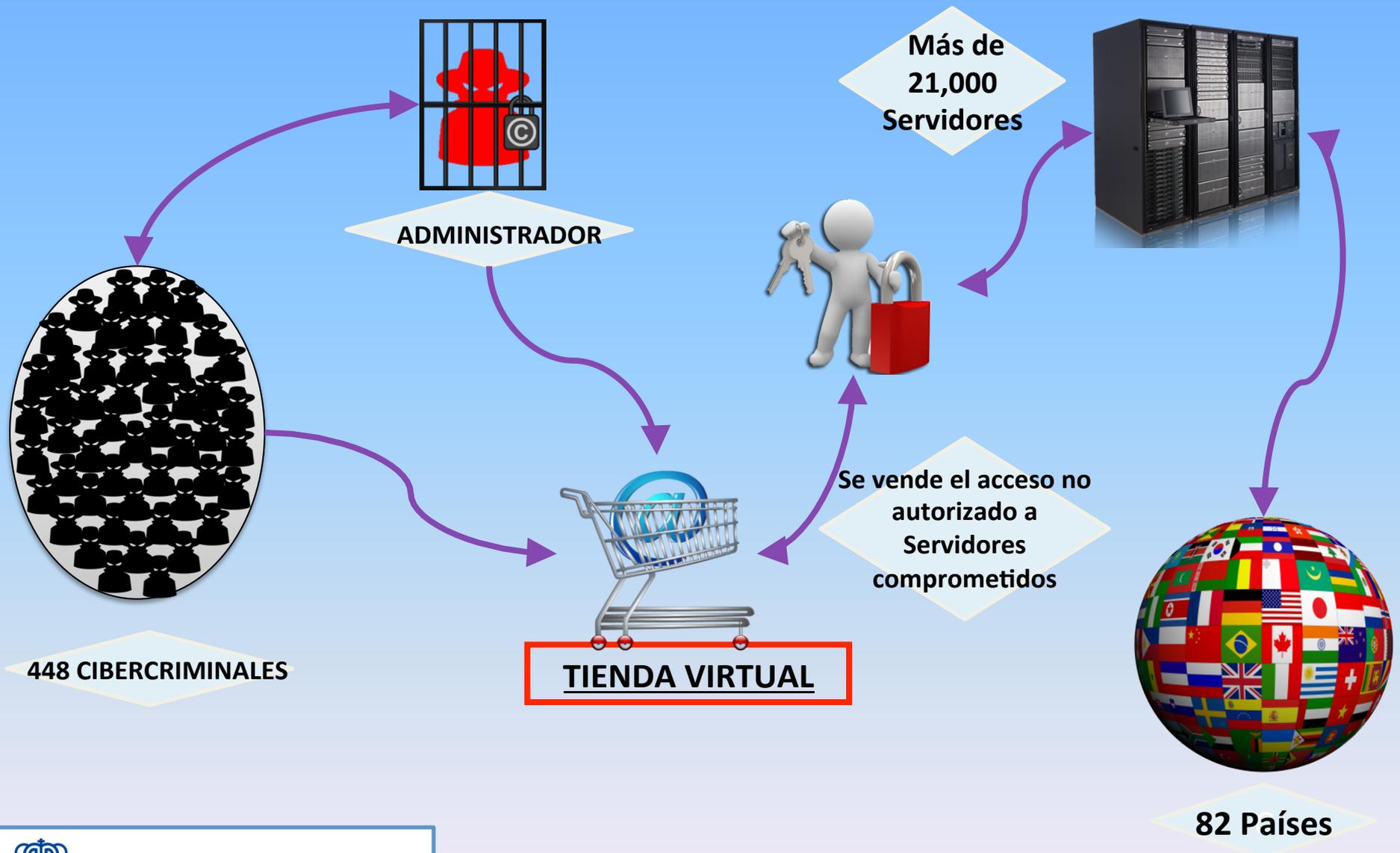
CUERPO NACIONAL DE POLICIA
COMISARÍA GENERAL DE POLICÍA JUDICIAL
U.I.T.
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA

ORDENADORES COMPROMETIDOS EN ESPAÑA





FUNCIONAMIENTO
TIENDA VIRTUAL DE
SERVIDORES
COMPROMETIDOS



BOTNET

PARTICULARES



ZOMBI



INFECCIÓN

- Virus
- Troyanos
- Malware

Determinadas ordenes

Disponible cuando está encendido

Actúan en conjunto

DDoS

Robo Credenciales

SPAM

Abuso de publicidad

Romper contraseñas

SERVIDORES RDP

SERVIDORES DE:
PYMES
CORPORACIONES
ORGANISMOS
UNIVERSIDADES



NO ZOMBI



SIN INFECCIÓN

Obtención contraseñas usando técnicas de Fuerza Bruta



Escritorio Remoto



Control Total

Infraestructura

Distribución Malware

Extorsión

Blanqueo de capitales electrónico



CUERPO NACIONAL DE POLICIA
COMISARÍA GENERAL DE POLICÍA JUDICIAL
U.I.T.
BRIGADA DE INVESTIGACIÓN TECNOLÓGICA



COMUNICADO VÍCTIMAS

“Por orden del Juzgado Central número 3 de la Audiencia Nacional, se le comunica que en la investigación llevada a cabo por la Unidad Central de Investigación Tecnológica del Cuerpo Nacional de Policía dentro de las Diligencias Previas 70/2012 de dicho juzgado, se ha descubierto que su dirección IP está siendo ofrecida y/o utilizada, sin su conocimiento ni consentimiento, en al menos un foro de ciberdelictivos para que mediante un acceso remoto pueda ser usada con fines delictivos.

Póngase en contacto con el Instituto Nacional de Tecnologías de la Comunicación <INTECO> -organismo oficial dependiente del Ministerio de Industria, Energía y Turismo- a través de la cuenta de correo electrónico incidencias@cert.inteco.es para recibir información y consejos sobre medidas de seguridad a adoptar.

Dicho organismo oficial ha sido expresamente autorizado por el juzgado a tal fin dado el elevado número de afectados.”

