ANEXO – IPs SOSPECHOSAS Y METODOLOGÍA PARA PERITOS UFECI

I. IPs Relevadas —

Acceso remoto no autorizado. -

— Intentos de login fallidos consecutivos. -

— Actividad nocturna fuera del patrón habitual.

Acceso IMAP sin intervención del denunciante.

II. Patrones detectados - Accesos fuera de geolocalización habitual. - Cambios SMTP/IMAP no autorizados. - Variaciones abruptas en headers Received-from. pronexo@gmail.com

III. Metodología sugerida para UFECI 1. Trazado de IPs (traceroute extendido). 2. Correlación de logs entre proveedor de correo y dispositivo. 3. Análisis de headers completos (DKIM, SPF, DMARC). 4. Revisión de sesiones activas (tokens OAuth, IMAP connections). 5. Peritaje de integridad de archivos ZIP y evidencia asociada.

De: Unidad de Respuesta Inmediata <uri@minseg.gob.ar>
Enviado: jueves, 20 de noviembre de 2025 16:29
Para: Juan Manuel De Castro <viking.power@outlook.com>
Asunto: Re: Acceso a documentaci=F3n relevante para investigaci=F3n de corr=
upci=F3n en Santa Fe y Otras