PROTOCOLO INTEGRAL DE INVESTIGACIÓN Y AUDITORÍA DE CEROS ENERGÉTICOS

Aplicación prioritaria a los sistemas eléctricos aislados de Canarias

PROPÓSITO DEL DOCUMENTO

Establecer un método completo, reproducible e independiente para investigar un cero energético: desde la secuencia física inmediata hasta las causas técnicas, organizativas, regulatorias y estructurales que permitieron que una perturbación evolucionara hasta el colapso total o casi total del sistema.

Canarias Sostenible

Documento técnico de referencia - Versión 1.0
3 de noviembre de 2026

Estado: propuesta metodológica profesional. No sustituye una investigación oficial, un peritaje judicial ni un dictamen jurídico.

Control del documento

Elemento	Contenido
Título	Protocolo Integral de Investigación y Auditoría de Ceros Energéticos en Sistemas Eléctricos Aislados
Ámbito	Sistemas eléctricos aislados; aplicación prioritaria a los Sistemas Eléctricos No Peninsulares de Canarias
Versión	1.0 - 3 de noviembre de 2026
Objetivo	Investigar hechos, conformidad técnica, causas directas, factores contribuyentes, condiciones latentes, fallos de barreras, reposición y causas estructurales
Uso previsto	Administraciones públicas, operadores, transportistas, distribuidores, generadores, expertos independientes y organizaciones interesadas en la seguridad de suministro
Limitación	La aplicación a un incidente real exige acceso íntegro a los datos primarios, documentación de configuración, modelos y personal técnico de los agentes implicados.

ADVERTENCIA SOBRE EL TÉRMINO "ÁRBITRO INDEPENDIENTE"

Este documento incorpora una metodología de revisión adversarial y arbitraje técnico separada de los equipos autores. En una investigación real, el árbitro debe ser una persona o panel externo, sin participación previa en el diseño, operación, mantenimiento o análisis del incidente. La revisión aplicada para preparar esta versión es una revisión metodológica interna y no equivale a una certificación externa independiente.

Contenido

- 1. Resumen ejecutivo
- 2. Alcance, principios y definiciones
- 3. Gobierno de la investigación, independencia y equipo multidisciplinar
- 4. Activación inmediata y preservación de evidencias
- 5. Paquete mínimo de información y trazabilidad de datos
- 6. Investigación técnica por dominios
- 7. Modelización, reproducción del incidente y pruebas contrafactuales
- 8. Auditoría organizativa, histórica, de planificación y regulatoria
- 9. Análisis causal y reglas para aceptar una conclusión
- 10. Recomendaciones, responsables, plazos y verificación
- 11. Sistema de loops, revisión adversarial y arbitraje técnico
- 12. Evaluación de la capacidad de la entidad auditora
- 13. Caso de interfaz 66/20 kV: ejemplo metodológico
- 14. Entregables y criterios de cierre
- Anexos operativos
- Referencias técnicas y normativas

1. Resumen ejecutivo

Un cero energético no se explica con una cronología. El listado de eventos puede mostrar qué relé actuó primero, qué interruptor abrió después y qué grupo se desconectó a continuación. Esa reconstrucción es imprescindible, pero solo responde a una pregunta: qué ocurrió. La investigación profesional empieza cuando se determina si cada actuación era la prevista, si las protecciones estaban correctamente coordinadas, si los grupos respondieron conforme a sus requisitos, si el sistema se explotaba dentro de márgenes adecuados y por qué las barreras de defensa no contuvieron la perturbación.

El método que se propone parte de una idea central: en un sistema aislado, la causa iniciadora y la causa del colapso pueden ser diferentes. Una falta, un disparo o la pérdida de un grupo pueden iniciar el incidente; el cero aparece cuando fallan o resultan insuficientes las barreras que debían limitar su propagación. Por eso la investigación debe examinar el sistema completo y no limitarse al elemento que primero aparece en el cronológico.

La experiencia internacional refuerza esta aproximación. La investigación de ENTSO-E sobre el apagón ibérico del 28 de abril de 2025 separó una primera fase factual de una segunda fase de causas raíz y recomendaciones, y reunió un panel técnico muy amplio. El precedente estadounidense-canadiense de 2003 distribuyó la investigación en grupos especializados de datos, modelización, operación, comunicaciones, transporte, generación, normativa, planificación y análisis causal. [R1][R2] Estas referencias no se trasladan mecánicamente a Canarias; sirven como evidencia de que un apagón de gran alcance exige trabajo multidisciplinar y acceso amplio a información primaria.

En Canarias, el marco nacional específico es determinante. El P.O. SENP 1 establece criterios de seguridad y funcionamiento para los sistemas eléctricos no peninsulares; el Real Decreto 738/2015 regula la producción y el despacho en estos sistemas; el P.O. 11.1 aprobado en 2026 unifica los criterios generales de protección para el sistema peninsular y no peninsular; y los planes de deslastre automático de cargas de 2024 recogen esquemas específicos por isla, incluida La Palma. [R3][R4][R5][R6]

PRINCIPIO RECTOR

La investigación no termina cuando se descubre qué elemento inició el incidente. Termina cuando puede explicarse, con evidencias reproducibles, por qué el sistema no evitó la propagación, qué barreras fallaron o fueron insuficientes y qué cambios concretos reducen de forma verificable el riesgo de repetición.

1.1. Las cuatro preguntas obligatorias

1. ¿Qué ocurrió? Reconstrucción factual, sincronizada y verificable del estado previo, la perturbación, la cascada y la reposición.
2. ¿Qué debía haber ocurrido? Contraste con normativa, procedimientos, ajustes aprobados, diseño, especificaciones del fabricante y buena práctica técnica aplicable.
3. ¿Por qué se produjo la desviación o por qué el sistema no contuvo el incidente? Identificación de causas técnicas, organizativas, humanas, de coordinación y estructurales.
4. ¿Qué debe cambiar y cómo se comprobará? Acciones correctoras con responsable, plazo, criterio de aceptación y verificación posterior.

1.2. Resultado que debe producir una investigación completa

- Una cronología maestra con incertidumbre temporal explícita y trazabilidad hasta los registros de origen.
- Una matriz de conformidad que diferencie incumplimiento, cumplimiento de una regla inadecuada, ausencia de requisito y requisito contradictorio u obsoleto.
- Un análisis técnico por dominios: protecciones, generación, transporte, distribución, operación, automatismos, comunicaciones, defensa y reposición.
- Modelos eléctricos y dinámicos validados contra las medidas reales del incidente, con pruebas de sensibilidad y escenarios contrafactuales.
- Un mapa causal que distinga evento iniciador, causas directas, factores de propagación, fallos de barreras, condiciones latentes y causas estructurales.
- Un examen histórico de planificación, mantenimiento, inversiones, cambios de configuración, recursos humanos, coordinación entre agentes y aprendizaje de incidentes previos.
- Recomendaciones priorizadas y verificables. Una recomendación sin responsable, fecha y prueba de cierre se considera incompleta.
- Una declaración explícita de incertidumbres y de cuestiones no resolubles por falta de datos.

2. Alcance, principios y definiciones

2.1. Alcance material

El protocolo se aplica a incidentes con pérdida total o muy extensa de suministro en un sistema eléctrico aislado, y también puede utilizarse, con alcance reducido, para perturbaciones graves que hayan estado próximas a producir un cero. El análisis comprende desde el estado del sistema antes del incidente hasta la estabilización y la reposición del suministro, e incluye las decisiones históricas que hayan creado o mantenido vulnerabilidades relevantes.

El alcance no se limita a activos de transporte. Incluye generación convencional y renovable, almacenamiento, compensación, redes de transporte y distribución, centros de control, telecomunicaciones, automatismos, protecciones, sistemas auxiliares, planes de defensa, reposición, mantenimiento, planificación y coordinación entre agentes. Cuando una función esté repartida entre empresas, la unidad de análisis será la función completa, no el límite societario.

2.2. Principios de investigación

Principio	Aplicación práctica
Primacía de la evidencia	Las conclusiones se apoyan en datos primarios, configuraciones vigentes, ensayos, registros y modelos reproducibles. La opinión experta orienta la investigación, pero no sustituye a la evidencia.
Separación hechos-causas	La cronología factual se congela antes de cerrar hipótesis causales importantes. Se evita codificar o etiquetar causas demasiado pronto para reducir el sesgo de confirmación, en línea con la práctica de análisis de eventos de NERC. [R7]
Independencia con conocimiento	La independencia no consiste en excluir a quienes conocen los activos. Los especialistas de los agentes investigados deben aportar datos y conocimiento, pero no controlar la formulación final de hallazgos que afecten a su propia actuación.
Visión sistémica	Se investiga por qué el incidente se propagó, no solo qué lo inició. Deben analizarse barreras de prevención, contención, defensa, reposición y gobernanza.
Reproducibilidad	Una conclusión técnica relevante debe poder ser reproducida por otro equipo competente a partir de los mismos datos, hipótesis y modelos.
Contradicción técnica	Toda conclusión crítica debe someterse a una revisión que intente refutarla con hipótesis alternativas y evidencia adversa.
No confundir cumplimiento con adecuación	Un agente puede haber cumplido un procedimiento y, sin embargo, el procedimiento ser insuficiente. La auditoría debe evaluar ambas dimensiones.
Proporcionalidad y seguridad	La publicidad de resultados no debe revelar configuraciones de protección o detalles de ciberseguridad que aumenten el riesgo del sistema. Se prevé un informe público y anexos técnicos de acceso restringido.
Cultura justa	Los errores individuales se estudian dentro del contexto organizativo, de carga de trabajo, interfaces, herramientas, formación y procedimientos. La finalidad técnica es prevenir recurrencias, no buscar culpables antes de entender el sistema.

2.3. Definiciones de trabajo

Término	Definición operativa
Cero energético	Pérdida total o prácticamente total de alimentación del sistema eléctrico considerado, con necesidad de reposición progresiva. El protocolo utiliza el término en sentido operativo; la calificación jurídica o regulatoria se hará conforme a la norma aplicable.
Evento iniciador	Suceso que abre la secuencia observable del incidente. No se presume que sea la causa raíz.
Causa directa	Mecanismo técnico u operativo sin el cual no se habría producido una parte concreta de la evolución observada.

Término	Definición operativa
Factor contribuyente	Condición que aumenta la probabilidad, severidad o extensión del incidente sin ser por sí sola necesaria.
Condición latente	Debilidad preexistente de diseño, mantenimiento, organización, procedimiento, formación, coordinación o planificación que permanecía oculta hasta combinarse con otros factores.
Barrera	Medida técnica u organizativa destinada a prevenir el incidente, limitar su propagación, defender el sistema o restaurarlo.
Causa estructural	Decisión, regla, modelo de gestión, política de inversión, asignación de responsabilidades o deficiencia sistémica que explica la persistencia de una vulnerabilidad.
Conclusión confirmada	Conclusión apoyada por evidencia primaria suficiente, mecanismo causal demostrable, consistencia con los registros y cierre razonable de hipótesis alternativas.
Conclusión probable	Conclusión fuertemente respaldada, pero con una incertidumbre residual que impide considerarla demostrada de forma completa.
Hipótesis plausible	Explicación técnicamente consistente que no dispone de evidencia suficiente para elevarse a conclusión.
No determinado	Cuestión para la que los datos disponibles no permiten discriminar entre explicaciones relevantes.

2.4. Marco normativo y referencias metodológicas

La investigación deberá construir al inicio una matriz normativa específica para el incidente, porque los requisitos aplicables dependen de la fecha, la tensión, el tipo de instalación y el régimen transitorio de cada norma. En particular, la Resolución de 16 de abril de 2026 aprobó el P.O. 11.1 Criterios Generales de Protección del Sistema Eléctrico Español y prevé transición desde los criterios anteriores; por ello no debe suponerse que el mismo régimen de protección era exigible a todos los activos en una fecha determinada. [R5]

Los Reglamentos europeos SO GL 2017/1485 y Emergency and Restoration 2017/2196 excluyen de su ámbito a las redes insulares no sincronizadas con las grandes zonas síncronas europeas. En consecuencia, para Canarias se utilizarán sus metodologías y experiencias como referencias comparativas cuando resulten útiles, no como obligaciones automáticas. [R8][R9] Esta distinción debe figurar expresamente en cualquier informe para evitar trasladar requisitos jurídicos que no sean aplicables.

3. Gobierno de la investigación, independencia y equipo multidisciplinar

3.1. Estructura de gobierno

Una investigación integral necesita una estructura que permita aprovechar el conocimiento interno sin convertir al investigado en juez de su propia actuación. Se propone una dirección independiente, equipos técnicos por dominio, una secretaría de datos y un panel de arbitraje. Los agentes implicados participan mediante puntos de contacto técnicos, entrega de información, entrevistas y revisión factual, pero no disponen de veto sobre las conclusiones.

Rol	Responsabilidad
Autoridad promotora	Define mandato, garantiza acceso a información, protege la independencia y recibe los informes. No interviene en la selección de una hipótesis técnica.
Director/a independiente de la investigación	Responsable del método, alcance, conflictos de interés, integración de disciplinas y decisión de elevar hallazgos al panel de arbitraje.
Secretaría técnica y de evidencias	Custodia datos, controla versiones, sincronización temporal, inventario, hashes, metadatos, permisos y trazabilidad.
Equipos de dominio	Analizan cada especialidad y emiten notas técnicas reproducibles, con supuestos, datos, herramientas, resultados y limitaciones.
Equipo de modelización	Construye o valida modelos de flujo de cargas, cortocircuito, dinámica RMS y, cuando sea necesario, EMT; reproduce el evento y ejecuta contrafactuales.

Rol	Responsabilidad
Equipo de revisión adversarial	Recibe los hallazgos provisionales y trata de refutarlos mediante hipótesis alternativas, inconsistencias de datos o pruebas adicionales.
Panel de arbitraje técnico	Resuelve discrepancias metodológicas o causales significativas. Sus miembros no deben haber participado en la ingeniería, operación o mantenimiento del sistema investigado durante el periodo relevante.
Agentes investigados	Aportan datos, expertos y observaciones. Pueden formular discrepancias documentadas y aportar contraevidencia, que debe quedar registrada.

3.2. Competencias mínimas que deben estar cubiertas

No se fija un número rígido de personas. Se fija cobertura funcional. Una misma persona puede acreditar más de una competencia adyacente, pero ningún informe integral debería depender de uno o dos profesionales que pretendan abarcar por sí solos todos los dominios. La experiencia internacional de investigaciones de apagones muestra precisamente la necesidad de equipos amplios y especializados. [R1][R2]

Dominio	Capacidad exigible
Operación de sistemas aislados	Despacho, reservas, criterios de seguridad, control frecuencia-potencia, tensión/reactiva, contingencias y procedimientos SENP.
Protecciones y automatismos	Cálculo de faltas, selectividad, tiempos críticos, relés, teleprotección, fallo de interruptor, intertrips, automatismos y pruebas extremo a extremo.
Generación térmica	Máquinas síncronas, turbinas/motores, gobernadores, excitación, PSS, limitadores, protecciones de grupo, auxiliares, arranque y rechazo de carga.
Generación basada en convertidores y almacenamiento	Controles de planta, PLL, límites de corriente, respuesta a huecos/sobretensiones, soporte de frecuencia/tensión, grid-following/grid-forming y lógica de desconexión.
Transporte y subestaciones	Topología, líneas, barras, transformadores, reactancias, compensación, interruptores, servicios auxiliares y configuración de subestaciones.
Distribución	Redes MT/BT, automatismos, protecciones, generación embebida, reconfiguración, fronteras transporte-distribución y planes de deslastre.
Estudios de sistema	Flujo de cargas, cortocircuito, estabilidad transitoria y de tensión, frecuencia, oscilaciones, EMT cuando proceda y validación de modelos.
SCADA/EMS/DMS, telecomunicaciones y tiempo	SOE, alarmas, historizadores, PMU, DFR, IEC 61850, telecontrol, sincronización GNSS/PTP/IRIG-B y calidad de sellado temporal.
Reposición y black start	Fuentes de arranque, reenergización, islas, sincronización, carga fría, prioridades y coordinación de maniobras.
Mantenimiento y gestión de activos	Pruebas de relés, interruptores, transformadores, baterías, obsolescencia, planes preventivos, correctivos y gestión de cambios.
Factores humanos y organización	Diseño de procedimientos, carga de alarmas, interfaces, formación, turnos, coordinación, transferencia de información y toma de decisiones bajo presión.
Marco regulatorio y planificación	Ley del Sector Eléctrico, normativa SENP, calidad de suministro, responsabilidades, planificación de red, inversiones y seguimiento de recomendaciones previas.

3.3. Reglas de independencia

- Declaración previa de intereses profesionales, societarios y contractuales de todos los investigadores y árbitros.
- Identificación de trabajos realizados para los agentes investigados que puedan afectar a la objetividad del análisis. No se presume conflicto por cualquier relación comercial; se evalúa su relevancia real.
- Nadie debe validar como revisor independiente un diseño, ajuste, estudio o procedimiento que haya elaborado o aprobado personalmente.

- La presidencia de la investigación y del panel de arbitraje debe recaer en expertos no afectados por el incidente y sin responsabilidad operativa en los activos analizados.
- Las discrepancias técnicas relevantes se documentan. El informe puede incorporar una opinión minoritaria motivada si no se alcanza consenso.
- La entidad auditora debe demostrar libertad para solicitar información adicional y para declarar un hallazgo como "no determinado" cuando falten datos.

4. Activación inmediata y preservación de evidencias

La pérdida de información comienza en el mismo momento de la perturbación. Los buffers de relés se sobrescriben, los historizadores pueden compactar datos, los equipos se reinician y las configuraciones cambian durante la reposición. Por ello, el primer objetivo no es formular una causa: es impedir que desaparezca la evidencia que permitiría investigarla.

4.1. Acciones de las primeras horas

Acción	Criterio de preservación
Congelar configuraciones	Exportar y custodiar ajustes activos de relés, PLC/RTU, protecciones de grupo, controladores de planta, AVR, PSS, gobernadores, PPC, BESS, esquemas de deslastre y automatismos. Registrar hash, fecha, equipo y persona que realiza la extracción.
Preservar registros nativos	Descargar SOE, COMTRADE, DFR, PMU, SCADA/EMS/DMS, DCS de centrales, registros de interruptores, alarmas, comunicaciones y sistemas auxiliares en formato original.
Capturar estado del sistema	Topología exacta, indisponibilidades, generación P/Q, reservas, consignas, demanda, tensiones, flujos, recursos de compensación y modo de control de cada unidad inmediatamente antes del evento.
Bloquear borrados automáticos	Suspender políticas de retención o rotación que puedan eliminar logs relevantes, sin interferir con la seguridad de la operación.
Preservar comunicaciones operativas	Conservar libros de operación, partes de turno, órdenes de despacho, mensajería operacional y, cuando exista base legal, grabaciones de voz de centros de control.
Identificar cambios posteriores	Toda modificación realizada para la reposición o para evitar repetición debe quedar registrada por separado. Nunca debe presentarse una configuración posterior como si fuera la existente durante el incidente.
Asegurar equipos dañados	Cuando exista un componente fallado, preservar evidencia física, fotografías, posiciones, sellos y condiciones antes de desmontar, salvo actuación necesaria por seguridad.

4.2. Cadena de custodia digital

Cada fichero debe tener identificador único, fuente, equipo, versión, hora de extracción, zona horaria, persona responsable, hash criptográfico y registro de transformaciones. Los análisis se realizan sobre copias de trabajo; el original se conserva inmutable. Si un dato ha sido convertido, filtrado o remuestreado, debe mantenerse el original y documentarse el proceso.

REGLA DE ORO DE LOS DATOS

Nunca corregir manualmente un sello de tiempo, un evento o una curva en el fichero original. La normalización temporal se realiza en una capa de análisis separada y deja constancia de la corrección aplicada y de su incertidumbre.

5. Paquete mínimo de información y trazabilidad de datos

La posibilidad de alcanzar conclusiones sólidas depende tanto del equipo investigador como del acceso real a la información. Una ingeniería excelente con datos parciales puede formular hipótesis de calidad, pero no debería presentar como definitiva una explicación que no pueda contrastar con configuraciones, registros y modelos de todos los agentes relevantes.

5.1. Información del operador del sistema y transporte

- Cronológicos SOE completos, alarmas, estados, órdenes y medidas analógicas a su resolución nativa.
- Datos PMU/DFR y oscilografías disponibles en subestaciones y nudos relevantes.
- Topología del sistema y estado de cada elemento antes, durante y después del incidente.
- Despacho programado y real, reservas disponibles, restricciones, indisponibilidades y consignas de potencia activa/reactiva.
- Resultados de estimación de estado, análisis de contingencias, límites operativos y alarmas del EMS.
- Procedimientos operativos vigentes, instrucciones de emergencia y reposición, planes de seguridad y criterios de reserva.
- Modelos de red utilizados en explotación y estudios: impedancias, transformadores, compensación, modelos dinámicos y parámetros de control.
- Ajustes de protecciones y automatismos bajo responsabilidad de transporte, incluido historial de cambios y pruebas.
- Registros de comunicaciones e interacciones con distribución, centrales y otros centros de control.
- Estudios previos que hubieran identificado vulnerabilidades relacionadas con el incidente.

5.2. Información de distribución

- SOE del DMS/SCADA, telemandos, estados de interruptores, reconectadores y automatismos.
- Esquemas unifilares y topología real de redes MT relevantes, incluida generación distribuida conectada a los alimentadores afectados.
- Ajustes de protecciones en posiciones frontera, transformadores y alimentadores; relés de deslastre por frecuencia y derivada.
- Carga asignada a cada escalón de deslastre y carga realmente desconectada en el incidente.
- Historial de cambios, pruebas, mantenimientos e incidencias de equipos de protección y telecontrol.
- Protocolos de coordinación con el operador del sistema y con titulares de generación conectada a distribución.
- Datos de calidad de suministro, interrupciones previas y anomalías recurrentes en la zona afectada.

5.3. Información de generación y almacenamiento

- DCS/SCADA de central o planta, SOE, trip logs, secuencia de primeros eventos y registros de alta resolución.
- Potencia activa/reactiva, tensión, frecuencia y velocidad; posición de válvulas/combustible; estado de excitación y limitadores; reservas y modos de control.
- Ajustes de gobernador, AVR, PSS, limitadores OEL/UEL, controles de planta y protecciones de máquina, transformador y servicios auxiliares.
- Curvas de capacidad, restricciones operativas, tiempos de arranque, mínimos técnicos y rampas vigentes.
- Informes de pruebas de respuesta, cumplimiento del P.O. SENP 12.2 cuando resulte aplicable, y modelos dinámicos entregados al operador del sistema. [R10]
- Historial de mantenimiento, averías, modificaciones de firmware/software, sustituciones de relés y cambios de parametrización.
- Para BESS o generación basada en convertidores: firmware, control de corriente, PLL, lógica de ride-through, modo grid-following/grid-forming, límites y registros del controlador de planta.

5.4. Documentación transversal

- Planos y esquemas "as built", matrices de disparo, lógicas, listas de señales y archivos de configuración IEC 61850 cuando existan.
- Actas de coordinación, estudios de protecciones, criterios de selectividad, tiempos críticos, comunicaciones de cambios y aprobaciones.
- Programas de mantenimiento, resultados de pruebas funcionales y extremo a extremo, fallos repetitivos y órdenes de trabajo abiertas.
- Informes de incidentes anteriores, recomendaciones, estado de cierre y justificaciones de medidas no ejecutadas.
- Planificación de inversiones, estudios de necesidad, restricciones presupuestarias o administrativas y decisiones de aplazamiento relevantes.
- Manuales del fabricante y boletines técnicos aplicables a los equipos implicados.

5.5. Calidad y sincronización temporal

Antes de construir el cronológico se debe auditar la calidad temporal de cada fuente. Un SOE de un relé, el SCADA de un centro de control, el DCS de una central y un PMU pueden tener referencias de tiempo diferentes. La sincronización de relojes es un requisito técnico crítico; IEEE 1588 define mecanismos de sincronización precisa en

sistemas de medida y control, y la familia IEC 61850 estructura la comunicación en automatización eléctrica. [R11][R12]

- Determinar la fuente de tiempo de cada dispositivo y si estaba sincronizada durante el incidente.
- Cuantificar desfases conocidos o estimados y representarlos como incertidumbre, no como una falsa precisión.
- Priorizar oscilografías y registros con reloj verificado para ordenar eventos separados por milisegundos.
- No inferir causalidad por un orden temporal cuando las incertidumbres de sellado son mayores que la separación entre eventos.

6. Investigación técnica por dominios

6.1. Reconstrucción del estado previo y cronología maestra

La cronología debe comenzar antes del primer disparo. Se reconstruye el estado estacionario previo, las indisponibilidades, las reservas, la configuración de red, la distribución de potencia reactiva, las tensiones, la inercia efectiva cuando sea relevante y cualquier condición anómala existente. El objetivo es saber si el sistema ya estaba operando con márgenes reducidos antes del evento iniciador.

- Estado de generación: unidades acopladas, potencia, reserva ascendente/descendente, modo de control, limitadores activos y unidades indisponibles.
- Estado de red: barras, acoplamientos, líneas, transformadores, reactancias/condensadores, trabajos y configuraciones excepcionales.
- Demanda total y distribución por zonas, incluyendo grandes consumidores y generación embebida.
- Tensiones, frecuencia, flujos y potencia reactiva en nudos clave.
- Alarmas previas, equipos fuera de servicio, protecciones bloqueadas, canales de teleprotección degradados y anomalías conocidas.
- Secuencia del incidente con una única escala temporal y referencia a cada evidencia primaria.

6.2. Protecciones, interruptores y automatismos

Este bloque debe responder a tres preguntas distintas: si la protección detectó correctamente la perturbación, si ordenó el disparo correcto con el tiempo previsto y si la coordinación del conjunto limitó la zona desconectada. El análisis no puede detenerse en comprobar que el relé "actuó según ajuste"; también debe comprobar si el ajuste, la lógica y la coordinación eran adecuados para la red real.

Área	Verificación
Configuración	Relés instalados, firmware, lógica activa, grupos de ajustes, funciones habilitadas/bloqueadas, entradas/salidas y matriz de disparo.
Medida	Transformadores de intensidad y tensión, relaciones, polaridad, saturación, circuitos secundarios, fusibles y calidad de señal.
Selectividad	Coordinación principal-respaldo, escalonamiento temporal, alcance de zonas, sobreintensidades direccionales, diferencial, distancia y funciones de tierra según el elemento.
Rapidez	Comparación entre tiempo de despeje real, tiempo de relé, tiempo de interruptor y tiempo crítico del sistema cuando resulte aplicable.
Redundancia	Doble sistema cuando sea exigible, independencia de alimentación y medida, comunicaciones y eliminación de fallos simples.
Fallo de interruptor	Lógica 50BF o equivalente, retrip, apertura de barras/adyacentes, temporización y actuación real.
Teleprotección e intertrip	Disponibilidad de canales, retardos, calidad, pérdida de canal, disparo transferido y pruebas extremo a extremo.
Reenganche/sincronismo	Lógicas de reenganche, comprobación de sincronismo, bloqueos, discordancia de polos y riesgo de extensión de perturbación.
Frecuencia y tensión	27/59, 81, RoCoF cuando exista, esquemas de defensa y compatibilidad con requisitos de permanencia conectada.
Historial	Última revisión de ajustes, cambios de topología, sustituciones de equipos, pruebas periódicas y desviaciones abiertas.

Los Criterios Generales de Protección del Sistema Eléctrico Español aprobados en 2026 son una referencia central: establecen criterios de selectividad, rapidez, redundancia y equipamiento, e incluyen para los territorios no peninsulares elementos de 66 kV en el ámbito de la red de transporte cuando corresponda. [R5] La investigación debe comprobar la norma y el régimen transitorio aplicables al activo concreto en la fecha del incidente.

6.3. Generación síncrona y centrales térmicas

En un sistema aislado, el comportamiento de cada grupo puede ser determinante por el tamaño relativo de la unidad respecto a la demanda. La investigación debe reconstruir no solo si el grupo disparó, sino qué magnitudes vio, qué controles llegaron a límite, qué protección decidió la desconexión y si el comportamiento real coincide con el modelo utilizado por el operador del sistema.

- Respuesta del gobernador y potencia mecánica ante la variación de frecuencia.
- Respuesta del AVR, PSS y limitadores de excitación; suministro o absorción de reactiva durante la perturbación.
- Protecciones de generador y transformador: diferencial, pérdida de excitación, potencia inversa, sobre/subfrecuencia, sobre/subtensión, sobreexcitación, desequilibrio, tierra y pérdida de sincronismo, según equipamiento real.
- Comportamiento del sistema de combustible, turbina o motor, caldera cuando proceda, y disparos de proceso que puedan preceder al disparo eléctrico.
- Servicios auxiliares, alimentación de control, baterías, UPS y secuencia de pérdida de auxiliares.
- Capacidad de rechazo de carga, operación en isla de servicios auxiliares y disponibilidad de arranque autónomo si está prevista.
- Concordancia entre modelo dinámico entregado al operador y respuesta medida del grupo.

6.4. Generación basada en convertidores y almacenamiento

La investigación debe tratar de forma específica los recursos electrónicos de potencia. El análisis de un disparo por tensión o frecuencia exige conocer la lógica interna y el controlador de planta, porque una planta puede cumplir un ajuste local y, al mismo tiempo, interactuar de forma no prevista con la estabilidad global.

- Ride-through de tensión y frecuencia; disparos por sobretensión/subtensión, frecuencia y RoCoF.
- Prioridad de corriente activa/reactiva y saturación del convertidor durante la perturbación.
- PLL, filtros, controles de tensión/reactiva, control de potencia y posibles oscilaciones de control.
- Modo grid-following o grid-forming, parámetros relevantes y cambios de modo.
- Respuesta del controlador de planta a consignas del centro de control y límites internos de los inversores.
- Eventos de firmware, watchdog, comunicaciones y desconexiones coordinadas de múltiples unidades.
- Validación del modelo agregado de planta frente a medidas reales.

6.5. Red de transporte

- Cálculo de la falta y ubicación probable; niveles de cortocircuito y contribución de generación.
- Estado y capacidad de líneas, barras, transformadores y compensación antes del incidente.
- Flujos y márgenes térmicos, de tensión y estabilidad; contingencias relevantes.
- Funcionamiento de interruptores, seccionadores, transformadores, cambiadores de tomas y servicios auxiliares.
- Efecto de la topología en la propagación del incidente: barras separadas, redes radiales, elementos fuera de servicio y zonas débiles.
- Consistencia entre el modelo de red operativo y la configuración real en campo.

6.6. Red de distribución y fronteras transporte-distribución

La interfaz entre transporte y distribución merece un análisis específico. En Canarias pueden existir instalaciones en las que la función protectora completa atraviese responsabilidades empresariales distintas. La auditoría debe reconstruir la cadena funcional extremo a extremo: medida, detección, orden de disparo, telecomunicación, interruptor, respaldo y reposición.

- Coordinación de protecciones en transformadores frontera y alimentadores asociados.
- Lógicas de apertura de ambos lados, enclavamientos, fallo de interruptor y disparos transferidos.
- Coordinación de ajustes entre empresas y evidencia formal de aprobación de cambios.
- Pruebas extremo a extremo realizadas después de modificaciones de relés, interruptores, RTU o telecomunicaciones.
- Efecto de generación embebida sobre direccionalidad, niveles de cortocircuito y selectividad.
- Comportamiento real de los alimentadores incluidos en esquemas de deslastre automático.

6.7. Operación del sistema y centros de control

La operación debe analizarse con el sistema y la información que realmente tenía disponible el personal, no con la ventaja retrospectiva del investigador. Se reconstruyen las alarmas visibles, los estudios disponibles, las instrucciones, las comunicaciones y el tiempo real de decisión.

- Criterios de reserva y unidades acopladas; tamaño de la mayor contingencia respecto a la reserva disponible.
- Restricciones técnicas, trabajos y condiciones excepcionales conocidas.
- Alarmas activas y posibles avalanchas de alarmas; señales inhibidas, mala calidad o discrepancias de estado.
- Resultado del estimador de estado y del análisis de contingencias antes del incidente.
- Órdenes a generación y distribución, confirmaciones y retrasos de comunicación.
- Aplicación de procedimientos normales, de alerta, emergencia y reposición.
- Dotación del turno, experiencia, formación, simulacros y transferencia de información entre turnos.
- Cambios manuales de consignas o topología que influyeran en la evolución.

El P.O. SENP 1 tiene por objeto establecer criterios de seguridad y funcionamiento para garantizar continuidad, seguridad y calidad en los sistemas no peninsulares. [R3] El análisis operativo debe contrastar la práctica real con estos criterios y con los procedimientos específicos vigentes, no con expectativas genéricas de sistemas peninsulares.

6.8. Planes de deslastre y otras defensas automáticas

Los planes de deslastre no se auditan solo comprobando si un relé alcanzó un umbral. Debe verificarse si la carga asignada existía realmente, si la apertura fue completa, si se desconectó generación embebida junto con la demanda y si el volumen y temporización efectivos fueron adecuados para la perturbación observada.

La Resolución de 16 de enero de 2024 aprobó planes específicos para Canarias e indica que se debe evitar, cuando sea posible, ubicar deslastres en posiciones con alta concentración de generación; si no puede evitarse la desconexión de generación, debe considerarse mayor deslastre para compensarla. Para La Palma se establecen escalones específicos de subfrecuencia y derivada de frecuencia. [R6]

- Inventario de relés instalados frente al plan aprobado y verificación de parametrización.
- Medición del tiempo real desde cruce de umbral hasta apertura efectiva.
- Cálculo de MW y MVAr realmente desconectados en cada escalón.
- Identificación de generación distribuida perdida simultáneamente.
- Evaluación de si el deslastre frenó la RoCoF y recuperó la frecuencia según el modelo.
- Revisión de mantenimiento, pruebas y actualizaciones de carga asignada conforme cambia la red.

6.9. Telecomunicaciones, SCADA, sincronización y cribado de ciberseguridad

Las comunicaciones y sistemas de control se investigan como parte del sistema físico. Una pérdida de teleprotección, una señal congelada o un reloj desincronizado puede alterar tanto la actuación como la interpretación posterior. La familia IEC 61850 y la norma IEC 60255 ofrecen referencias técnicas para automatización y equipos de protección; IEEE 1588 aporta referencia de sincronización precisa. [R11][R12][R13]

- Disponibilidad y latencia de canales de teleprotección y telecontrol.
- Calidad de datos, estados inválidos, alarmas de comunicaciones y pérdidas de paquetes cuando sean relevantes.
- Fuentes de sincronización, degradación GNSS, PTP/IRIG-B y discrepancias entre equipos.
- Cambios de configuración remotos y accesos administrativos durante el periodo relevante.
- Cribado de ciberseguridad solo cuando existan indicadores objetivos. La ausencia de causa inmediata no justifica atribuir el incidente a un ciberataque por descarte.

6.10. Reposición del sistema

La reposición es parte de la investigación, no un apéndice. Un sistema puede haber sufrido un cero inevitable ante una combinación excepcional y, aun así, revelar graves problemas de restauración; o puede mostrar que los planes y recursos de reposición funcionaron correctamente. Ambas cosas deben documentarse.

- Disponibilidad real de fuentes de arranque autónomo y su tiempo de puesta en servicio.
- Secuencia de reenergización de barras, líneas y transformadores; control de sobretensiones y reactiva.
- Formación de islas, control de frecuencia y tensión, y criterios de sincronización.
- Carga fría y escalonado de demanda; prioridad de servicios esenciales.
- Coordinación entre centro de control del sistema, distribución y centrales.
- Fallos de comunicaciones o equipos que retrasaran la reposición.

- Comparación entre tiempos previstos en planes/simulacros y tiempos reales.

7. Modelización, reproducción del incidente y pruebas contrafactuales

El modelo no debe utilizarse para sustituir datos que faltan, sino para comprobar si una explicación reproduce el comportamiento medido. Un modelo que no reproduce tensiones, frecuencia, flujos y secuencia de desconexiones del caso real no puede utilizarse con seguridad para declarar causas ni para justificar una medida correctora.

7.1. Escalera de modelos

Modelo	Pregunta que debe responder
Flujo de cargas	Reconstruir el punto de operación previo, tensiones, reactiva, flujos y márgenes.
Cortocircuito	Verificar corrientes de falta, contribuciones, sensibilidades de relés y niveles de red.
Coordinación de protecciones	Comprobar selectividad, tiempos, respaldos y consecuencias de fallos de interruptor.
Dinámica RMS	Reproducir frecuencia, tensión, respuesta de gobernadores/AVR, deslastres, desconexiones y estabilidad transitoria.
EMT, si procede	Investigar interacciones rápidas de convertidores, controles, resonancias o fenómenos que el modelo RMS no reproduzca.

7.2. Validación obligatoria

- Utilizar topología y despacho reales, no un caso genérico de planificación.
- Contrastar el modelo con PMU, oscilografías, medidas SCADA y registros de centrales.
- Ajustar únicamente parámetros justificables y registrar cada modificación.
- Comparar no solo el valor final, sino la trayectoria temporal de frecuencia, tensión y potencia.
- Si un modelo dinámico de una unidad no reproduce el evento, investigar si el modelo está desactualizado o si la unidad se comportó fuera de especificación.

7.3. Contrafactuales

Una vez validado el caso real se ejecutan escenarios contrafactuales. Su finalidad es distinguir causas de correlaciones y comprobar si una medida habría contenido el incidente. Los contrafactuales no deben presentarse como hechos; son experimentos de modelización.

- Mismo evento con el ajuste de protección teóricamente correcto.
- Mismo evento con el interruptor o canal de teleprotección funcionando según diseño.
- Mismo evento con distinta disponibilidad de reserva o recursos de soporte de tensión.
- Mismo evento con cada escalón de deslastre funcionando según el plan y con la carga real.
- Mismo evento evitando una desconexión de generación concreta para medir su contribución a la cascada.
- Mismo evento con la topología normal frente a la topología excepcional existente.

CRITERIO DE CAUSALIDAD

Si corregir una supuesta deficiencia en un modelo validado no cambia de forma material la evolución del incidente, esa deficiencia puede ser real pero no debe etiquetarse sin más como causa del cero. Puede seguir siendo un hallazgo de seguridad que requiera corrección.

8. Auditoría organizativa, histórica, de planificación y regulatoria

Una investigación completa debe ir más atrás que el día del incidente. El objetivo es determinar si existían vulnerabilidades conocidas, si fueron correctamente evaluadas, qué medidas se decidieron, cuáles se ejecutaron y quién tenía capacidad para actuar. Esta parte es la que permite diferenciar una avería imprevisible de un fallo sistémico acumulado.

8.1. Horizonte histórico

Como criterio de trabajo se recomienda revisar, al menos, los cinco años anteriores y ampliar el periodo hasta el último cero relevante, la última reconfiguración estructural importante o la fecha de implantación del esquema técnico implicado. El horizonte se adapta a cada caso; no debe usarse un corte temporal para excluir decisiones que sigan produciendo efectos.

8.2. Planificación y suficiencia del sistema

- Evolución de la demanda y de la potencia firme realmente disponible, no solo potencia nominal instalada.
- Tamaño relativo de los grupos y contingencias dominantes en cada condición de demanda.
- Criterios de reserva, mínimos técnicos, rampas y riesgo de indisponibilidades simultáneas.
- Necesidades de potencia reactiva, soporte de tensión, inercia/fast frequency response y nivel de cortocircuito cuando sean relevantes.
- Limitaciones de red conocidas, configuraciones radiales, puntos únicos de fallo y indisponibilidades recurrentes.
- Necesidad y disponibilidad de almacenamiento, compensación, refuerzos de red, nueva generación o medidas equivalentes desde el punto de vista de seguridad.
- Decisiones de planificación adoptadas, retrasos y medidas temporales utilizadas para cubrir el riesgo.

8.3. Mantenimiento y gestión del cambio

- Cumplimiento de periodicidades de pruebas y mantenimiento en protecciones, interruptores, transformadores, baterías, UPS y comunicaciones.
- Órdenes de trabajo abiertas, defectos repetitivos y desviaciones aceptadas.
- Gestión de obsolescencia y disponibilidad de repuestos críticos.
- Procedimiento formal para cambios de ajustes, firmware, lógica, topología y comunicaciones.
- Reestudio de coordinación después de modificaciones relevantes en generación o red.
- Control de documentación "as built" y coherencia entre planos, base de datos del centro de control y campo.

8.4. Organización, recursos y interfaces

- Definición de responsabilidades entre operador del sistema, transportista, distribuidor y productores.
- Protocolos de coordinación en posiciones frontera y cambios que afecten a más de un agente.
- Capacidad y experiencia del personal de operación y mantenimiento; formación y simulacros.
- Carga de trabajo, cobertura de turnos, disponibilidad de especialistas y tiempos de respuesta.
- Mecanismos para escalar riesgos técnicos desde los equipos de campo y centros de control hasta la dirección y la Administración.
- Tratamiento de recomendaciones de incidentes previos y existencia de hallazgos repetidos.

8.5. Cumplimiento normativo frente a adecuación técnica

Cada hallazgo debe situarse en una de cuatro categorías. Esta clasificación evita una conclusión demasiado cómoda: "se cumplió el procedimiento". Cumplir una regla no demuestra que la regla protegiera suficientemente al sistema.

Categoría	Significado
A. Incumplimiento	Existía un requisito aplicable y no se cumplió.
B. Cumplimiento insuficiente	El agente cumplió el requisito, pero el requisito o criterio resultó técnicamente insuficiente para el riesgo real.
C. Vacío normativo o procedimental	No existía una regla adecuada para una situación relevante.
D. Requisito contradictorio/obsoleto	Dos requisitos eran incompatibles o el requisito no reflejaba la configuración/tecnología actual.

8.6. Responsabilidades y marco legal

La Ley 24/2013 atribuye al operador del sistema la función principal de garantizar la continuidad y seguridad del suministro y la correcta coordinación del sistema de producción y transporte. La misma ley diferencia funciones de productores, transportistas y distribuidores. [R14] El Real Decreto 1955/2000 regula, entre otros aspectos, la calidad del servicio en transporte y distribución y prevé registros de incidencias y responsabilidades en calidad. [R15]

El análisis técnico debe identificar responsabilidades funcionales: quién debía diseñar, aprobar, mantener, operar, supervisar o corregir una barrera. La atribución de responsabilidad jurídica, sancionadora o civil requiere un análisis legal específico y no debe deducirse automáticamente de una causa técnica. IEC 62740 también distingue el análisis de causas de la asignación de responsabilidad o liability. [R16]

9. Análisis causal y reglas para aceptar una conclusión

Los sistemas eléctricos complejos rara vez colapsan por una sola causa raíz. El protocolo evita forzar una explicación monocausal. Se construye una cadena de causalidad con distintos niveles y se identifica qué barreras debían haber interrumpido la propagación.

9.1. Taxonomía causal

Nivel	Descripción
Evento iniciador	Primer suceso relevante de la cadena observable.
Causa técnica directa	Fallo o comportamiento que produce inmediatamente una desconexión, desequilibrio o inestabilidad.
Factor de propagación	Condición que amplía la perturbación: ajustes, reservas, topología, respuesta de controles, desconexiones adicionales, etc.
Fallo de barrera de defensa	Deslastre, automatismo, protección de respaldo u otra defensa que no actuó, actuó tarde o fue insuficiente.
Condición latente	Debilidad preexistente de mantenimiento, configuración, documentación, coordinación, formación o gestión del cambio.
Causa estructural	Problema de planificación, gobernanza, incentivos, reparto de responsabilidades, regulación o inversión que permitió persistir a la vulnerabilidad.
Factor de reposición	Elemento que aceleró o retrasó la recuperación después del cero.

9.2. Técnicas de análisis

Se utilizarán varias técnicas porque cada una responde a preguntas diferentes. IEC 62740 describe principios y técnicas de análisis de causa raíz para incidentes y reconoce causas de diseño, organización, factores humanos y sucesos externos. [R16]

- Gráfico de eventos y factores causales: une cronología y mecanismos sin confundir simultaneidad con causalidad.
- Análisis de barreras: identifica qué debía impedir, contener o mitigar cada fase y por qué no lo hizo.
- Árbol de fallos: útil para comprobar combinaciones lógicas necesarias para un evento superior.
- Análisis de cambios: compara la condición del incidente con una condición anterior estable.
- Cinco porqués: herramienta auxiliar, nunca suficiente por sí sola para un sistema multidisciplinar.
- Contrafactuales de modelo: prueban sensibilidad y necesidad causal de determinados factores.
- Revisión de factores humanos y organizativos: explica por qué decisiones o errores fueron posibles dentro del sistema de trabajo.

9.3. Test de aceptación de una conclusión causal

Prueba	Criterio
1. Temporalidad	La causa propuesta precede al efecto considerando la incertidumbre de sellado temporal.
2. Mecanismo	Existe un mecanismo eléctrico, mecánico, de control u organizativo capaz de producir el efecto.
3. Evidencia	La afirmación se apoya en datos primarios y/o documentación controlada; no solo en testimonios.
4. Coherencia	La hipótesis explica todas las observaciones relevantes sin contradicciones significativas.
5. Alternativas	Se han buscado y probado explicaciones alternativas razonables.
6. Reproducción	Cuando sea aplicable, el modelo o prueba reproduce el comportamiento medido.

Prueba	Criterio
7. Contrafactual	Corregir o retirar el factor modifica materialmente la evolución prevista del incidente, si la técnica permite evaluarlo.
8. Revisión cruzada	La conclusión ha sido revisada por al menos otra disciplina pertinente y por el equipo adversarial si es crítica.

9.4. Escala de confianza

Nivel	Uso
Confirmado	Evidencia primaria suficiente, mecanismo demostrado, alta reproducibilidad y alternativas relevantes razonablemente descartadas.
Muy probable	Evidencia fuerte y mecanismo consistente, con incertidumbre residual limitada que no cambia la conclusión principal.
Plausible	Explicación técnicamente coherente, pero faltan datos o pruebas para discriminarla de alternativas.
No determinado	La información disponible no permite una conclusión responsable.

REGLA DE REDACCIÓN

El informe no utilizará expresiones como "causa definitiva" cuando la evidencia corresponda a un nivel plausible o no determinado. La incertidumbre forma parte del resultado técnico y debe hacerse visible.

10. Recomendaciones, responsables, plazos y verificación

El objetivo práctico de investigar es evitar la repetición. Las recomendaciones deben atacar las causas y las barreras fallidas, no limitarse a reparar el componente dañado. Una recomendación puede ser técnicamente correcta y aun así ser inútil si no tiene propietario, plazo, recursos y prueba de cierre.

10.1. Contenido obligatorio de cada acción

- Hallazgo y mecanismo causal que pretende corregir.
- Medida técnica u organizativa concreta, evitando formulaciones genéricas como "mejorar la coordinación".
- Responsable primario y agentes que deben colaborar.
- Prioridad y plazo objetivo.
- Criterio de aceptación medible: ensayo, simulación, inspección, auditoría, KPI o demostración documental.
- Riesgo residual después de la medida.
- Dependencias con otras acciones y necesidad de actualización de modelos/procedimientos.

10.2. Priorización propuesta

Prioridad	Criterio
P0 - Inmediata	Riesgo de repetición inminente o defecto que compromete una barrera esencial. Medidas provisionales antes de volver a una configuración equivalente.
P1 - Corto plazo	Corrección necesaria para recuperar márgenes adecuados de seguridad y coordinación.
P2 - Medio plazo	Cambios de ingeniería, mantenimiento, formación o procedimientos que requieren proyecto y pruebas.
P3 - Estructural	Planificación, regulación, inversiones o rediseños de largo alcance. Deben tener hitos intermedios para no quedar abiertos indefinidamente.

10.3. Verificación de eficacia

El cierre administrativo no equivale al cierre técnico. Una acción solo se considera cerrada cuando se ha demostrado que funciona. En protecciones, puede exigir prueba extremo a extremo; en modelos, reproducción y sensibilidad; en operación, simulacro; en planificación, puesta en servicio y verificación del margen conseguido.

11. Sistema de loops, revisión adversarial y arbitraje técnico

El protocolo incorpora ciclos de revisión cerrados. Cada loop tiene un criterio de salida y puede devolver el trabajo a una fase anterior. El objetivo es evitar que un error temprano de datos o cronología contamine todo el análisis causal.

Ciclo	Pregunta de control
Loop 1 - Suficiencia de evidencia	¿Se han identificado todas las fuentes críticas? ¿Existen huecos que impiden resolver hipótesis relevantes? Si faltan datos, se emite requerimiento adicional antes de avanzar.
Loop 2 - Cronología y sincronización	Cada disciplina revisa la cronología maestra. Se resuelven discrepancias de reloj y se congelan hechos antes de cerrar causalidad.
Loop 3 - Validación técnica por dominio	Cada hallazgo se contrasta con ajustes, pruebas, normativa, modelo y especialista de una disciplina adyacente.
Loop 4 - Red team causal	Un equipo que no haya elaborado el hallazgo intenta refutarlo. Debe presentar hipótesis alternativas y señalar evidencia que falte.
Loop 5 - Arbitraje	Las discrepancias significativas se someten a un panel independiente, que puede confirmar, degradar el nivel de confianza, pedir prueba adicional o declarar no determinado.
Loop 6 - Validación de recomendaciones	Se comprueba mediante modelo, prueba o análisis de ingeniería que la medida propuesta reduce el riesgo sin crear otro problema relevante.
Loop 7 - Revisión final de trazabilidad	Toda afirmación crítica debe poder seguirse desde el texto final hasta evidencia, cálculo o referencia. Se eliminan conclusiones que no superen este test.

11.1. Panel de arbitraje

El panel de arbitraje no reescribe el informe. Decide sobre cuestiones técnicas controvertidas y sobre el nivel de confianza que puede asignarse. Se recomienda una composición impar, multidisciplinar y ajena a las áreas directamente investigadas. Para cada controversia se entrega un expediente breve con la afirmación, evidencias a favor y en contra, hipótesis alternativas, cálculos y posiciones de las partes.

- El árbitro puede pedir una prueba o simulación adicional.
- La ausencia de consenso no se oculta: se registra la posición minoritaria y su fundamento.
- El panel no debe sustituir la falta de evidencia por autoridad personal.
- Las decisiones sobre responsabilidad jurídica quedan fuera del arbitraje técnico salvo que el mandato incluya expertos jurídicos y procedimiento específico.

11.2. Criterios de calidad del informe final

Criterio	Condición de aceptación
Trazabilidad	100 % de hallazgos críticos enlazados a evidencias identificables.
Reproducibilidad	Cálculos y modelos documentados con versión, datos de entrada y supuestos.
Separación factual	Hechos, inferencias e hipótesis claramente diferenciados.
Cobertura multidisciplinar	Ningún dominio relevante queda sin revisión competente.
Contradicción	Hipótesis alternativas relevantes consideradas y documentadas.
Incertidumbre	Limitaciones y datos faltantes explícitos.
Accionabilidad	Cada recomendación tiene responsable, plazo y prueba de cierre.
Seguridad de información	Versión pública sin exposición innecesaria de datos sensibles.

12. Evaluación de la capacidad de la entidad auditora

Antes de adjudicar una investigación integral se debe auditar al propio auditor. Una empresa puede ser excelente en subestaciones y protecciones y no disponer de experiencia equivalente en operación de sistemas aislados, grupos térmicos, distribución o dinámica. La independencia tampoco compensa una carencia técnica, del mismo modo que el conocimiento interno no compensa una falta de independencia.

12.1. Puertas de entrada obligatorias

Requisito	Prueba exigible
Independencia y conflictos	Declaración completa y medidas de mitigación. Si un conflicto afecta al núcleo del incidente y no puede aislarse, la entidad no debe liderar ese bloque.
Cobertura multidisciplinar	Debe demostrar especialistas identificados para todos los dominios necesarios. No basta con una lista corporativa de capacidades generales.
Acceso a datos	El contrato debe garantizar requerimiento de información a todos los agentes. Sin acceso, el alcance debe declararse expresamente limitado.
Herramientas y modelos	Capacidad para analizar COMTRADE/SOE, estudios de protección, flujo de cargas, cortocircuito y dinámica; EMT si la hipótesis lo requiere.
Experiencia relevante	Experiencia demostrable en incidentes, puesta en servicio, protección, operación o estudios de sistemas de características comparables.
Gobierno de evidencias	Procedimiento de cadena de custodia, control de versiones y confidencialidad.
Revisión independiente	Equipo de revisión y arbitraje separado del autor de cada bloque crítico.

12.2. Matriz de competencia documental

Para cada especialista propuesto deben aportarse proyectos concretos, función desempeñada, años de experiencia, herramientas dominadas y posibles conflictos. La evaluación no se realiza sobre el nombre de la empresa, sino sobre el equipo nominal que ejecutará el contrato.

Competencia	Evidencia mínima a solicitar
Operación SENP / sistemas aislados	CV y casos reales; conocimiento de despacho, reserva, tensión/frecuencia y procedimientos.
Protecciones	Estudios de coordinación, pruebas, ajustes y análisis de actuaciones reales.
Generación térmica	Experiencia en controles/protecciones de grupos y auxiliares; análisis de trips.
Distribución	Protecciones MT, automatismos, DMS y fronteras con transporte.
Modelización dinámica	Casos de validación contra medidas reales, no solo estudios de planificación.
Reposición	Diseño o prueba de black start y planes de restauración.
Datos y tiempo	SOE/COMTRADE/PMU, sincronización y reconstrucción forense.
Factores organizativos	Investigación de incidentes y gestión de cambios/procedimientos.

APLICACIÓN A UNA EMPRESA CONCRETA

Esta matriz permite evaluar posteriormente a cualquier ingeniería -incluida Iprocel- sin prejuzgar su capacidad. La pregunta correcta no es si la empresa "sabe de electricidad", sino si el equipo asignado cubre todas las disciplinas, dispone de acceso a datos y puede integrar conclusiones sin depender de los propios agentes investigados.

13. Caso de interfaz 66/20 kV: ejemplo metodológico

Se incluye este ejemplo porque representa bien el riesgo de analizar por compartimentos empresariales. No se afirma que todas las subestaciones canarias tengan la misma titularidad o esquema; antes de aplicar el ejemplo se debe verificar quién es propietario, operador y responsable de cada posición concreta.

Supóngase una falta interna en un transformador 66/20 kV situado en una frontera funcional entre transporte y distribución. El objetivo no es comprobar por separado que "la protección de 66 kV funcionó" y que "la de 20 kV funcionó". El objeto de auditoría es el sistema de despeje completo del transformador y sus consecuencias sobre el sistema.

Pregunta	Comprobación
Detección	¿Qué funciones detectan faltas internas: diferencial de transformador, REF, sobreintensidad, gas/Buchholz, otras? ¿Qué relé es principal y cuál respaldo?
Disparo	¿Qué interruptores deben abrir para cada tipo de falta? ¿Existe disparo directo a ambos lados? ¿Hay 86 de bloqueo?
Interfaz	¿La orden cruza fronteras empresariales? ¿Mediante qué canal, protocolo y acuerdo operativo?
Tiempos	¿Cuál es el tiempo total esperado desde la falta hasta la apertura de cada lado? ¿Es compatible con estabilidad y daños admisibles?
Fallo de interruptor	Si un interruptor no abre, ¿qué lógica de respaldo desconecta barras o elementos adyacentes? ¿Se ha probado extremo a extremo?
Ajustes	¿Quién calcula, revisa y aprueba ajustes? ¿Cómo se comunica un cambio en un lado al otro?
Medida	¿CT/VT, polaridades, saturación y circuitos secundarios están verificados para la función diferencial y respaldos?
Sincronización	¿Los relés de ambos lados comparten referencia de tiempo fiable? ¿Puede demostrarse el orden de milisegundos?
Pruebas	¿Cuándo se realizó la última prueba funcional completa, incluyendo disparos reales o simulados y comunicaciones?
Consecuencia sistémica	Si el despeje fue correcto, ¿por qué la pérdida del transformador o la secuencia posterior pudo propagarse? ¿Reserva, topología, generación, deslastre, automatismos?

LECTURA CORRECTA DEL CRONOLÓGICO

Que dos relés actúen en el orden previsto no demuestra por sí solo que el esquema fuese adecuado. La auditoría debe comprobar qué debía ocurrir, con qué tiempos, bajo qué contingencias y qué consecuencias tenía la actuación conjunta sobre el sistema insular.

14. Entregables y criterios de cierre

14.1. Entregables mínimos

Entregable	Contenido
D0 - Acta de preservación	Inventario inicial de evidencias, fuentes, datos faltantes y medidas para evitar pérdida de información.
D1 - Informe factual	Estado previo, cronología sincronizada, afectación, secuencia de reposición. Sin cerrar causas no demostradas.
D2 - Informes de dominio	Protecciones, generación, red, distribución, operación, defensa, comunicaciones, reposición y factores organizativos.
D3 - Informe de modelización	Modelos, validación, reproducción del caso real, sensibilidades y contrafactuales.

Entregable	Contenido
D4 - Informe causal integral	Causas, factores contribuyentes, fallos de barreras, condiciones latentes, causas estructurales y niveles de confianza.
D5 - Plan de acciones	Recomendaciones, responsables, prioridad, plazo y criterio de cierre.
D6 - Informe público	Conclusiones y recomendaciones compatibles con la transparencia y la protección de información sensible.
D7 - Registro de cierre	Seguimiento posterior de acciones y verificación de eficacia.

14.2. Cuándo puede declararse terminada la investigación

- La cronología crítica está cerrada con incertidumbres explícitas.
- Se ha alcanzado una conclusión o se ha declarado honestamente "no determinado" para cada hipótesis material.
- Los modelos utilizados en causalidad han sido validados frente a medidas.
- Los hallazgos críticos han superado revisión adversarial y, cuando hubo conflicto, arbitraje.
- Las recomendaciones tienen responsable, plazo y criterio de verificación.
- Se ha emitido un registro de datos no disponibles y de cómo esa ausencia limita las conclusiones.
- El informe diferencia con claridad responsabilidad técnica funcional y eventual responsabilidad jurídica.

14.3. Qué no debe aceptarse como investigación integral

- Un informe basado esencialmente en declaraciones de los propios agentes sin acceso a datos primarios.
- Una simple cronología de disparos sin análisis de ajustes, coordinación, cumplimiento y adecuación.
- Un estudio de protecciones que no examine generación, operación, red, defensa y reposición cuando sean relevantes.
- Una simulación con un caso de red genérico no validado contra el incidente.
- Conclusiones "definitivas" con datos críticos ausentes o relojes no sincronizados.
- Recomendaciones genéricas sin prueba de que habrían evitado o contenido el incidente.
- Una auditoría en la que el mismo equipo diseña, opera o mantiene el elemento y actúa como único revisor de su propia actuación.

ANEXO A. Lista maestra de solicitud de información

ID	Información requerida
A1	Cronológicos SOE de todos los centros de control implicados, resolución nativa, con diccionario de señales.
A2	Oscilografías COMTRADE/DFR y registros PMU de la ventana completa disponible.
A3	Exportaciones de ajustes activos e históricos de relés y automatismos.
A4	Esquemas unifilares y funcionales as built; matrices de disparo e interlocking.
A5	Topología de red y estados de interruptores antes/durante/después del evento.
A6	Despacho, generación P/Q, reserva, demanda, tensiones, flujos y compensación.
A7	Modelos de red y dinámicos usados por el operador; versiones y fecha de validación.
A8	DCS/trip logs de cada grupo/planta que intervino en la cascada.
A9	Ajustes y modelos de gobernador, AVR, PSS, limitadores y protecciones de generación.
A10	Datos de control de plantas renovables/BESS, firmware y eventos del PPC.
A11	Registros de telecomunicaciones/teleprotección y alarmas de canales.
A12	Fuente y estado de sincronización temporal de cada equipo.
A13	Plan de deslastre aplicable, relés instalados, carga asignada y prueba de actuación.
A14	Procedimientos de operación, emergencia, reposición y coordinación vigentes.
A15	Partes de turno, órdenes operativas, comunicaciones y grabaciones cuando legalmente proceda.
A16	Mantenimientos y pruebas de relés, interruptores, baterías, UPS y comunicaciones.
A17	Incidencias anteriores, recomendaciones y estado de cierre.
A18	Estudios de contingencias, estabilidad, cortocircuito, protecciones y tiempos críticos.
A19	Planificación e inversiones relacionadas con vulnerabilidades identificadas.
A20	Cambios de configuración, firmware, relés o lógicas en el periodo histórico revisado.

ANEXO B. Ficha de evidencia

Campo	Contenido a registrar
ID de evidencia	Código único
Fuente/propietario	Empresa, instalación, equipo y responsable
Tipo	SOE, COMTRADE, configuración, plano, test, entrevista, etc.
Periodo	Fecha/hora inicio-fin y zona horaria
Formato original	Extensión, versión y tamaño
Hash	Huella de integridad del fichero original
Sincronización	Fuente de tiempo y precisión/incertidumbre conocida
Extracción	Fecha, persona y método
Transformaciones	Conversión, filtrado, normalización o remuestreo realizados
Permisos	Público, restringido, confidencial, sensible de seguridad

Campo	Contenido a registrar
Hallazgos relacionados	IDs de hallazgos que utilizan esta evidencia

ANEXO C. Plantilla de hallazgo

Campo	Contenido
ID / título	Identificador y frase factual breve
Hecho observado	Qué ocurrió; sin interpretación innecesaria
Evidencia	IDs de registros, documentos, ensayos y entrevistas
Requisito aplicable	Norma, procedimiento, ajuste, diseño o buena práctica
Análisis	Mecanismo y comparación entre esperado y observado
Clasificación causal	Directa, contribuyente, barrera, latente, estructural, reposición
Nivel de confianza	Confirmado / Muy probable / Plausible / No determinado
Hipótesis alternativas	Alternativas consideradas y por qué se descartan o mantienen
Impacto	Efecto sobre seguridad, propagación o reposición
Recomendación	Acción específica y trazable al hallazgo
Responsable / plazo	Propietario y fecha objetivo
Verificación	Prueba o criterio de cierre

ANEXO D. Guía de entrevistas técnicas

- Entrevistar primero por hechos: qué observó, qué información tenía, qué acción realizó y con qué objetivo.
- Evitar preguntas que sugieran una causa antes de cerrar la cronología.
- Separar memoria personal de registros: una discrepancia no implica mala fe y debe resolverse con evidencia.
- Mostrar posteriormente al entrevistado la cronología relevante para que pueda corregir errores factuales.
- Preguntar por condiciones previas: alarmas habituales, equipos degradados, cambios recientes, instrucciones especiales y problemas conocidos.
- Preguntar qué barreras esperaba que actuaran y qué señales le hicieron confiar o desconfiar de ellas.
- Documentar presiones de tiempo, carga de alarmas, interfaces con otros centros y disponibilidad de especialistas.
- Permitir una declaración adicional escrita y registrar desacuerdos sin penalizar la aportación de información.

ANEXO E. Registro de recomendaciones

ID	Hallazgo	Acción	Prioridad	Responsable	Plazo	Prueba de cierre	Estado
R-001	[hallazgo]	[acción concreta]	P0/P1/P2/P3	[entidad]	[fecha]	[ensayo/simulación/auditoría]	Abierta
R-002	[hallazgo]	[acción concreta]	P0/P1/P2/P3	[entidad]	[fecha]	[criterio medible]	Abierta

ANEXO F. Lista de comprobación para contratar una auditoría de cero

Área	Pregunta de aceptación

Área	Pregunta de aceptación
Mandato	¿El contrato permite investigar causas técnicas, organizativas, históricas y estructurales, no solo reconstruir eventos?
Datos	¿La Administración puede requerir información completa a operador, transporte, distribución y generación?
Equipo	¿Se identifica nominalmente quién cubrirá cada especialidad?
Protecciones	¿Incluye coordinación extremo a extremo, ajustes, oscilografías, teleprotección y pruebas?
Generación	¿Incluye especialistas en grupos térmicos y controles/protecciones de generación?
Operación	¿Incluye experiencia real en operación de sistemas aislados y procedimientos SENP?
Distribución	¿Incluye análisis de redes MT y fronteras transporte-distribución?
Modelos	¿Incluye validación dinámica contra medidas y contrafactuales?
Independencia	¿Se declaran conflictos y se separa al revisor del autor?
Arbitraje	¿Existe mecanismo para resolver discrepancias técnicas sin que prevalezca la parte con mayor poder contractual?
Transparencia	¿Se prevé informe público y anexos confidenciales?
Seguimiento	¿El contrato llega hasta verificar el cierre de recomendaciones?

Referencias técnicas y normativas

[R1] ENTSO-E. "28 April 2025 Blackout" y Final Report del Expert Panel, publicado el 20 de marzo de 2026. Investigación en dos fases: informe factual y análisis de causas/recomendaciones; panel multidisciplinar dirigido por expertos de TSOs no afectados. Fuente oficial / técnica

[R2] U.S.-Canada Power System Outage Task Force / FERC. August 14th 2003 Blackout: Causes and Recommendations. Organización de equipos especializados en datos, modelización, operación, comunicaciones, transporte, generación, normativa, planificación e investigación causal. Fuente oficial / técnica

[R3] Resolución de 11 de diciembre de 2019. P.O. SENP 1 "Funcionamiento de los sistemas eléctricos no peninsulares" y otros procedimientos SENP. BOE-A-2019-18275. Fuente oficial / técnica

[R4] Real Decreto 738/2015, de 31 de julio, producción de energía eléctrica y despacho en los sistemas eléctricos de los territorios no peninsulares. BOE-A-2015-8646. Fuente oficial / técnica

[R5] Resolución de 16 de abril de 2026. P.O. 11.1 "Criterios Generales de Protección del Sistema Eléctrico Español". BOE-A-2026-8786. Fuente oficial / técnica

[R6] Resolución de 16 de enero de 2024. Planes de deslastre automático de cargas en los sistemas no peninsulares balear y canario. BOE-A-2024-1858. Fuente oficial / técnica

[R7] NERC. Cause Code Assignment Process Manual, 2025. Advierte contra asignar causas antes de completar investigación y análisis; distingue iniciador de causa raíz. Fuente oficial / técnica

[R8] Reglamento (UE) 2017/1485, System Operation Guideline. Su artículo 2 excluye redes insulares no sincronizadas con las grandes zonas síncronas europeas; se usa aquí solo como referencia metodológica cuando proceda. Fuente oficial / técnica

[R9] Reglamento (UE) 2017/2196, Network Code on Electricity Emergency and Restoration. También excluye determinadas redes insulares no sincronizadas; referencia comparativa para defensa y reposición. Fuente oficial / técnica

[R10] Resolución de 1 de febrero de 2018. P.O. SENP 12.2: requisitos mínimos de diseño, equipamiento, funcionamiento, puesta en servicio y seguridad de instalaciones y generación en SENP. BOE-A-2018-2198. Fuente oficial / técnica

[R11] IEEE 1588-2019. Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. Fuente oficial / técnica

[R12] IEC 61850 series. Communication networks and systems for power utility automation; IEC TR 61850-1-1:2026, overview. Fuente oficial / técnica

[R13] IEC 60255-1:2022. Measuring relays and protection equipment - Common requirements. Fuente oficial / técnica

[R14] Ley 24/2013, de 26 de diciembre, del Sector Eléctrico. Funciones de sujetos y del operador del sistema. BOE-A-2013-13645. Fuente oficial / técnica

[R15] Real Decreto 1955/2000, de 1 de diciembre. Transporte, distribución, calidad del servicio, registros de incidencias y responsabilidades. BOE-A-2000-24019. Fuente oficial / técnica

[R16] IEC 62740:2015. Root cause analysis (RCA). Principios y técnicas de análisis de causas; distingue RCA de asignación de responsabilidad jurídica. Fuente oficial / técnica

[R17] IEC 61000-4-30:2025. Power quality measurement methods. Referencia para medición e interpretación de frecuencia, tensión, huecos, interrupciones y otros parámetros de calidad. Fuente oficial / técnica

[R18] Red Eléctrica. Acuerdo de condiciones y ajustes de relés en redes radiales a tensión inferior a 66 kV en los SENP. Ejemplo relevante de coordinación OS-distribuidor-generación. Fuente oficial / técnica

Nota final sobre el uso del protocolo

Este protocolo está diseñado deliberadamente para impedir dos errores frecuentes: confundir el cronológico con la causa y confundir independencia con autosuficiencia técnica. Un cero energético de un sistema aislado exige combinar el conocimiento profundo de quienes operan y mantienen sus instalaciones con una dirección y revisión capaces de cuestionar sus decisiones. Solo esa combinación permite pasar de "esto fue lo que disparó" a una respuesta mucho más útil: "esto es lo que permitió que la perturbación se convirtiera en un cero y esto es lo que hay que cambiar para que no vuelva a ocurrir".