Integrated Framework for Operational Continuity and Reliability Assessment of Mission-Critical EMS Systems in Technological Transition

Marco Integrado de Continuidad Operativa y Evaluación de Confiabilidad para Sistemas EMS de Misión Crítica en Transición Tecnológica

M.L. Farinango[1] 0000-0002-7319-4614 G.P. Rivera[1] 0000-0002-3059-7974
F.A. de Lima[2] 0009-0002-0978-1950

[1]Operador Nacional de Electricidad CENACE, Quito, Ecuador
E-mail: lfarinango@cenace.gob.ec, grivera@cenace.gob.ec
[2]deBarr, Caracas, Venezuela
E-mail: fdelima@debarr.com

Abstract

The management of mission-critical operational technology (OT) platforms such as Energy Management Systems (EMS) that have exceeded their design useful life poses a major technical and strategic challenge for power System Operators (SO), particularly during prolonged technology transitions. This paper aims to assess the reliability and sustain the operational continuity of an EMS platform under obsolescence, through an integrated framework of seven strategic components supported by a quantitative formulation that combines availability, redundancy, bounded dynamic risk, and degraded service states modeled by a numerically solved four-state Markov chain. The approach is applied to the real case of the EMS platform of a System Operator (SO) in an emerging economy, currently transitioning toward a new EMS expected by 2027. Measured results include a baseline availability of 99.91 %, a mean time to repair (MTTR) of 2.7 h, and the rationalization of more than 20 % of historian signals; the Markov-based assessment yields an effective availability of approximately 99.91 %, and the dynamic risk model quantifies risk-exposure reductions in the range of 29–55 % per failure mode, while a threshold-based economic assessment establishes the cost-effectiveness condition of the plan. Collectively, these measures strengthen the operator's ability to maintain high availability and reduce risk exposure during the transition window, and provide a structured basis for prioritizing mitigation actions and supporting technical and managerial decision-making aimed at preserving the secure operation of the power system.

Index terms— Operational continuity, Availability, Reliability, EMS, Mission-critical systems, Risk management, Condition-based maintenance, Technology obsolescence.

Resumen

La gestión de plataformas de tecnología operacional de misión crítica como los Sistemas de Gestión de Energía (EMS, *Energy Management System*) que han superado su vida útil de diseño constituye un desafío técnico y estratégico para los Operadores de Sistemas (OS), particularmente durante transiciones tecnológicas prolongadas. Este artículo tiene por objetivo evaluar la confiabilidad y sostener la continuidad operativa de un EMS en obsolescencia, mediante un marco integrado de siete componentes estratégicos respaldado por una formulación que articula disponibilidad, redundancia, riesgo dinámico acotado y estados degradados de servicio modelados con cadenas de Markov de cuatro estados. El enfoque se aplica al caso real del EMS de un OS con economía emergente, en transición hacia un nuevo EMS previsto para 2027. Los resultados incluyen una disponibilidad de 99,91 %, un tiempo medio de reparación (MTTR, Mean Time To Repair) de 2,7 h y la racionalización de más del 20% de señales de historización; la evaluación mediante Markov entrega una disponibilidad del orden de 99,91 %, y el modelo de riesgo dinámico cuantifica reducciones en el rango de 29–55 % por modo de falla, mientras que la evaluación económica por análisis de umbral establece la condición de costo-efectividad del plan. En conjunto, estas medidas fortalecen la capacidad del OS para sostener alta disponibilidad y reducir la exposición al riesgo durante la ventana de transición y aportan una base estructurada para priorizar medidas de mitigación y apoyar la toma de decisiones técnicas y de gestión para preservar la operación segura del sistema eléctrico.

Palabras clave— Continuidad operativa, Disponibilidad, Confiabilidad, EMS, Cadena de Markov, Sistemas de misión crítica, Gestión de riesgos, Mantenimiento basado en la condición, Obsolescencia tecnológica.

Recibido: 29-04-2026, Aprobado tras revisión: 20-07-2026
Forma sugerida de citación: Farinango, L.; Rivera, G.; De Lima, F. (2026) "Marco Integrado de Continuidad Operativa y Gestión de Riesgos para Sistemas EMS de Misión Crítica en Transición Tecnológica". Revista Técnica ***"energía"***. No. 23, Issue I.
Pp. 33-54
ISSN On-line: 2602-8492 - ISSN Impreso: 1390-5074
Doi: https://doi.org/10.37116/revistaenergia.v23.n1.2026.760

1. INTRODUCCIÓN

La operación coordinada de un sistema eléctrico de potencia interconectado con otros países requiere plataformas de tecnología operacional (OT, Operational Technology) de misión crítica capaces de consolidar en tiempo real la información de generación, transmisión, subtransmisión e interconexiones internacionales. Estas plataformas, conocidas como Sistemas de Gestión de Energía (EMS, Energy Management System), soportan funciones esenciales como la adquisición de datos SCADA (Supervisory Control and Data Acquisition), el Control Automático de Generación (AGC, Automatic Generation Control), el Estimador de Estado (SE, State Estimator), el Análisis de Contingencias (CA, Contingency Analysis), el Flujo de Potencia del Operador (DPF, Dispatcher Power Flow), el Flujo de Potencia Óptimo (OPF, Optimal Power Flow) y el Flujo de Potencia Óptimo con Restricciones de Seguridad (SCOPF, Security-Constrained Optimal Power Flow) [1], [2]. En el caso del operador de sistema bajo estudio (en adelante, el OS), la plataforma EMS integra más de 50 000 señales y ejecuta más de 13 000 subrutinas sobre aproximadamente 700 000 líneas de código, lo que refleja el elevado nivel de complejidad funcional y tecnológica característico de este tipo de sistemas.

No obstante, los estándares industriales [3], [4] sitúan la vida útil de diseño (*design useful life*) de estas plataformas entre 8 y 10 años. Conviene distinguir esta magnitud del horizonte operativo real y de la ventana de transición tecnológica. La primera corresponde a la vida útil para la cual el activo fue concebido por el fabricante, mientras que la ventana de transición designa el periodo, típicamente de 24 a 48 meses, durante el cual el operador migra hacia una nueva plataforma y debe sostener simultáneamente la operación del sistema heredado. Superar la vida útil de diseño activa vectores de riesgo críticos, entre ellos la discontinuidad del soporte de hardware, la limitada capacidad de escalamiento frente a nuevas tecnologías como renovables y almacenamiento; y una mayor vulnerabilidad durante la propia ventana de transición. En este contexto, la probabilidad de falla tiende a incrementarse de manera no lineal, en concordancia con la zona de desgaste de la curva de bañera (*bathtub curve*) [5], lo que exige evolucionar desde un enfoque predominantemente reactivo hacia una gestión preventiva formal de riesgos orientada a la continuidad operativa.

La literatura relacionada con la continuidad operativa ha evolucionado desde marcos generales de gestión de continuidad y riesgo, como ISO 22301 e ISO 31000 [6], [7], hacia normativas y marcos específicos para infraestructuras críticas, como NERC CIP y los enfoques de ciberseguridad promovidos por NIST e IEC [8]–[11]. En el ámbito de los sistemas eléctricos, NERC CIP aborda requisitos de protección y resiliencia para sistemas de control de infraestructura crítica [8], mientras que el Cybersecurity Framework del NIST proporciona una estructura escalable para la identificación, protección, detección, respuesta y recuperación frente a amenazas [9]. Por su parte, la serie IEC 62443 complementa este enfoque mediante requisitos específicos para redes y sistemas industriales [10] y la norma IEEE Std 1686 define capacidades de ciberseguridad aplicables a dispositivos electrónicos inteligentes [11].

En paralelo, diversas investigaciones han abordado la cuantificación de la disponibilidad y la confiabilidad mediante modelos estocásticos. Los trabajos de Billinton y Allan [12] establecieron bases analíticas fundamentales para la evaluación de confiabilidad en sistemas eléctricos, posteriormente extendidas por Chowdhury y Koval [13] a plataformas de control industrial. Asimismo, la modelación de estados degradados mediante cadenas de Markov ha sido explorada por Rausand y Høyland [14] y aplicada a sistemas SCADA por Bompard et al. [15]. En esta misma línea, EPRI ha publicado mejores prácticas para la extensión de vida útil de plataformas EMS/SCADA [16], mientras que CIGRÉ ha desarrollado lineamientos sobre estrategias de modernización de plataformas EMS [17].

Complementariamente, las estrategias de confiabilidad han transitado desde esquemas basados estrictamente en el tiempo hacia enfoques de confiabilidad y mantenimiento basados en la condición (CBM, *Condition-Based Maintenance*), en los cuales las decisiones de intervención se adoptan según el estado real y el desempeño observado del equipo y no únicamente a partir de estimaciones temporales [18], [19]. Este paradigma resulta particularmente pertinente para plataformas EMS que han superado su vida útil de diseño.

La observación continua de indicadores operativos, utilización de recursos, latencias, tasas de error y eventos de degradación permite anticipar la transición hacia estados de servicio degradado y calibrar la dinámica de riesgo a partir de datos reales, en lugar de asumir tasas de falla puramente teóricas. Como se mostrará, la formulación de riesgo dinámico de este trabajo se ancla precisamente en una tendencia de utilización observada, lo que la sitúa dentro de la lógica CBM.

Adicionalmente, las técnicas de priorización y evaluación de riesgos han sido empleadas para apoyar la gestión en entornos complejos. El Análisis de Modos de Falla y Efectos (FMEA, *Failure Mode and Effects Analysis*) ha sido ampliamente documentado por Stamatis [20] y posteriormente adaptado al contexto de sistemas de protección, automatización y control por Apostolov [21]. De forma complementaria, la valoración económica de la carga no servida (VoLL, *Value of Lost Load*) aporta una base metodológica para el análisis costo-beneficio de medidas orientadas a reducir el impacto de interrupciones; no obstante, su aplicación a sistemas de control exige un tratamiento cuidadoso de la cadena causal entre la indisponibilidad del sistema de

control y la pérdida efectiva de suministro, aspecto que este trabajo formaliza explícitamente [22], [23].

Sin embargo, a pesar de este cuerpo de conocimiento, persiste una brecha en la literatura relacionada con la limitada disponibilidad de marcos integrados que articulen, dentro de un mismo esquema, componentes técnicos, organizativos y cuantitativos específicamente orientados a plataformas EMS en condiciones de obsolescencia tecnológica. También se observa una escasa formalización de la dinámica de riesgo bajo degradación temporal acelerada y, de manera particular, una reducida documentación de casos reales en Operadores de Sistemas de economías emergentes, donde las restricciones presupuestarias, institucionales y normativas condicionan de forma significativa las estrategias de transición tecnológica.

Para abordar estas deficiencias, este artículo presenta las siguientes contribuciones principales:

1. Propone un Marco Integrado de Continuidad Operativa, estructurado en siete componentes estratégicos, para la gestión de plataformas EMS en condiciones de obsolescencia tecnológica.

2. Desarrolla una formulación cuantitativa de soporte que integra disponibilidad, redundancia y estados degradados de servicio mediante una cadena de Markov de cuatro estados resuelta numéricamente para la evaluación de confiabilidad, junto con un modelo de riesgo dinámico acotado por tasa de riesgo, físicamente consistente con la zona de desgaste.

3. Aplica el marco propuesto al caso real de la plataforma EMS del OS bajo estudio, documentando resultados operacionales medidos y atribuyéndolos a los componentes del marco, con el fin de evaluar su utilidad práctica en un entorno de transición tecnológica prolongada.

4. Define un conjunto de indicadores clave de desempeño KPIs, (Key Performance Indicators) con umbrales operativos y formula una evaluación económica por análisis de umbral (threshold analysis), robusta frente a la disponibilidad limitada de datos por confidencialidad, para apoyar el monitoreo del plan y la toma de decisiones de gobernanza operativa.

El resto de segmentos del artículo se organizan en seis secciones. La Sección 2 desarrolla el marco teórico y la formulación matemática. La Sección 3 presenta el diagnóstico del sistema bajo estudio, incluyendo el análisis FMEA. La Sección 4 describe el marco integrado de continuidad operativa y sus siete componentes. La Sección 5 expone la aplicación al caso de estudio y discute los resultados, incluyendo las lecciones aprendidas. La Sección 6 resume las conclusiones y el trabajo futuro.

2. MARCO TEÓRICO Y FORMULACIÓN MATEMÁTICA

La gestión de continuidad operativa de una plataforma EMS en obsolescencia requiere un soporte cuantitativo que permita, primero, caracterizar el estado de confiabilidad del sistema; segundo, anticipar la evolución temporal del riesgo en la zona de desgaste; y tercero, sustentar económicamente las decisiones de mitigación. Esta sección presenta esa formulación en cinco bloques: disponibilidad y redundancia, riesgo, confiabilidad por cadenas de Markov, priorización por FMEA y evaluación económica, finalizando con una declaración explícita de sus limitaciones. Cada bloque se aplica numéricamente al caso de estudio en la Sección 5.

2.1 Modelo de Disponibilidad con Redundancia

La disponibilidad de estado estable de un componente reparable se define como la fracción de tiempo en que el sistema permanece operativo, en función de su tiempo medio entre fallas y su tiempo medio de reparación, conforme a las definiciones normalizadas de confiabilidad y disponibilidad [12], [24]:

$$A = \frac{MTBF}{MTBF + MTTR} \tag{1}$$

Donde A (*Availability*) es la disponibilidad adimensional, en [0,1], MTBF (*Mean Time Between Failures*) es el tiempo medio entre fallas y MTTR (*Mean Time To Repair*) es el tiempo medio de reparación, ambos términos se expresan en unidades de tiempo coherentes.

La indisponibilidad anual asociada, expresada en horas por año, se obtiene como:

$$U = (1 - A) \cdot 8760 \quad [\text{h/año}] \tag{2}$$

Donde U (*Unavailability*) es la indisponibilidad anual en horas y 8760 es el número de horas en un año no bisiesto.

Una disponibilidad de cuatro nueves (A=0,9999) corresponde a U≈ 52,56 min/año, valor que constituye la meta de referencia del indicador de disponibilidad.

Cuando el servicio se sostiene mediante arquitecturas redundantes, la disponibilidad equivalente depende de la configuración. Para n componentes en redundancia paralela, el subsistema opera si al menos uno está disponible [13]:

$$A_{par} = 1 - \prod_{i=1}^{n}(1 - A_i) \tag{3}$$

Donde Ai son las disponibilidades de los componentes individuales de un total de m componentes.

Para n componentes en serie, el subsistema opera solo si todos sus elementos A_j están disponibles:

$$A_{ser} = \prod_{i=1}^{n} A_i \tag{4}$$

La disponibilidad de una arquitectura serie-paralelo A_{eq} se obtiene combinando las ecuaciones (3) y (4) según el tipo de topología. Una cadena de subsistemas redundantes en serie-paralelo se obtiene como:

$$A_{\text{eq}} = \prod_{k} \left[1 - \prod_{i} (1 - A_{ik}) \right] \tag{5}$$

Donde A_{ik} es la disponibilidad del componente i del subsistema redundante k. La defensa en profundidad descrita en la Sección 4, es decir, sistema principal y respaldos de SCADA y AGC, responde a esta lógica de redundancia, en donde su efecto es mejorar A_{eq} por encima de la disponibilidad del sistema principal aislado.

La redundancia paralela opera como un esquema de protección con respaldo, es decir, para que exista la pérdida de suministro se requiere que falle simultáneamente la protección principal y la de respaldo, de modo que la probabilidad conjunta del evento indeseado es el producto de probabilidades individuales, cuyo valor es pequeño aun cuando cada una no lo sea.

2.2 Cuantificación de Riesgo Operacional

La cuantificación del riesgo en infraestructuras críticas adopta el marco general establecido por la norma ISO 31000 [7], que define el riesgo como la combinación de la probabilidad de un evento y sus consecuencias. Esta formulación ha sido analizada al dominio de sistemas industriales por Stamatis [20] y aplicada específicamente a sistemas SCADA por Bompard et al. [15].

El riesgo asociado a un modo de falla se cuantifica convencionalmente como el producto de su probabilidad de ocurrencia por su impacto [7]:

$$R = P \cdot I \tag{6}$$

Donde R es el índice de riesgo, P la probabilidad de ocurrencia e I el impacto, todos normalizados en [0,1] mediante la escala de mapeo cualitativo-cuantitativo de la Tabla I (Sección 3). La expresión (6) proporciona una fotografía estática del riesgo, adecuada para ordenar modos de falla en un instante dado, pero insuficiente para representar la degradación temporal acelerada que es una característica de la zona de desgaste, donde la propensión a la falla crece de forma no lineal con el tiempo.

Para un sistema expuesto a n amenazas independientes durante una ventana temporal arbitraria, el riesgo acumulado se expresa mediante [14]:

$$R_{total} = \sum_{i=1}^{n} P_i \cdot I_i \cdot E_i \tag{7}$$

Donde $E_i \in [0,1]$ representa el factor de exposición asociado a la amenaza i, utilizado para ponderar su contribución relativa dentro de la ventana de vulnerabilidad analizada. Este factor incorpora la influencia de la duración o persistencia de la condición de exposición sobre el nivel total de riesgo.

Para capturar esa dinámica se adopta una formulación basada en la tasa de riesgo (*hazard rate*), físicamente consistente con la zona de desgaste de la curva de bañera, en la que la tasa de fallas es creciente con el tiempo [5], [14]. Dentro de la ventana de transición, dicha tasa se modela con crecimiento exponencial. Esta forma corresponde a la ley de Gompertz, cuya tasa de riesgo es:

$$\lambda(t) = \lambda_0 \, e^{\alpha t} \tag{8}$$

Donde $\lambda(t)$ es la tasa de riesgo instantánea, λ_0 la tasa de falla base del modo al inicio de la ventana de tiempo, α el coeficiente de degradación por envejecimiento (en mes^{-1}) y t el tiempo transcurrido (en meses). El parámetro λ_0 se calibra a partir de la frecuencia de ocurrencia del modo en el FMEA. El factor α conocido como el factor de envejecimiento, hará que la tasa crezca si $\alpha > 0$. Su valor se obtiene a partir de la tendencia de degradación observada en los indicadores operativos del sistema, en línea con el enfoque de confiabilidad basada en la condición [18], [19].

La probabilidad acumulada de ocurrencia de al menos una falla crítica del modo en el intervalo [0, t] se obtiene mediante la relación estándar de confiabilidad entre la función de riesgo acumulado y la probabilidad de falla:

$$F(t) = 1 - \exp\left[-\frac{\lambda_0}{\alpha} (e^{\alpha t} - 1) \right] \tag{9}$$

Donde F(t) es la probabilidad acumulada de falla, acotada por construcción en el intervalo [0, 1], puesto que resulta de $1\text{-}e^{-\Lambda(t)}$ con $\Lambda(t)=\in t_0{}^t\lambda(\tau)\, d\tau \geq 0$. Esta propiedad de acotamiento es la diferencia esencial respecto de una formulación que multiplique directamente un índice de riesgo por un factor exponencial no acotado, debido a que tal producto puede exceder la unidad y perder su interpretación probabilística, mientras que (9) permanece siempre dentro de [0, 1].

El efecto de las medidas de mitigación se incorpora reduciendo la tasa de riesgo efectiva mediante un factor de completitud de mitigación:

$$M(t) = \sum_{k} w_k c_k(t), \quad \sum_{k} w_k \leq 1 \tag{10}$$

Donde M(t) es la completitud de mitigación acumulada en [0,1], w_k es la ponderación de la acción de mitigación k, cuyo valor representa la contribución máxima a la reducción del riesgo del modo y $c_k(t) \in [0, 1]$ es el grado de avance de la acción en el tiempo t.

La restricción $\sum k \, w_k \leq 1$ admite deliberadamente sumas inferiores a la unidad. El complemento $1 - \sum k \, w_k$ representa la porción de riesgo que las acciones contempladas no alcanzan a mitigar, es decir, es el riesgo residual estructural.

La tasa efectiva de fallas $\lambda_{\text{eff}}(t)$ se expresa como:

$$\lambda_{\text{eff}}(t) = \lambda_0 \, e^{\alpha t} \left(1 - M(t)\right) \tag{11}$$

Donde λ_0 la tasa de falla base del modo al inicio de la ventana de tiempo, α es el coeficiente de degradación por envejecimiento, $e^{\alpha t}$ es el crecimiento exponencial de la tasa de fallas por desgaste, $M(t)$ es el factor de mitigación, es decir, representa la efectividad del mantenimiento o las acciones correctivas. $1 - M(t)$ es la cantidad de fallas que no pudieron ser mitigadas.

La probabilidad acumulada de falla mitigada $F_{\text{mit}}(t)$, es decir, la probabilidad de que el sistema falle antes del tiempo t considerado para el mantenimiento se expresa como:

$$F_{\text{mit}}(t) = 1 - \exp\left[-\int_0^t \lambda_{\text{eff}}(\tau)\, d\tau\right] \tag{12}$$

Donde $\exp\left[-\int_0^t \lambda_{\text{eff}}(\tau)\, d\tau\right]$ es conocida como la función de supervivencia, es decir, la probabilidad de no haber fallado hasta el tiempo t. La expresión completa representa la probabilidad de falla de un sistema que envejece exponencialmente, pero que ese envejecimiento se mitiga mediante mantenimiento programado que se ejecuta a lo largo de la ventana de tiempo.

Finalmente, el riesgo dinámico del modo, ponderado por su impacto, se define como:

$$R(t) = F(t) \cdot I, \quad 0 \le R(t) \le I \tag{13}$$

Donde I es el impacto normalizado del modo. La reducción de exposición lograda por la mitigación se expresa como la diferencia $R_{sin}(t) - R_{con}(t) = [F(t) - F_{mit}(t)] \cdot I$, que depende de la integral de la tasa de riesgo y no se reduce a una identidad trivial con M(t). Esta es una propiedad deseable de la formulación. La dinámica temporal del modelo contribuye efectivamente al resultado. El acotamiento de (10) es análogo a la saturación de un integrador de anti enrollamiento *anti-windup* que deja de acumular cuando llega a un valor máximo hasta que la señal de error cambie y permita reducir esta acumulación, consiguiendo que por intensa que sea la tasa de riesgo creciente, la probabilidad de falla nunca rebasa su límite físico.

2.3 Evaluación de Confiabilidad y Estados Degradados Aplicando la Cadena de Markov

La continuidad operativa de una plataforma EMS no es un fenómeno binario con estados disponible e indisponible. Ante la degradación, el sistema transita por niveles intermedios de servicio. Esta dinámica se formaliza como una Cadena de Markov de tiempo continuo de cuatro estados, formalismo validado en la evaluación de confiabilidad de sistemas reparables [14] y aplicado a infraestructuras SCADA por Bompard et al. [15]. Los estados son: S_1, Normal (100% de funcionalidad); S_2, Degradado Leve (funciones críticas operativas); S_3, Degradado Severo (solo SCADA básico); y S_4, Emergencia (indisponibilidad del sistema principal y operación mediante respaldos).

La dinámica de transición entre estados adyacentes se describe mediante la matriz generadora Q de una Cadena de Markov de Tiempo Continuo, donde λ_{ij} son las tasas de degradación y μ_{ji} las tasas de recuperación:

$$Q = \begin{bmatrix} -\lambda_{12} & \lambda_{12} & 0 & 0 \\ \mu_{21} & -(\mu_{21} + \lambda_{23}) & \lambda_{23} & 0 \\ 0 & \mu_{32} & -(\mu_{32} + \lambda_{34}) & \lambda_{34} \\ 0 & 0 & \mu_{43} & -\mu_{43} \end{bmatrix} \tag{14}$$

A la matriz Q también se la conoce como la Matriz Tridiagonal, puesto que está conformada por una diagonal superior que determina las tasas de transición hacia estados más degradados, una diagonal inferior que determina las tasas de transición hacia estados de mejor funcionalidad y la diagonal principal, en donde cada elemento de la diagonal es el negativo de la suma de las tasas de salida del estado, de modo que cada fila suma cero para garantizar que la probabilidad total se conserve.

El diagrama de la cadena de Markov de cuatro estados de tiempo continuo se presenta en la Fig. 1.

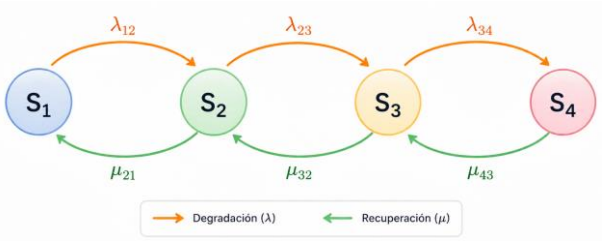

Figura 1: Diagrama de Transición de Estados de la Matriz Q

Siendo S_1, S_2, S_3 y S_4 los estados que representan:

- S_1: Normal (100 % funcionalidad),
- S_2: Degradado Leve (funciones críticas operativas)
- S_3: Degradado Severo (solo SCADA básico)
- S_4: Emergencia (indisponibilidad total de sistema principal y operación mediante sistemas de respaldo)

En la distribución de probabilidad estacionaria $\pi = (\pi_1, \pi_2, \pi_3, \pi_4)$ la fracción de tiempo de largo plazo que el sistema permanece en cada estado, se obtiene resolviendo el balance presentado a continuación:

$$\pi\, Q \;=\; 0, \qquad \sum_{i=1}^{4} \pi_i \;=\; 1 \tag{15}$$

A partir de π se define la disponibilidad efectiva del servicio, que pondera cada estado por su capacidad funcional:

$$A_{\text{ef}} = \sum_{i=1}^{4} \pi_i \; a_i \qquad (16)$$

Donde $a_i \in [0,1]$ es la capacidad funcional del estado i, con $a_{S1} = 1$ para el estado Normal y $a_{S4} = 0$ para el estado de Emergencia. Los valores intermedios se definen según el grado de funcionalidad preservada. A diferencia de la disponibilidad binaria de (1), A_{ef} reconoce el valor operativo de los estados degradados, en los que el sistema mantiene funciones esenciales aunque no la totalidad de sus capacidades. Las tasas λ_{ij} y μ_{ji} se calibran a partir de datos operativos del caso de estudio como frecuencias de degradación derivadas de la ocurrencia FMEA y tiempos de recuperación derivados del MTTR observado, cuya resolución numérica se presenta en la Sección 5.2.

2.4 Priorización de Modos de Falla FMEA

La priorización de modos de falla se realiza mediante el Análisis de Modos de Falla y Efectos (FMEA), que asigna a cada modo un Número de Prioridad de Riesgo (RPN, *Risk Priority Number*) como producto de tres factores [20], [21]:

$$RPN = S \cdot O \cdot D \qquad (17)$$

Donde S es la severidad del efecto, O la ocurrencia (frecuencia del modo) y D la detectabilidad, cada uno en una escala ordinal de 1 a 10. Conviene precisar la convención de la escala de detectabilidad adoptada: D=1 corresponde a un modo de falla fácilmente detectable y D=10 a uno prácticamente indetectable; en consecuencia, un valor alto de D señala dificultad de detección. Las anclas de las tres escalas, el procedimiento de elicitación de S, O y D, el umbral de priorización y su justificación para el dominio EMS se desarrollan en la Sección 3.

2.5 Evaluación Económica por Análisis de Umbral

La justificación económica del plan de continuidad requiere estimar el costo esperado de las interrupciones evitadas. La valoración de la carga no servida (VoLL) ofrece una base para ello, pero su aplicación a un sistema de control exige tratar explícitamente la cadena causal entre la indisponibilidad del EMS y la pérdida efectiva de suministro [22], [23]. Esta cadena no es directa debido a la defensa en profundidad (respaldos de SCADA y AGC), la indisponibilidad del sistema principal solo se traduce en pérdida de carga si dicha defensa también es vencida, considerado como un evento de orden superior y, por tanto, de baja probabilidad.

Se distingue, en consecuencia, entre una cota superior pesimista y un costo esperado realista. La cota superior supone transferencia total de la indisponibilidad a energía no servida sobre la carga completa:

$$C_{\max} = \text{VoLL} \cdot P_{\text{carga}} \cdot t_{\text{down}} \qquad (18)$$

Donde $C_{\max}$ es el costo máximo (USD), VoLL el valor de la carga no servida (USD/MWh), P_{carga} la potencia media de la carga (MW) y t_{down} el tiempo de indisponibilidad considerado en horas. El costo esperado realista corrige esta cota mediante dos factores condicionales de probabilidad y cobertura:

$$\mathbb{E}[C] = C_{\max} \cdot p_{\text{prop}} \cdot f_{\text{carga}} \qquad (19)$$

Donde p_{prop} es la probabilidad de que la falla del EMS se propague hasta una pérdida efectiva de suministro pese a los respaldos, es decir, la probabilidad de vencer la defensa en profundidad y $f_{\text{carga}} \in [0,1]$ es la fracción de la carga realmente en riesgo, determinada por la naturaleza de las funciones afectadas.

Dado que p_{prop} involucra datos sensibles de incidentes, no se afirma un valor puntual del beneficio, sino que se adopta un análisis de umbral: el plan de continuidad es un costo-efectivo cuando el costo esperado evitado supera la inversión del plan:

$$\theta^* = \frac{C_{\text{plan}}}{C_{\max}}; \qquad (20)$$

$$\text{plan costo-efectivo} \Leftrightarrow p_{\text{prop}} \cdot f_{\text{carga}} > \theta^*$$

Donde C_{plan} es el costo de implementación del plan y $\theta*$ el umbral mínimo del producto $p_{\text{prop}} \cdot f_{\text{carga}}$ requerido para la justificación. La conclusión económica se establece demostrando que el producto $p_{\text{prop}} \cdot f_{\text{carga}}$ supera holgadamente a $\theta*$ para todo el rango defendible de VoLL, sin necesidad de revelar el valor exacto de los parámetros condicionales que son datos confidenciales. La Sección 5.5 presenta el análisis de sensibilidad correspondiente.

2.6 Limitaciones de la Formulación

Por transparencia metodológica, se declaran explícitamente las limitaciones de la formulación, cuyo alcance condiciona la interpretación de los resultados de la Sección 5:

1. Carácter indicativo de la evaluación económica. Las expresiones (18)-(20) constituyen una estimación de orden de magnitud orientada a la toma de decisiones, no una auditoría costo-beneficio. El parámetro p_{prop} se trata como una cota conservadora derivada de registros internos, no publicables en detalle por confidencialidad; en consecuencia, el resultado económico se expresa como una condición de umbral y no como un beneficio puntual.
2. Supuestos de la cadena de Markov. El modelo (14)–(16) asume transiciones markovianas entre estados adyacentes con tasas constantes en el régimen estacionario; su calibración depende de la calidad de los datos operativos disponibles y de la representatividad de la ventana de observación.

3. Alcance del modelo de riesgo dinámico. Las expresiones (8)–(13) modelan la degradación en la zona de desgaste mediante una tasa de riesgo exponencial; la calibración de λ_0 y α está sujeta a la incertidumbre propia de la estimación a partir de datos históricos, por lo que la Sección 5.3 incluye un análisis de sensibilidad sobre estos parámetros y sobre los pesos w_k.
4. Normalización de impactos. Los valores de P, I, S, O y D provienen de un proceso de elicitación experta documentado en la Sección 3; aunque trazable, conserva el carácter ordinal inherente a las escalas cualitativas.

3. DIAGNÓSTICO DEL SISTEMA BAJO ESTUDIO

El sistema analizado corresponde a una plataforma EMS comercial desplegada sobre una arquitectura redundante, cuya infraestructura de Hardware ha superado su horizonte útil de diseño. Desde el punto de vista funcional, la plataforma EMS comprende seis subsistemas principales: adquisición de datos SCADA, procesamiento de aplicaciones avanzadas, historiador de proceso, gestión de alarmas, interfaz humano-máquina y comunicaciones para el esquema de AGC de respaldo.

En cuanto a la integración de información y aplicaciones, la plataforma se apoya en los estándares IEC 61970 (*Common Information Model*, CIM) [25] e IEC 61968 [26]. Por su parte, el subsistema de comunicaciones implementa los protocolos ICCP/TASE.2 para la interconexión con operadores de países vecinos, así como DNP3, IEC 60870-5-101 e IEC 60870-5-104 para la adquisición de datos desde unidades terminales remotas (RTU) ubicadas en subestaciones de centrales de generación.

3.1 Caracterización de Obsolescencia Tecnológica

El diagnóstico identifica tres dimensiones de obsolescencia operando simultáneamente. La Fig. 2 sitúa el sistema en la zona de desgaste de la curva de ciclo de vida, donde la tasa de fallas crece de manera no lineal con el tiempo.:

- **Dimensión 1 – Hardware:** La plataforma de procesamiento y almacenamiento ha superado su horizonte útil de diseño. El mercado de repuestos presenta una disponibilidad cada vez más limitada y costos crecientes. Además, los recursos de memoria y almacenamiento fueron dimensionados para condiciones operativas inferiores a las demandas actuales del sistema eléctrico. A ello se suma la degradación natural del rendimiento derivada de años de operación continua, lo que restringe la capacidad de crecimiento frente a la incorporación de nuevas subestaciones
- **Dimensión 2 – Software:** La versión actualmente en operación presenta limitaciones estructurales para su actualización y evolución sobre la infraestructura instalada. Se identifican restricciones concretas en la capacidad de almacenamiento del historiador, saturación en tablas de cálculo y cuellos de botella en las colas de procesamiento de eventos y mensajes entre procesos.
- **Dimensión 3 – Temporal:** El proyecto de implementación del nuevo EMS se encuentra en fase inicial de ejecución, con una fecha estimada de puesta en servicio hacia finales de 2027. Esta situación configura una ventana de exposición operacional prolongada, que requiere una gestión activa de continuidad durante el período transitorio.

Figura 2: Curva de Ciclo de Vida del Sistema con Ubicación de Zona de Desgaste

3.2 Metodología de Evaluación de Riesgos: Escalas y Elicitación

La priorización de modos de falla mediante FMEA de la ecuación (17) requiere la asignación de los factores de Severidad (S), Ocurrencia (O) y Detectabilidad (D). Para garantizar la reproducibilidad del análisis, estos factores no se asignaron de forma ad hoc, sino mediante un procedimiento estructurado de elicitación experta.

La valoración fue realizada por un panel conformado por el equipo técnico responsable de la administración de la plataforma EMS y por expertos del sistema con experiencia directa en la gestión de plataformas en tiempo real. Cada factor se asignó sobre escalas ordinales ancladas de 1 a 10, conforme a las definiciones de Stamatis [20], mediante consenso y validación por revisión cruzada entre los miembros del panel. Las anclas adoptadas se resumen a continuación:

- **Severidad (S):** 1–2 insignificante (sin efecto operativo perceptible); 3–4 menor (degradación de funciones no críticas); 5–6 moderada (pérdida de aplicaciones avanzadas); 7–8 mayor (pérdida de funciones críticas con respaldo disponible); 9–10 catastrófica (pérdida de regulación de frecuencia o de supervisión).
- **Ocurrencia (O):** 1–2 remota (improbable en la ventana de transición); 3–4 baja (esporádica); 5–6

moderada (ocasional); 7–8 alta (frecuente, con tendencia creciente); 9–10 muy alta (recurrente o persistente).

- **Detectabilidad (D):** Bajo la convención adoptada, D=1 indica detección inmediata y D=10 falla prácticamente indetectable. Anclas: 1–2 detección muy alta (alarma automática inmediata); 3–4 alta (detectable por monitoreo rutinario); 5–6 moderada (detectable por inspección periódica); 7–8 baja (detectable solo en pruebas programadas: falla latente); 9–10 muy baja (prácticamente indetectable hasta el fallo en demanda).

El índice de riesgo estático representado en la ecuación (6) y el riesgo dinámico representado en la ecuación (11) operan sobre valores normalizados de probabilidad (P) e impacto (I) en el intervalo [0,1]. La Tabla I establece la correspondencia entre los niveles cualitativos, las bandas de la escala FMEA y los valores numéricos, en una escala homogénea de cinco niveles. Esta correspondencia hace trazable cada valor empleado en las secciones posteriores: por ejemplo, un modo con O=8 se clasifica como probabilidad "Alta" (P=0,80) y un modo con S=7 como impacto "Alto" (I=0,90), ambos dentro de la banda 7–8.

Tabla 1: Escala de Mapeo Cualitativo-Cuantitativo de Probabilidad e Impacto

Nivel Cualitativo	Banda FMEA (S, O)	Probabilidad (P)	Impacto (I)
Muy Bajo	1–2	0,10	0,15
Bajo	3–4	0,20	0,30
Medio	5–6	0,50	0,60
Alto	7–8	0,80	0,90
Muy Alta / Crítico	9–10	0,95	1,00

La definición explícita de esta escala resuelve la valoración del modo "saturación del historiador" que es directamente trazable a sus factores FMEA (O=8, S=7).

3.3 Análisis FMEA y Priorización de Modos de Falla

Aplicando la ecuación (17) a los modos de falla identificados, se obtuvo la priorización resumida en la Tabla II. Bajo el criterio adoptado en este trabajo, cuatro modos de falla superan el umbral de priorización $RPN \geq 125$: la saturación del historiador de proceso, la indisponibilidad del AGC principal, la degradación progresiva del subsistema de cálculos y el congelamiento de aplicaciones críticas que se resumen en la Tabla II.

La suma total de los RPN evaluados es 1052; los cuatro modos priorizados aportan 830, esto es, aproximadamente el 79,0 % de la exposición total. Este resultado confirma que el riesgo se concentra en un conjunto reducido de modos de falla, lo que facilita la focalización de las acciones de mitigación que se ilustran mediante un diagrama de Pareto presentado más adelante en la Fig. 3.

Tabla 2: Modos de Falla Principales y su Número Prioritario de Riesgo

Modo de Falla	Severidad (S)	Ocurrencia (O)	Detectabilidad (D)	RPN
Falla catastrófica de servidores principales	9	2	5	90
Corrupción de base de datos histórica	8	3	3	72
Saturación del historiador de proceso	7	8	5	280
Degradación progresiva del subsistema de cálculos	6	7	5	210
Indisponibilidad de AGC principal	10	3	6	180
Congelamiento de aplicaciones críticas	8	4	5	160
Pérdida de sincronización de tiempo	5	4	3	60

Se presenta el Diagrama de Pareto ordenado por RPN descendente.

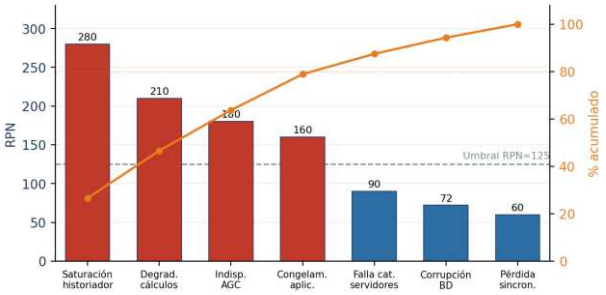

Figura 3: Diagrama de Pareto de los Modos de Falla Ordenados por RPN Descendente

3.3.1 Justificación del umbral de priorización para el contexto EMS

El umbral RPN ≥ 125 proviene del criterio reportado por Apostolov [21] para sistemas de protección, automatización y control. Dado que dicho dominio no es idéntico al de una plataforma EMS basada en software, su transferibilidad se sustenta sobre dos bases. Primera, en términos absolutos, RPN=125 corresponde a una combinación moderada-alta (del orden de 5×5×5) en las escalas 1–10, coherente con el criterio general de práctica FMEA que sitúa el umbral de acción prioritaria en torno a 100–125 para sistemas críticos [20].

Segunda, y de forma decisiva, la elección del umbral resulta robusta frente a su valor exacto en este caso: la distribución de RPN presenta una discontinuidad natural entre 90 y 160 (una banda vacía de 70 puntos), de modo que cualquier umbral dentro del intervalo (90, 160) produce el mismo conjunto de cuatro modos priorizados.

La priorización no depende, por tanto, de la calibración fina del umbral, sino de una separación estructural presente en los propios datos.

3.3.2 Justificación de la detectabilidad del modo "Indisponibilidad de AGC principal"

El modo "Indisponibilidad de AGC principal" presenta la máxima severidad (S=10, por su efecto sobre la regulación de frecuencia y los intercambios internacionales), una ocurrencia baja (O=3, por todas las acciones realizadas para evitar estas fallas) y una detectabilidad (D=6). Bajo la convención adoptada (D=10 indetectable), D=6 indica una dificultad moderada de detección de la falla.

La asignación D=6 responde a que el AGC principal depende de varios factores tanto internos como externos. Generalmente, los factores externos no pueden ser determinados de manera expedita. Esta característica de indisponibilidad no revelada por factores externos se penaliza con detectabilidad baja en las escalas FMEA.

Conviene notar que el factor de detectabilidad es determinante para la priorización, puesto que con una detectabilidad alta (por ejemplo, D=2), el RPN del modo descendería a 60 y quedaría fuera del conjunto priorizado. El reconocimiento de la falla latente por factores externos y su impacto en la operación del sistema eléctrico la sitúa correctamente en un modo de altísima severidad y baja detectabilidad dentro del enfoque del plan de continuidad operativa.

4. MARCO INTEGRADO DE CONTINUIDAD OPERATIVA

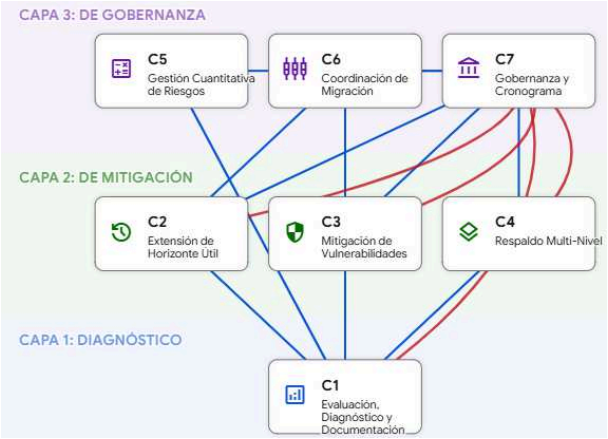

Figura 4: Diagrama Conceptual del Marco Integrado

El marco propuesto se estructura en siete componentes estratégicos interdependientes, concebidos como un sistema integrado de continuidad operativa. Su principio rector es que la resiliencia de una plataforma de misión crítica no depende únicamente de la redundancia de hardware, sino de la interacción coordinada entre infraestructura, procesos, capacidades humanas y capacidades organizativas.

La Fig. 4 presenta la articulación general de estos componentes, agrupados en tres dimensiones: técnica (C1–C4), de gestión (C5–C6) y organizacional (C7). Para sostener la trazabilidad entre el marco y la evidencia, cada componente se cierra con la indicación del indicador o resultado mediante el cual su efecto se evalúa en la Sección 5.

4.1 Componente C1 – Evaluación, Diagnóstico y Documentación

Este componente comprende una evaluación integral de la plataforma, orientada a generar cuatro entregables principales: un inventario consolidado de hardware y software, con estimación de la vida útil remanente por componente; un mapa de puntos únicos de falla (*Single Points of Failure*, SPOF); un catálogo actualizado de la documentación técnica; y un programa de transferencia de conocimiento dirigido al personal técnico de respaldo.

La transferencia de conocimiento mitiga de forma específica el riesgo organizacional asociado a la rotación, ausencia o pérdida de disponibilidad del personal clave. Este aspecto generalmente se subestima en los análisis convencionales de continuidad operativa.

La Evaluación de C1 se realiza en la Sección 5.4 que contiene la completitud de entregables (inventario, mapa de SPOF, programa de transferencia).

4.2 Componente C2 – Extensión de Horizonte Útil de Diseño

La extensión planificada del horizonte útil de diseño del sistema actual se apoya en tres estrategias complementarias: la adquisición anticipada de repuestos críticos, la ampliación del soporte contractual con el proveedor del software y la reducción sistemática de la carga computacional.

La reducción de la carga computacional constituye una estrategia transversal de alto impacto, implementada mediante la gestión selectiva de datos históricos, la depuración de señales de la base de datos, la optimización de consultas y reportes automáticos, el ajuste de tasas de escaneo para puntos no críticos y el monitoreo proactivo de los recursos del servidor, incluyendo CPU, memoria, disco y red.

La Evaluación de C2 se realiza con el KPI1 (disponibilidad), en la extensión de capacidad de historización reportada en la Tabla VII y en la calibración de α a partir de la tendencia de utilización en Sección 5.3.

4.3 Componente C3 – Mitigación de Vulnerabilidades de Software

Las vulnerabilidades del software y de su entorno operativo se abordan mediante un conjunto coordinado de acciones, entre ellas la verificación periódica de la sincronización de tiempo entre nodos, la revisión de registros de seguridad, la segmentación de red con aislamiento de sistemas críticos y la aplicación de un

criterio de equilibrio entre endurecimiento de seguridad y estabilidad operacional.

Este último principio reconoce que, en plataformas obsoletas, la introducción no controlada de actualizaciones o medidas de seguridad puede generar inestabilidad funcional. Por ello, se requiere un enfoque diferenciado de gestión del cambio, que permita reducir vulnerabilidades sin comprometer la continuidad operativa del sistema.

La Evaluación de C3 se realiza con KPI3 (incidentes no planificados) y en la cadencia de revisión de seguridad de la Sección 5.

4.4 Componente C4 – Arquitectura de Respaldo Multi-Nivel

La arquitectura de respaldo implementa el modelo de cuatro estados formalizado en las ecuaciones (10)–(12). Cada estado define un nivel funcional con procedimientos operativos específicos:

- **Nivel 1 – Normal:** Operación con el EMS principal y disponibilidad plena de funcionalidades.
- **Nivel 2 – Degradado Leve:** Actividades de mantenimiento de las funciones críticas con el SCADA principal operativo y limitaciones en las aplicaciones avanzadas.
- **Nivel 3 – Degradado Severo:** Operación restringida al SCADA básico, con las funciones analíticas avanzadas deshabilitadas.
- **Nivel 4 – Emergencia:** Indisponibilidad del EMS principal y operación mediante SCADA y AGC de respaldo

El componente se sustenta en tres pilares técnicos:

1. Un SCADA de respaldo con tiempo objetivo de conmutación menor a 15 minutos
2. Un AGC de respaldo implementado en una central de gran capacidad designada como central que ejecuta AGC, con verificación funcional mensual
3. Una estrategia reforzada de respaldo y recuperación, basada en copias incrementales diarias, copias completas semanales y un tiempo objetivo de restauración inferior a 4 horas

La Evaluación de C4 se realiza con el KPI5 (tiempo de conmutación), KPI2 (MTTR) y la disponibilidad efectiva A_{ef} obtenida del modelo de Markov que se presenta en la Sección 5.2.

4.5 Componente C5 – Gestión Cuantitativa de Riesgos

Este componente aplica las ecuaciones (6) y (8)–(11) a la matriz de amenazas identificadas, con el fin de estimar la exposición relativa del sistema y priorizar medidas de mitigación. La Tabla III resume las principales amenazas operacionales consideradas, junto con su caracterización cualitativa y las estrategias de mitigación asociadas. El riesgo total $R(t)$ se reevalúa trimestralmente, permitiendo ajustar dinámicamente el plan de contingencia en función de la evolución de la exposición y de la efectividad de las medidas implementadas

Tabla 3: Principales Amenazas Operacionales Externas y Medidas de Mitigación

Amenaza	Descripción	Probabilidad	Impacto	Estrategia de Mitigación
Fallas de hardware	Servidores, consolas o dispositivos de red que han superado su vida útil	Alta	Crítico	Repuestos estratégicos, contratos de soporte extendido
Fallas de software	Corrupción de bases de datos, errores de configuración	Media	Alto	Respaldos frecuentes, procedimientos de restauración validados
Ciberataque	Malware, *ransomware* o intrusiones que paralicen el sistema	Media-Alta	Crítico	Seguridad perimetral, segmentación de red, áreas de responsabilidad
Desastres físicos	Incendio, inundación, corte prolongado de energía	Baja	Crítico	Sitio alterno, UPS dimensionados

La Evaluación de C5 se realiza el ítem reducción de exposición por modo de falla del modelo de riesgo dinámico de la Sección 5.3 y el resultado de la reevaluación trimestral de riesgo.

4.6 Componente C6 – Coordinación con Migración Tecnológica

La estrategia de transición contempla interfaces entre el sistema actual y el nuevo EMS, sincronización de bases de datos, procedimientos operativos para la fase de convivencia y criterios objetivos de aceptación para la entrada en servicio. La preparación de la base de datos actual mediante depuración, optimización, estandarización de nomenclaturas y documentación de modelos, facilita la migración y reduce el riesgo asociado al proceso de *cutover* hacia el nuevo sistema.

Una contribución específica de este componente consiste en reconocer que muchas de las acciones de optimización requeridas para sostener la plataforma obsoleta constituyen, al mismo tiempo, actividades preparatorias para la migración tecnológica. Esta convergencia genera una sinergia concreta entre los objetivos de continuidad operativa de corto plazo y los objetivos de transición de mediano plazo.

La Evaluación de C6 se realiza con los hitos de preparación para la migración y estandarización de la base de datos (Tabla VII: definición de señales estándar).

4.7 Componente C7 – Gobernanza y Cronograma

El plan se desarrolla sobre un horizonte de 24 meses, comprendido entre enero de 2026 y diciembre de 2027 estructurada en ocho trimestres. El primer año abarca el establecimiento de la línea base, la implementación de mejoras urgentes, la validación del nivel de preparación y los ajustes al plan de contingencia. El segundo año comprende la preparación para la transición, el inicio de la migración, la fase activa de migración y el cierre formal del plan.

La gobernanza del componente se articula mediante revisiones mensuales de avance a nivel técnico, reuniones trimestrales del comité de seguimiento con participación ejecutiva y reportes periódicos al comité ejecutivo de la organización.

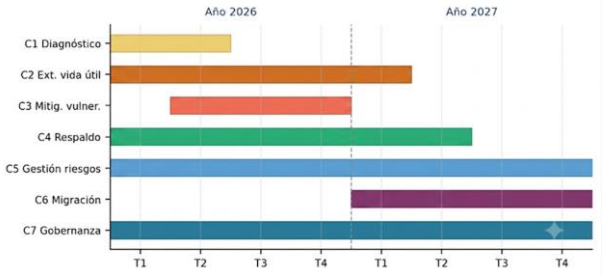

Figura 5: Diagrama de Gantt del Cronograma de los Siete Componentes

La Evaluación de C7 se realiza con KPI4 (desempeño de simulacros) y la adherencia de las actividades ejecutadas al cronograma trimestral presentadas en la Sección 5.4.

5. APLICACIÓN Y RESULTADOS

En esta sección se aplica el marco propuesto al caso de estudio y analiza la efectividad de los resultados. Se reporta primero la línea base de disponibilidad medida; a continuación se evalúa la confiabilidad mediante la Cadena de Markov, se aplica el modelo de riesgo dinámico a los cuatro modos priorizados, se atribuyen los resultados a los componentes del marco y se presenta la evaluación económica por umbral; finalmente se comparan los indicadores con referentes internacionales y se consolidan las lecciones aprendidas.

Es importante mencionar que los parámetros del modelo, tales como las tasas de Markov, λ_0, α y M por modo y parámetros económicos; corresponden a estimaciones derivadas de las metas de disponibilidad y de la ocurrencia FMEA y se identifican como valores a calibrar con datos operacionales longitudinales.

5.1 Línea Base de Disponibilidad Medida

La efectividad del marco de continuidad de la operación se mide mediante cinco KPIs presentados en la Tabla IV. Estos KPIs cubren las dimensiones de disponibilidad técnica, capacidad de recuperación, ocurrencia de incidentes, preparación del personal y efectividad de los sistemas de respaldo.

Tabla 4: Indicadores Clave de Desempeño del Marco de Continuidad Operativa

KPI	Métrica	Meta	V Medido	Responsable
KPI1: Disponibilidad EMS	% tiempo operativo	≥ 99,99 %	99,91 %	Adm. Técnica / Adm. Funcional
KPI2: MTTR	Tiempo promedio recuperación	≤ 4 h	2,7 h	Adm. Técnica / Adm. Funcional
KPI3: Incidentes no planificados	Número de caídas del sistema	Tendencia decreciente	1 período	Adm. Técnica / Adm. Funcional
KPI4: Desempeño de simulacros	% objetivos alcanzados	≥ 90 %	En medición	Adm. Funcional
KPI5: Tiempo de conmutación	Tiempo para activar respaldos	≤ 15 min	En medición	Adm. Funcional

La Fig. 6 presenta el *dashboard* de monitoreo correspondiente. El resultado más significativo es la brecha de disponibilidad: el valor medido de 99,91 % equivale a una indisponibilidad de aproximadamente 7,8 h/año que se obtiene de (1-0,9991) * 8760, frente a la meta de 99,99 %, que corresponde a 52,56 min/año. Esta brecha, lejos de constituir una contradicción del marco, cuantifica precisamente la exposición que el plan busca reducir y, por tanto, es el punto de partida de su evaluación.

Conviene interpretar correctamente este valor con respecto a los demás indicadores. Un MTTR de 2,7 h y un único incidente de indisponibilidad total no explican por sí solos una pérdida de 7,9 h: la diferencia corresponde a la operación en estados de servicio degradado, en los que el sistema permanece parcialmente funcional, pero por debajo de su capacidad plena. En consecuencia, el 99,91 % debe entenderse como una disponibilidad efectiva que es ponderada por la capacidad funcional de cada estado y no como una disponibilidad binaria. Esta interpretación es la que conecta la medición empírica con el modelo de Markov de la subsección siguiente, cuya disponibilidad efectiva A_{ef} se calibra precisamente para reproducir este valor observado.

5.2 Evaluación de Confiabilidad Mediante Cadena de Markov

Se resuelve numéricamente la Cadena de Markov de cuatro estados representadas en las ecuaciones (14)–(16) para el caso de estudio. Las tasas de transición se estiman a partir de la disponibilidad efectiva medida y de la ocurrencia FMEA, adoptando capacidades funcionales a_i coherentes con la definición de cada estado.

Tabla 5: Tasas de Transición Calibradas (Escenario Línea Base)

Parámetro	λ_{12}	λ_{23}	λ_{34}	μ_{21}	μ_{32}	μ_{43}
Valor (mes^{-1})	0,26	0,17	0,15	30,0	18,0	15,0

Capacidades funcionales adoptadas: $a_{S_1} = 1{,}00$ (Normal), $a_{S_2} = 0{,}90$ (Degradado Leve), $a_{S_3} = 0{,}50$ (Degradado Severo), $a_{S_4} = 0{,}00$ (Emergencia). Las tasas de degradación se derivan de la frecuencia de ocurrencia FMEA de cada modo prioritario proyectada sobre la ventana de transición; las tasas de recuperación se estiman a partir del MTTR observado de 2,7 h, ajustadas por estado según la complejidad del proceso de restauración. La condición de calibración exige $\mu_{ji} \gg \lambda_{ij}$ que es propia de un sistema reparable que se recupera mucho más rápido de lo que se degrada y se satisface con holgura: $\mu_{21}/\lambda_{12} = 115 \gg 1$.

La matriz generadora resultante Q, con filas $[S_1, S_2, S_3, S_4]$, es:

$$Q = \begin{pmatrix} -0{,}26 & 0{,}26 & 0 & 0 \\ 30{,}0 & -30{,}17 & 0{,}17 & 0 \\ 0 & 18{,}0 & -18{,}15 & 0{,}15 \\ 0 & 0 & 15{,}0 & -15{,}0 \end{pmatrix}$$

Resolviendo $\pi Q = 0$ con $\sum_i \pi_i = 1$ mediante balance detallado se obtiene la distribución estacionaria:

$$\boldsymbol{\pi} = (0{,}9913,\ 0{,}0086,\ 0{,}000081,\ 8{,}1 \times 10^{-7})$$

y aplicando (16), la disponibilidad efectiva:

$$A_{\text{ef}} = 0{,}9913(1{,}0) + 0{,}0086(0{,}9) + 0{,}000081(0{,}5) + 8{,}1 \times 10^{-7}(0) = 0{,}9991$$

Es decir, $A_{\text{ef}} = 99{,}91\,\%$. Este resultado es relevante en dos sentidos. Primero, reproduce la disponibilidad efectiva medida (99,91 %), lo que valida empíricamente la calibración del modelo y confiere significado operativo al formalismo de Markov más allá de su formulación. Segundo, muestra que la casi totalidad del tiempo de servicio se concentra en el estado normal ($S_1, \pi_1 = 99{,}13\,\%$), mientras que el servicio degradado leve ($S_2, \pi_2 \approx 0{,}86\,\%$) y los estados severos son marginales. Este patrón es consistente con un sistema que, pese a haber superado su vida útil de diseño, conserva sus funciones críticas gracias a la arquitectura de respaldo del Componente C4 y las acciones de mitigación realizadas en el sistema.

La indisponibilidad efectiva de la línea base equivale a $(1 - 0{,}9991) \cdot 8760 \approx 7{,}9$ h/año, frente a la meta de 99,99 % que corresponde a 52,6 min/año. La brecha de $\approx 7{,}0$ h/año cuantifica la exposición que el plan busca reducir.

Para evaluar el efecto proyectado del plan, se reestiman las tasas suponiendo que las medidas de mitigación reducen las tasas de degradación en $\approx$ 70 % y mejoran las de recuperación en 50 %: $\lambda'_{12} = 0{,}08$, $\lambda'_{23} = 0{,}05$, $\lambda'_{34} = 0{,}04$; $\mu'_{21} = 45{,}0$, $\mu'_{32} = 27{,}0$, $\mu'_{43} = 22{,}0$. La distribución resultante es:

$$\boldsymbol{\pi}' = (0{,}9982,\ 0{,}0018,\ 3{,}3 \times 10^{-6},\ 6{,}0 \times 10^{-9})$$

Donde $A'_{\text{ef}} \approx 99{,}98\,\%$. La indisponibilidad proyectada con el plan es $\approx 1{,}6$ h/año, lo que estrecha la brecha respecto de la meta de forma sustancial de 7,0 h/año a $\approx$ 0,7 h/año sin cerrarla por completo hasta el objetivo de 99,99%. Esta brecha residual de $\approx$ 42 min/año es coherente con la presencia de fallas de causa común, errores humanos sistémicos y dependencias compartidas que el marco mitiga pero no elimina.

5.3 Riesgo Dinámico Aplicado a los Cuatro Modos Críticos

Se aplica el modelo de riesgo dinámico acotado de las ecuaciones (8)–(13) a los cuatro modos priorizados en la Tabla II. Para cada modo, la tasa base λ_0 se estima a partir de la ocurrencia FMEA (mediante λ_0=(O/10)·0,1 mes^{-1}), el coeficiente de envejecimiento se adopta como α=0,05 mes^{-1} que es el valor derivado de la tendencia de utilización observada del historiador (5 % mensual), extendido a los demás modos, el impacto I se toma de la Tabla I según la severidad y la completitud de mitigación M(24) se estima a partir de las acciones de la Tabla VII asociadas a cada modo. La probabilidad de falla mitigada se evalúa mediante $F_{mit}(24) = 1 - (1 - F(24))(1 - M)$, que resulta de aplicar el factor (1-M) a la tasa de riesgo en (10) bajo la hipótesis de efectividad sostenida.

Tabla 6: Riesgo Dinámico de los Cuatro Modos Críticos (t = 24 Meses)

Modo de Falla	I	λ_0	M(24)	F(24)*	R(24)*	R(24) mit	R** %
Saturación Historiador	0,90	0,08	0,80	0,976	0,878	0,472	46,3
Indispon. AGC Pr.	1,00	0,03	0,70	0,751	0,751	0,341	54,6
Degrad. Cálculos	0,60	0,07	0,65	0,961	0,577	0,408	29,3
Cong. App Críticas	0,90	0,04	0,60	0,844	0,759	0,472	37,9

* Valores sin Mitigación ** Porcentaje de Reducción

Tres observaciones se desprenden de la Tabla VI. Primera, todos los valores de riesgo permanecen acotados en [0,1]. Segunda, las reducciones difieren entre modos (29,3 %–54,6 %) y no coinciden con el valor de M, lo que confirma que la dinámica temporal del modelo contribuye efectivamente al resultado. Tercera, el resultado actual constituye, por tanto, una estimación conservadora y defendible.

Dado que el resultado depende de parámetros estimados, se evalúa su sensibilidad para el modo de mayor exposición (historiador). Variando el coeficiente de envejecimiento, la reducción de exposición pasa de 54,2% (α=0,03) a 36,5 % (α=0,07), con 46,3 % en el caso base (α=0,05): un envejecimiento más rápido erosiona la efectividad de la mitigación. Variando la completitud de

mitigación, la reducción pasa de 31,2 % (M=0,70) a 68,2 % (M=0,90), con 46,3 % en el caso base (M=0,80). Esta fuerte dependencia respecto de M subraya la importancia de documentar y validar los pesos w_k y de sostener la efectividad de las acciones a lo largo de la ventana de transición.

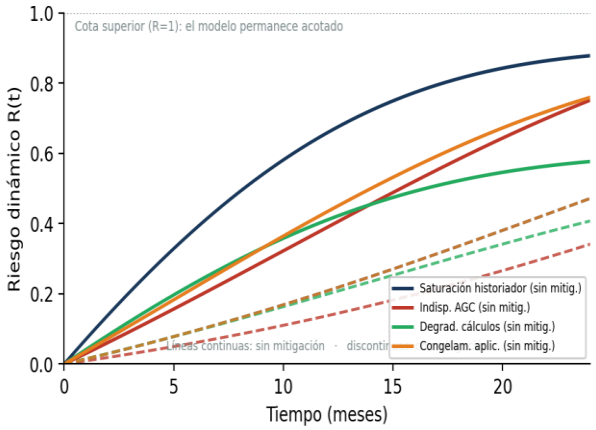

Figura 6: Trayectorias de Riesgo R(t) con y sin Mitigación para los Cuatro Modos Críticos.

5.4 Atribución de Resultados a los Componentes del Marco

Para evidenciar que los resultados derivan de la aplicación del marco, la Tabla VII mapea cada actividad preventiva ejecutada a su componente, al modo de falla FMEA que atiende, a su ubicación en el cronograma (Fig. 5) y a su efecto operacional antes/después.

Tabla 7: Actividades Preventivas Ejecutadas e Impacto Operacional

Actividad ejecutada	Componente	FMEA Atendido	Trimestre	Efecto antes → después
Racionalización > 20 % de señales de historización	C2	Saturación historiador	T1–T2 2026	Capacidad Historización extendida ≈ 24 meses
Optimización de cálculos	C2	Degrad. Cálculos	T2 2026	Reducción de carga en servidores aplicaciones
Incremento de colas de procesamiento	C2/C3	Congel. Apps	T2 2026	Mitigación de cuellos de botella ejecución
Gestión y racionalización de alarmas	C3	Reducción Procesamiento de Señales	T2–T3 2026	Reducción de carga en servidores aplicaciones
Definición de señales estándar	C6	Optimización BDD	T3–T4 2026	Reducción de tamaño BDD
Verificación funcional de AGC de respaldo	C4	Indispon. de AGC	Mensual (T1–T8)	Dispon. AGC alternativo

El mapeo evidencia que los modos de mayor exposición (Tabla II) son atendidos por actividades concretas vinculadas a componentes específicos y ejecutadas dentro del cronograma del Componente C7.

La concentración de las acciones de racionalización y optimización (C2) en el primer año, sobre los modos de saturación del historiador y degradación de cálculos, es coherente con la reducción de exposición estimada para esos modos en la Tabla VI. Asimismo, la verificación mensual del AGC de respaldo (C4) es la medida que atiende el modo de falla latente de máxima severidad identificado en la Sección 3.3.2.

5.5 Evaluación Económica por Análisis de Umbral

La justificación económica del plan se establece mediante el análisis de umbral formulado en la Sección 2.5, que evita afirmar un beneficio puntual y respeta la confidencialidad de los datos de incidentes. Se adopta como cota superior pesimista, bajo la hipótesis de transferencia total entre indisponibilidad del EMS y energía no servida, un valor representativo $C_{max} \approx 15{,}3M\ USD$ para la ventana de 24 meses, calculado con VoLL =5000 USD/MWh (valor intermedio del rango [2000, 8000] reportado en [23]) y la diferencia de indisponibilidad entre la línea base (99,91 %) y la meta (99,99 %).

El beneficio esperado realista corrige esta cota mediante los dos factores condicionales de la ecuación (19): $\mathbb{E}[C] = C_{\max} \cdot p_{\text{prop}} \cdot f_{\text{carga}}$. El plan es costo-efectivo cuando dicho beneficio supera su costo de implementación C_{plan}, esto es, cuando $p_{\text{prop}} \cdot f_{\text{carga}} > \theta* = C_{\text{plan}}/C_{\max}$. Para un costo de plan representativo del orden de 150 000 – 460 000 USD, el umbral θ* se sitúa entre 1,0 % y 3,0 %. La Tabla VIII presenta el análisis de sensibilidad del beneficio esperado frente a los rangos defendibles de VoLL y del producto $p_{\text{prop}} \cdot f_{\text{carga}}$ (la cota $C_{\max}$ escala proporcionalmente con VoLL respecto del valor base de 5000 USD/MWh).

Tabla 8: Sensibilidad del Beneficio Esperado (miles de USD)

$p_{\text{prop}} \cdot f_{\text{carga}}$	VoLL = 2000	VoLL = 5000	VoLL = 8000
1 %	61	153	245
2 %	123	306	490
3 %	184	459	734

La conclusión económica se establece, por tanto, como una condición de umbral: el plan es costo-efectivo para todo $p_{\text{prop}} \cdot f_{\text{carga}}$ superior a θ* (del orden de 1% – 3%), sin necesidad de afirmar el valor exacto de los parámetros condicionales. De forma corroborativa y subordinada, los registros operativos internos [27] indican que el producto $p_{\text{prop}} \cdot f_{\text{carga}}$ se encuentra acotado de manera conservadora por encima del umbral θ*. Este resultado es consistente con la pérdida efectiva de suministro que requiere vencer la defensa en profundidad de SCADA y AGC (Componente C4), que es un evento de orden superior. Esta evidencia interna confirma, sin exponer los datos sensibles, que la condición de costo-efectividad se satisface. La naturaleza indicativa de esta

estimación y el carácter no publicable de p_{prop} se declaran en la Sección 2.6.

5.6 Comparación con Referentes Internacionales

La Tabla IX compara las metas operativas del marco con valores de referencia reportados por organismos y publicaciones internacionales. Los objetivos adoptados para disponibilidad, tiempo medio de recuperación y frecuencia de pruebas de respaldo se sitúan en un rango exigente y consistente con prácticas documentadas para infraestructura crítica. Esta comparación es orientativa, ya que los marcos citados no siempre presentan métricas directamente equivalentes ni bajo los mismos supuestos.

Tabla 9: Comparación de KPIs con Benchmarks Internacionales

Indicador	NERC CIP [8]	EPRI Best Practices [16]	Marco Propuesto
Disponibilidad EMS	≥ 99,90 %	≥ 99,95 %	≥ 99,99 %
MTTR	≤ 8 h	≤ 6 h	≤ 4 h
Frecuencia de pruebas de respaldo	Semestral	Trimestral	Mensual

5.7 Lecciones Aprendidas

El estudio muestra que la gestión efectiva de la obsolescencia tecnológica en sistemas de misión crítica trasciende el enfoque centrado exclusivamente en la renovación de hardware. La integración coordinada de componentes técnicos (C1–C4), de gestión (C5–C6) y organizacionales (C7) genera un efecto de resiliencia mayor comparado con el que podría lograrse mediante medidas aisladas. La aplicación del marco deja tres lecciones de valor para operadores de sistema en situaciones análogas:

1. **Sinergia entre mantenimiento y preparación para la migración:** Las acciones de optimización requeridas para sostener la plataforma actual constituyen simultáneamente actividades preparatorias para el nuevo EMS, como evidencia la doble función de la racionalización de señales y la estandarización de datos (Tabla VII). Esta dualidad incrementa la eficiencia de las inversiones técnicas y reduce fricciones durante la transición.
2. **El factor humano como multiplicador de resiliencia:** Sin capacitación continua y documentación actualizada, la redundancia de hardware pierde efectividad operativa. En este contexto, los simulacros trimestrales sin aviso previo surgen como una intervención de alta relación impacto-costo para fortalecer la preparación del personal y la capacidad de respuesta.
3. **La cuantificación como habilitador de gobernanza:** La formulación cuantitativa del riesgo mediante modelos de disponibilidad, evaluación de confiabilidad por Markov, riesgo dinámico acotado y evaluación económica por umbral permite traducir implicaciones técnicas en términos comprensibles para la toma de decisiones ejecutivas, facilitando la priorización presupuestaria y el respaldo institucional. La adopción de un análisis de umbral, en particular, demuestra que es posible sustentar decisiones de inversión incluso bajo restricciones de confidencialidad de los datos operativos.

6. CONCLUSIONES Y TRABAJO FUTURO

En el presente artículo se propone un marco integrado de continuidad operativa estructurado en siete componentes, apoyado en una formulación cuantitativa que incorpora disponibilidad, redundancia, evaluación de confiabilidad mediante cadenas de Markov, riesgo dinámico acotado y evaluación económica por análisis de umbral. A partir de su aplicación al caso de estudio, se desprenden las siguientes conclusiones.

6.1 Conclusiones

1. **La formulación de riesgo dinámico** formulada sobre la base de la tasa de riesgo (*hazard rate*), representa la evolución de la exposición durante la ventana de transición de forma físicamente consistente y, por construcción, acotada en el intervalo [0,1]. Aplicada a los cuatro modos de falla prioritarios, estima reducciones de exposición del orden de 29% a 55%, cerca del 46% para el modo de mayor exposición. Estos valores difieren entre modos y, por tanto, reflejan la dinámica del modelo.
2. **La evaluación de confiabilidad mediante la cadena de Markov de cuatro estados**, resuelta numéricamente con tasas calibradas a partir de datos operativos, arroja una disponibilidad efectiva del orden de 99,908% que reproduce la línea base observada (99,91%), lo que confiere anclaje empírico al modelo. Bajo el escenario con plan, la disponibilidad efectiva proyectada se aproxima al 99,98%, estrechando de forma sustancial la brecha respecto del objetivo de referencia de 99,99% (equivalente a 52,56 min/año), sin eliminarla por completo. La arquitectura de respaldo multinivel (Componente C4), complementada con la verificación funcional mensual del AGC de respaldo, constituye la base estructural de este resultado; la brecha residual es atribuible a fallas de causa común, errores humanos sistémicos y dependencias compartidas, que el marco mitiga, pero no suprime.
3. **La articulación del marco con referencias internacionales** como NERC CIP, NIST CSF, IEC 62443, IEEE 1686 e ISO 22301 proporciona una base conceptual consistente para la gestión de infraestructura crítica durante ventanas prolongadas de transición tecnológica. Su aplicación al contexto de Operadores de Sistemas Eléctricos presenta el potencial del enfoque para

adaptarse a restricciones técnicas, presupuestarias e institucionales propias de los operadores de sistemas eléctricos en economías emergentes.

4. **Las acciones de optimización ejecutadas sobre la plataforma actual** incluyendo racionalización de señales de historización, estandarización y optimización de datos y racionalización de alarmas, generan un doble beneficio, al contribuir simultáneamente a la sostenibilidad operativa de corto plazo y a la preparación de la migración hacia el nuevo EMS. Como se evidencia en la atribución de actividades a componentes (Sección 5.4), esta convergencia reduce la incertidumbre y mejora la preparación para el proceso de transición.
5. **La evaluación económica por análisis de umbral** establece que el plan de continuidad es costo-efectivo siempre que la probabilidad de propagación combinada con la fracción de carga en riesgo supere un umbral del orden de 1% a 3%, condición corroborada por los registros operativos internos sin necesidad de divulgar datos confidenciales de incidentes. Esta formulación sustituye la estimación puntual previa por una condición robusta frente a la incertidumbre y a las restricciones de confidencialidad, y constituye una base de decisión defendible para la gobernanza del plan.
6. **La metodología propuesta** se está aplicando al EMS del operador de sistema bajo estudio y es transferible a otros sistemas críticos del sector eléctrico, incluidos los de empresas de distribución, generación y transmisión.

6.2 Recomendaciones

1. **Soporte extendido con el proveedor del software**: Mantener contratos que incluyan atención remota permanente con ingenieros especialistas, atención presencial de emergencia en un plazo máximo de 48 horas y acceso a la base de conocimiento técnico, con el fin de reducir el MTTR ante incidentes complejos que requieran diagnóstico especializado.
2. **Equipo formal de gestión de continuidad del EMS:** Establecer una estructura multifuncional con disponibilidad permanente mediante turnos rotativos, protocolos claros de escalamiento y reuniones mensuales de seguimiento, como medida de alta relación impacto-esfuerzo para mejorar la velocidad y coordinación de la respuesta ante incidentes.
3. **Institucionalización de pruebas periódicas:** Realizar pruebas mensuales obligatorias de todos los sistemas de respaldo incluyendo el SCADA alternativo y el AGC de respaldo implementado en la central designada, complementadas con simulacros trimestrales sin aviso previo que involucren al personal de turno completo.
4. **Evaluación formal de aceleración de la implementación del nuevo EMS**: Desarrollar un análisis costo-beneficio dirigido a la alta dirección, orientado a valorar alternativas que reduzcan el período de exposición al riesgo operacional, considerando la posibilidad de adelantar componentes de infraestructura o software parcialmente independientes del sistema definitivo.

6.3 Trabajo Futuro

Las líneas de investigación prioritarias incluyen:

1. Extensión del marco a operadores multisistema con EMS regionales interconectados, incorporando el acoplamiento de riesgos entre centros de control vecinos.
2. Desarrollo de un gemelo digital (digital twin) del EMS para ejecutar simulaciones predictivas de degradación y validación anticipada de parches de mantenimiento [28], [29].
3. Profundización del enfoque de confiabilidad basada en la condición (CBM), integrando el monitoreo continuo de los indicadores operativos con la calibración dinámica de los parámetros del modelo de riesgo y la planificación de intervenciones según el estado real del equipo, en convergencia con el gemelo digital de la línea anterior.
4. Integración de técnicas de aprendizaje automático para la detección temprana de anomalías en los KPIs operacionales, mediante modelos de regresión y clasificación sobre las series temporales históricas [30], [31].
5. Calibración empírica de los parámetros $\lambda 0$, α y de las tasas de transición de Markov, así como del modelo de riesgo dinámico (ecuaciones (7)–(11)), mediante datos operacionales longitudinales multianuales de múltiples operadores.
6. Determinación del factor de propagación p_{prop} probabilidad de pérdida de suministro atribuible a la indisponibilidad del EMS pese a los respaldos para el sistema bajo estudio, a partir del análisis de registros operativos, con el fin de afinar la evaluación económica por umbral.
7. Aplicación del marco propuesto a otras infraestructuras de misión crítica del sector eléctrico, incluyendo sistemas de gestión de distribución (ADMS, Advanced Distribution Management System), de generación (GMS, Generation Management System) y de automatización de subestaciones [32].

7. AGRADECIMIENTOS

Los autores agradecen al Operador Nacional de Electricidad CENACE del Ecuador por el soporte institucional y el acceso brindando al entorno de desarrollo del EMS que permitió validar la metodología propuesta. Las licencias del EMS utilizadas en dicho

entorno son de propiedad de CENACE. Asimismo, los autores declaran que en la preparación de este artículo se empleó una herramienta de inteligencia artificial generativa como apoyo en tareas de redacción y revisión bibliográfica. Los autores verificaron y validaron el contenido resultante y asumen plena responsabilidad por el artículo elaborado. Todo el contenido técnico, la formulación matemática, el diseño del marco, la obtención de los resultados y las conclusiones son responsabilidad exclusiva de los autores.

8. REFERENCIAS BIBLIOGRÁFICAS

[1] A. J. Wood, B. F. Wollenberg, y G. B. Sheblé, Power Generation, Operation, and Control, 3ª ed. Hoboken, NJ, EE. UU.: Wiley-IEEE Press, 2013.

[2] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach. Boston, MA, EE. UU.: Kluwer Academic Publishers, 1999.

[3] Electric Power Research Institute, "EMS/SCADA System Lifecycle Management Guidelines," EPRI Technical Report 3002014929, Palo Alto, CA, EE. UU., 2019.

[4] CIGRE Working Group D2.34, "Operational Experience and Asset Management of EMS/SCADA Systems," CIGRE Technical Brochure 737, París, Francia, 2018.

[5] P. D. T. O'Connor y A. Kleyner, Practical Reliability Engineering, 5ª ed. Chichester, Reino Unido: Wiley, 2012.

[6] International Organization for Standardization, "Security and resilience — Business continuity management systems — Requirements," ISO 22301:2019, Ginebra, Suiza, 2019.

[7] International Organization for Standardization, "Risk management — Guidelines," ISO 31000:2018, Ginebra, Suiza, 2018.

[8] North American Electric Reliability Corporation, "CIP Reliability Standards — Critical Infrastructure Protection," Atlanta, GA, EE. UU., 2023. [En línea]. Disponible: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[9] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Gaithersburg, MD, EE. UU., feb. 2024. doi: 10.6028/NIST.CSWP.29.

[10] International Electrotechnical Commission, "Industrial communication networks — Network and system security," IEC 62443 Series, Ginebra, Suiza, 2018-2023.

[11] IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Std 1686-2013, Piscataway, NJ, EE. UU., 2014.

[12] R. Billinton y R. N. Allan, Reliability Evaluation of Power Systems, 2ª ed. Nueva York, NY, EE. UU.: Plenum Press, 1996.

[13] A. A. Chowdhury y D. O. Koval, Power Distribution System Reliability: Practical Methods and Applications. Hoboken, NJ, EE. UU.: Wiley-IEEE Press, 2009.

[14] M. Rausand y A. Høyland, System Reliability Theory: Models, Statistical Methods, and Applications, 2ª ed. Hoboken, NJ, EE. UU.: Wiley-Interscience, 2004.

[15] E. Bompard, P. Cuccia, M. Masera, y I. Fovino, "Cyber vulnerability in power systems operation and control," en Critical Infrastructure Protection, J. López, R. Setola, y S. Wolthusen, Eds. Berlín, Alemania: Springer, 2012, pp. 197-234.

[16] Electric Power Research Institute, "EMS/SCADA Life Extension and Technology Transition: Best Practices for Critical Infrastructure," EPRI Technical Report 3002019756, Palo Alto, CA, EE. UU., 2021.

[17] CIGRE Study Committee D2, "Information Systems and Telecommunication — EMS Platform Modernization Strategies," CIGRE Technical Brochure 825, París, Francia, 2021.

[18] A. K. S. Jardine, D. Lin, y D. Banjevic, "A review on machinery diagnostics and prognostics implementing condition-based maintenance," Mechanical Systems and Signal Processing, vol. 20, n.º 7, pp. 1483-1510, 2006. doi: 10.1016/j.ymssp.2005.09.012.

[19] International Organization for Standardization, "Condition monitoring and diagnostics of machines — General guidelines," ISO 17359:2018, Ginebra, Suiza.

[20] D. H. Stamatis, Failure Mode and Effect Analysis: FMEA from Theory to Execution, 2ª ed. Milwaukee, WI, EE. UU.: ASQ Quality Press, 2003.

[21] A. Apostolov, "End-to-end testing and FMEA of modern protection and control systems," IEEE Trans. Power Del., vol. 32, n.º 2, pp. 1026-1034, abr. 2017. doi: 10.1109/TPWRD.2016.2582820.

[22] T. Schröder y W. Kuckshinrichs, "Value of lost load: An efficient economic indicator for power supply security? A literature review," Frontiers Energy Research, vol. 3, art. 55, 2015. doi: 10.3389/fenrg.2015.00055.

[23] N. Schuerhoff, P. Linares, y M. Ortega-Vazquez, "Estimating the value of lost load in emerging economies: A South American case study," Energy Policy, vol. 156, art. 112392, 2021. doi: 10.1016/j.enpol.2021.112392.

[24] IEEE Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity, IEEE Std 762-2006, Piscataway, NJ, EE. UU., 2007. doi: 10.1109/IEEESTD.2007.335902.

[25] International Electrotechnical Commission, "Energy management system application program interface (EMS-API) — Common information model (CIM) base," IEC 61970-301:2020, Ginebra, Suiza, 2020.

[26] International Electrotechnical Commission, "Application integration at electric utilities — System interfaces for distribution management," IEC 61968 Series, Ginebra, Suiza, 2012-2022.

[27] Operador Nacional de Electricidad del Ecuador, "Plan de Continuidad Operativa del Sistema EMS," Reporte Técnico Interno, Unidad Administradora de Sistemas de Control, Quito, Ecuador, 2025.

[28] F. Arraño-Vargas y G. Konstantinou, "Modular design and real-time simulators toward power system digital twins implementation," IEEE Trans. Ind. Informat., vol. 19, n.º 1, pp. 52-61, ene. 2023. doi: 10.1109/TII.2022.3178713.

[29] Y. Ghahremani, W. Li, y V. Dinavahi, "Digital twin for power system protection and control: A review," IEEE Access, vol. 10, pp. 102148-102168, 2022. doi: 10.1109/ACCESS.2022.3207908.

[30] M. Cui, J. Wang, y M. Yue, "Machine learning-based anomaly detection for load forecasting under cyberattacks," IEEE Trans. Smart Grid, vol. 10, n.º 5, pp. 5724-5734, sep. 2019. doi: 10.1109/TSG.2018.2890809.

[31] Y. Zhang, T. Huang, y E. F. Bompard, "Big data analytics in smart grids: A review," Energy Informatics, vol. 1, art. 8, 2018. doi: 10.1186/s42162-018-0007-5.

[32] IEEE Standard for SCADA and Automation Systems, IEEE Std C37.1-2007, Piscataway, NJ, EE. UU., 2008.

Lourdes Farinango Cisneros.- Ingeniera Eléctrica y Magíster en Ingeniería Eléctrica por la Escuela Politécnica Nacional EPN, Quito, Ecuador. Magíster en Energías Renovables por la Escuela Superior Politécnica del Ejército, ESPE. Actualmente se desempeña como Especialista Nacional de Operación en Tiempo Real en el Operador Nacional de Electricidad CENACE. Sus áreas de interés incluyen la gestión de sistemas SCADA/EMS/GMS y OTS la Modelación de Sistemas Eléctricos y Energías Renovables, desarrollo de aplicaciones para sistemas EMS.

Gabriel P. Rivera Gárate.- Ingeniero Eléctrico y Magíster en Ingeniería Eléctrica por la Escuela Politécnica Nacional EPN, Quito, Ecuador. Cuenta con alrededor de tres décadas de experiencia en la gestión de sistemas SCADA/EMS en el Operador Nacional de Electricidad CENACE. Sus áreas de interés incluyen la gestión de sistemas EMS/GMS y OTS, desarrollo de aplicaciones para la operación del sistema eléctrico en tiempo real, desarrollos de aplicaciones para la gestión del estimador de estado, flujo de potencia, análisis de contingencias, control automático de generación y simuladores de entrenamiento para operadores.

Francisco de Lima Garmendia.- Recibió el título de Ingeniero Electricista por la Universidad Metropolitana, Caracas, Venezuela, y el grado de Magíster en Ingeniería Gerencial por la misma institución. Actualmente se desempeña como director de deBarr, Venezuela. Cuenta con más de tres décadas de experiencia en sistemas SCADA/EMS, ciberseguridad, integración de centros de control, auditoría técnica, migración de plataformas, puesta en servicio y capacitación especializada para operadores y empresas del sector eléctrico en América Latina, el Caribe, Norteamérica, Europa, Medio Oriente, África y Asia. Sus áreas de interés profesional incluyen sistemas EMS/SCADA, seguridad operacional, integración de bases de datos y aplicaciones, modernización tecnológica de centros de control, continuidad operativa y gestión de riesgos en infraestructuras críticas.