1 Objeto

Establecer las acciones de contingencia para responder, contener, recuperar y restablecer de manera controlada la infraestructura tecnológica y los componentes físicos y lógicos del centro de datos de la Corporación Autónoma Regional del Atlántico — CRA, ante eventos que afecten o puedan afectar su disponibilidad, integridad, seguridad, capacidad de procesamiento, almacenamiento, conectividad o condiciones de operación.

El presente PCE busca reducir la interrupción de los servicios tecnológicos que dependen de la infraestructura institucional, preservar la continuidad de los sistemas de información priorizados y orientar la coordinación de la Oficina Asesora de Ciencia, Tecnología e Innovación — CTeI con el personal técnico, proveedores, supervisores contractuales y demás responsables que intervengan en la recuperación.

2 Alcance

El presente PCE aplica a la infraestructura tecnológica física y lógica ubicada en el centro de datos y demás espacios tecnológicos bajo administración, supervisión, soporte o coordinación de la Oficina Asesora de CTeI de la CRA.

Comprende, según su existencia y aplicabilidad, servidores físicos, hosts de virtualización, máquinas virtuales, sistemas operativos, almacenamiento, discos, arreglos RAID, NAS, SAN, repositorios de respaldo, software base, racks, gabinetes, cableado estructurado asociado, switches CORE o de borde, firewall alojado localmente, UPS, tableros eléctricos asociados, climatización de sala, sensores, mecanismos de monitoreo, accesos administrativos, licencias, configuraciones, medios de respaldo y demás activos definidos en el inventario técnico oficial.

Este PCE cubre eventos de falla, degradación, indisponibilidad, daño físico, alteración de configuración, pérdida de capacidad, compromiso de seguridad o afectación ambiental que comprometan la infraestructura. No reemplaza los PCE específicos de aplicaciones, sistemas de información, conectividad externa, plataformas en nube o servicios administrados por proveedores; cuando la recuperación de estos dependa de infraestructura de centro de datos, se aplicará este PCE en coordinación con el protocolo específico correspondiente.

3 Escenarios de contingencia

Escenario	Ejemplos de eventos	Respuesta inicial esperada
Falla de energía	Corte eléctrico, falla de UPS, agotamiento de baterías, daño de fuente, fluctuación, sobrecarga o disparo de protecciones	Proteger personas y equipos, verificar energía, evaluar autonomía, apagar de forma controlada si se requiere y escalar soporte

Escenario	Ejemplos de eventos	Respuesta inicial esperada
Daño o falla de hardware	Falla de servidor, disco, RAID, memoria, fuente de poder, tarjeta de red, host, almacenamiento, switch de centro de datos o componente físico crítico	Aislar el activo afectado, verificar alertas y registros, identificar impacto, usar garantía, repuesto o soporte especializado
Falla de virtualización o software base	Host no disponible, hipervisor degradado, máquina virtual inaccesible, error de sistema operativo, servicio base detenido o configuración corrupta	Evaluar alcance, preservar registros, verificar dependencia y aplicar recuperación o restauración según protocolo técnico o escalar a soporte especializado
Falla de almacenamiento	Capacidad agotada, pérdida de volumen, corrupción, degradación de RAID, indisponibilidad de NAS/SAN o error de repositorio	Detener acciones que agraven la pérdida, verificar integridad, aislar si hay riesgo, escalar y recuperar según respaldo o redundancia disponible
Falla ambiental o física	Temperatura fuera de rango, falla de climatización, humedad, inundación, incendio, humo, polvo, acceso físico no autorizado o daño de rack y/o cableado	Proteger vida y seguridad física, activar protocolos institucionales aplicables, suspender operación si es necesario, preservar equipos y escalar
Falla de configuración	Configuración errónea, pérdida de parámetros, cambio no autorizado, error durante mantenimiento, actualización fallida o eliminación de configuraciones	Detener cambios, preservar evidencia, identificar última configuración válida, aplicar reversión o restauración controlada
Incidente de ciberseguridad	Malware, ransomware, acceso no autorizado, compromiso de cuenta privilegiada, explotación de vulnerabilidad o alteración maliciosa	Activar o consultar el PCE de ciberseguridad antes de restaurar; aislar, preservar evidencia, controlar accesos y recuperar solo tras validación
Falla de proveedor o soporte	Ausencia de soporte, incumplimiento de ANS, demora de garantía, falla de componente sin reemplazo o indisponibilidad de plataforma administrada	Escalar conforme al contrato o garantía; registrar la afectación, activar alternativas disponibles y elevar al supervisor contractual
Saturación o pérdida de capacidad	CPU, memoria, almacenamiento, red o recursos de virtualización insuficientes; crecimiento no previsto	Identificar servicios afectados, priorizar recursos, reducir carga no esencial, aplicar ajustes disponibles y registrar necesidad de mejora

4 Dependencias

Categoría	Dependencias que deben verificarse
Recursos físicos	Sede habilitada, acceso físico autorizado, racks, energía regulada, UPS, cableado, climatización, iluminación, seguridad física, herramientas y repuestos disponibles
Cómputo y virtualización	Servidores físicos, hosts, hipervisor, imágenes de instalación, máquinas virtuales, sistemas operativos, drivers, firmware, almacenamiento y capacidad disponible
Almacenamiento y respaldo	Volúmenes, arreglos RAID, NAS/SAN, repositorios, medios de respaldo, software de copias, configuraciones exportadas, procedimientos de restauración y última copia válida
Red interna	Switches CORE o borde, interfaces de red, VLAN, direccionamiento, DNS interno, DHCP cuando aplique, rutas, firewall, reglas y cableado
Seguridad	Antivirus, firewall, registros de eventos, control de acceso físico, cuentas privilegiadas, doble custodia cuando aplique, certificados, mecanismos de cifrado y respaldo seguro
Accesos administrativos	Cuentas privilegiadas vigentes, mecanismos de custodia, MFA cuando aplique, acceso a consolas físicas o remotas, acceso a hipervisores, sistemas operativos, dispositivos de red y herramientas de respaldo
Proveedores	Contactos de soporte, contratos, garantías, ANS, horas de atención, canales de escalamiento, licencias, manuales, niveles de soporte de fabricante y responsables de supervisión
Información técnica	Inventario actualizado, diagramas de infraestructura, configuraciones de red, licencias, manuales, contratos, bitácoras de mantenimiento, registros de cambio y PCE aplicables
Validación funcional	Responsable o enlace del sistema afectado, cuando se requiera comprobar que la recuperación de infraestructura permite reanudar funciones esenciales

5 Activación

Este PCE se activará cuando se presente o se identifique una condición que afecte o pueda afectar de manera significativa la infraestructura tecnológica del centro de datos, la disponibilidad de servicios transversales o la capacidad de operación de uno o varios sistemas de información, y cuya atención requiera coordinación extraordinaria, recuperación técnica, escalamiento a proveedores, uso de respaldos, reparación especializada, acciones de seguridad o comunicación a responsables institucionales.

La activación podrá ser solicitada por el personal técnico, la mesa de ayuda, el proveedor de soporte, el responsable de seguridad de la información o cualquier funcionario que detecte el evento. El Profesional Especializado grado 20 de la Oficina Asesora de CTeI realizará la valoración inicial y coordinará la respuesta, informando al Jefe de la Oficina Asesora de CTeI cuando el evento sea crítico, afecte

múltiples servicios, implique riesgo de seguridad, supere la capacidad de atención ordinaria o requiera decisiones institucionales.

Cuando el evento corresponda a una incidencia de atención ordinaria, se gestionará mediante el procedimiento de Soporte Técnico y el registro en KAÍA. Si el impacto aumenta o se evidencia afectación relevante de infraestructura, podrá escalarse a este PCE. El procedimiento de soporte exige registrar las solicitudes en la mesa de ayuda y escalar las que no pueden resolverse en el nivel inicial.

6 Roles y contactos

Rol	Responsabilidades
Jefe de la Oficina Asesora de CTeI	Autorizar o ratificar decisiones críticas; gestionar escalamiento institucional; orientar comunicaciones de alto impacto; autorizar, cuando corresponda, acciones que afecten de forma significativa la operación.
Profesional Especializado Grado 20 de CTeI	Coordinar la activación del PCE; valorar impacto; definir prioridad técnica; verificar dependencias; coordinar personal, proveedores y supervisión; mantener trazabilidad; validar recuperación técnica y presentar informe de cierre. Orientar o ejecutar acciones de contención, preservación de evidencia, análisis de compromiso y autorización técnica de recuperación segura cuando aplique.
Personal técnico de apoyo de CTeI	Detectar, registrar, diagnosticar, contener, recuperar, documentar y escalar conforme a sus funciones y a las instrucciones del coordinador técnico.
Proveedor de infraestructura o soporte especializado	Entregar y aplicar el protocolo técnico específico del activo bajo su responsabilidad; suministrar soporte, repuestos, garantía, configuraciones, respaldos, diagnósticos, evidencias y recomendaciones dentro del alcance contractual.
Supervisor contractual	Exigir la atención del proveedor, verificar los compromisos contractuales, documentar incumplimientos y gestionar acciones derivadas cuando aplique.
Profesional Universitario grado 8 (Mesa de ayuda)	Registrar el evento, asignar y escalar tickets, mantener trazabilidad, apoyar comunicaciones y consolidar tiempos de atención y cierre.

7 Contención y seguridad

Antes de iniciar acciones de recuperación, se deberá:

- Proteger la vida, integridad y seguridad física de las personas. Ante incendio, humo, inundación, riesgo eléctrico o daño físico, se aplicarán primero los protocolos institucionales de emergencias y seguridad física.
- Registrar el evento en Kaía y conservar información básica: fecha, hora, activo afectado, síntomas, personal interviniente, acciones iniciales y evidencia disponible.

- Aislar el componente afectado cuando exista riesgo de propagación de falla, daño eléctrico, sobrecalentamiento, corrupción, acceso no autorizado o incidente de ciberseguridad.
- Suspender cambios, actualizaciones, reinicios no controlados, formateos, borrados o restauraciones que puedan destruir evidencia, agravar la falla o afectar otros servicios.
- Verificar si el evento puede estar relacionado con malware, ransomware, uso indebido de privilegios, cambio no autorizado o compromiso de credenciales. Cuando exista sospecha razonable, debe activarse o consultarse el PCE de Ciberseguridad e Incidente Tecnológico Grave antes de reconectar, restaurar o poner en producción el activo afectado.
- Verificar el estado de cuentas privilegiadas, acceso a consolas y mecanismos de custodia necesarios para la recuperación, sin registrar contraseñas, tokens, llaves privadas ni secretos dentro del PCE o del ticket ordinario.
- Aplicar el procedimiento de gestión de cambios cuando la recuperación implique modificaciones permanentes de configuración, sustitución de infraestructura, cambio de arquitectura o ajuste de controles de seguridad. La política institucional exige que los cambios sean formalmente documentados y que no reduzcan la seguridad existente.

8 Recuperación técnica

La recuperación técnica se realizará con base en el diagnóstico, la criticidad del servicio afectado, la disponibilidad de recursos, los protocolos técnicos del proveedor, el inventario institucional y las condiciones de seguridad verificadas.

La secuencia técnica mínima será:

- Confirmar el activo afectado, su función, servicios dependientes, criticidad, estado de garantía, proveedor y soporte disponible.
- Revisar registros de monitoreo, eventos, mantenimiento, cambios recientes, alertas de UPS, almacenamiento, virtualización, temperatura, red y seguridad, según corresponda.
- Determinar si la falla se puede resolver mediante corrección controlada, reversión de cambio, reemplazo de componente, recuperación de configuración, restauración de imagen, recuperación de máquina virtual, reparación de almacenamiento o intervención del proveedor.
- Verificar que existan accesos privilegiados autorizados, herramientas, licencias, medios de respaldo, recursos de cómputo, almacenamiento y conectividad necesarios para la intervención.
- Ejecutar el protocolo específico del fabricante, proveedor o responsable técnico para el activo afectado. Cuando el activo esté bajo soporte externo, el proveedor deberá entregar y aplicar el procedimiento detallado de recuperación conforme a contrato, garantía, manuales y condiciones reales de infraestructura.
- Recuperar primero los componentes habilitadores transversales necesarios para restablecer otros servicios, tales como energía, almacenamiento, hosts de virtualización, red interna, DNS, autenticación o herramientas de respaldo, según el análisis del evento.
- Registrar toda acción ejecutada, incluyendo hora, responsable, decisión, configuración

restaurada, componente reemplazado, respaldo utilizado, resultado y condición pendiente.

- Si la recuperación técnica no es viable con recursos disponibles, se deberá mantener el servicio en condición controlada o fuera de operación, informar la limitación, activar el escalamiento contractual o institucional y registrar la brecha para tratamiento posterior.

9 Recuperación de información

La recuperación de información se realizará cuando el evento haya afectado, pueda haber afectado o requiera reconstruir datos, configuraciones, máquinas virtuales, imágenes de servidores, bases de datos, archivos institucionales, repositorios, registros de auditoría o cualquier otro activo de información asociado a la infraestructura.

La restauración solo se iniciará después de verificar que la causa del evento ha sido contenida o que existen controles suficientes para evitar que la información recuperada sea nuevamente afectada. En incidentes de ciberseguridad, la restauración deberá coordinarse con el PCE de Ciberseguridad e Incidente Tecnológico Grave.

La recuperación de información debe considerar:

- Identificación de la información, configuración o componente que requiere restauración.
- Confirmación del último respaldo, réplica, imagen o exportación disponible y su fecha.
- Verificación de la integridad, legibilidad, completitud y pertinencia del medio de recuperación.
- Definición del punto de recuperación alcanzable y la posible pérdida de información.
- Restauración en ambiente controlado cuando sea técnicamente posible.
- Validación de archivos, bases de datos, configuraciones, registros o máquinas virtuales restauradas.
- Documentación del respaldo utilizado, fecha, resultado, información no recuperable y acciones requeridas.
- Escalamiento al proveedor cuando la restauración requiera licenciamiento, herramientas propietarias, claves, conocimiento especializado o acceso a plataformas externas.

Las copias de configuraciones de infraestructura —por ejemplo, firewall, switches, plataformas de monitoreo, almacenamiento o virtualización— deben tratarse como información crítica de recuperación.

10 Infraestructura y conectividad

La recuperación de infraestructura debe verificar y restablecer las condiciones mínimas de operación antes de declarar disponible un servicio:

Componente	Validaciones mínimas
Energía y UPS	Alimentación eléctrica estable, carga de UPS, autonomía disponible,

Componente	Validaciones mínimas
	baterías, alarmas, protecciones y condiciones de apagado controlado
Ambiente físico	Temperatura, climatización, humedad, ventilación, limpieza, racks, cableado, seguridad física y ausencia de condiciones que puedan generar daño
Servidores y virtualización	Estado de hardware, firmware, host, hipervisor, máquinas virtuales, recursos asignados, almacenamiento y servicios base
Almacenamiento	Estado de discos, RAID, volúmenes, capacidad libre, integridad, conectividad y acceso desde los hosts o servicios requeridos
Red interna	Interfaces, switches, puertos, VLAN, direccionamiento, rutas, DNS, DHCP, conectividad entre componentes y reglas internas
Seguridad perimetral y de red	Firewall, reglas, segmentación, VPN, registros, certificados, control de accesos y ausencia de indicadores de compromiso
Conectividad externa	Internet, enlaces, DNS público, direccionamiento, disponibilidad de proveedor y rutas de acceso cuando aplique
Servicios habilitadores	Autenticación, directorio, NTP, monitoreo, respaldo, licenciamiento, administración remota y herramientas de gestión
Configuraciones	Existencia de configuraciones respaldadas, versiones vigentes, control de cambios y validación de parámetros restaurados

Cuando la afectación principal sea de red, Internet, VPN, DNS, firewall, enlaces o comunicaciones, se deberá activar o aplicar complementariamente el PCE de Conectividad, Redes y Comunicaciones. Cuando existan indicios de ataque, acceso no autorizado o manipulación, se deberá aplicar el PCE de Ciberseguridad e Incidente Tecnológico Grave antes de restablecer completamente los servicios.

11 Validación

El servicio o componente intervenido solo se considerará recuperado cuando se verifique, según corresponda:

- Estabilidad de energía, UPS y condiciones ambientales.
- Disponibilidad y estado saludable de servidores, almacenamiento, virtualización y servicios base.
- Conectividad interna y externa requerida.
- Funcionamiento de controles de seguridad, monitoreo, registros y accesos autorizados.
- Integridad básica de configuraciones, máquinas virtuales, datos y repositorios restaurados.
- Operación de los sistemas o servicios dependientes prioritarios.
- Ausencia de alertas críticas no tratadas o de evidencia de compromiso activo.
- Confirmación técnica por el responsable funcional y, cuando aplique, validación por el responsable del sistema o proceso usuario.
- Registro de las restricciones temporales, servicios pendientes o acciones posteriores.

La validación no significa que el incidente esté completamente resuelto a nivel de causa raíz. Significa que el servicio puede regresar a operación controlada. La causa raíz, las debilidades y las acciones

permanentes deben continuar en seguimiento hasta su cierre.

12 Comunicaciones

Momento	Responsable	Destinatarios	Canal	Contenido mínimo
Detección	Usuario, personal técnico o mesa de ayuda	Profesional Especializado grado 20 de CTeI	KAÍA, teléfono o correo	Activo afectado, hora, síntomas, alcance inicial y datos de contacto
Activación	Profesional Especializado grado 20 de CTeI	Jefe de CTeI, técnicos, proveedor, supervisor y seguridad cuando aplique	Teléfono, correo institucional y ticket	Severidad, alcance, servicios potencialmente afectados, medidas iniciales y protocolo aplicable
Seguimiento	Profesional Especializado grado 20 de CTeI	Jefe de CTeI y responsables definidos	Correo, ticket o canal institucional autorizado	Estado, acciones realizadas, riesgos, restricciones, requerimientos y próxima actualización
Restablecimiento	Soporte	Jefe de CTeI, Profesional Especializado grado 20 de CTeI, mesa de ayuda, usuarios o responsables afectados	Correo y ticket	Alcance de recuperación, validaciones realizadas, restricciones y recomendaciones
Cierre	Profesional Especializado grado 20 de CTeI	Jefe de CTeI, supervisor, proveedor y responsables involucrados	Informe, ticket y correo	Duración, causa preliminar, evidencia, acciones, hallazgos y compromisos de mejora

13 Restricciones

Este PCE establece coordinación y acciones mínimas, pero su eficacia depende de condiciones que deben declararse de manera expresa:

- La recuperación está limitada por la capacidad instalada, inventario, licenciamiento, vigencia de garantías, disponibilidad de componentes, conectividad y soporte contratado.
- No se garantiza la recuperación inmediata de servicios cuando no exista redundancia, ambiente

alterno, respaldo válido, equipo de reemplazo o soporte especializado disponible.

- Los tiempos de recuperación son estimados mientras no existan ANS, RTO/RPO validados o pruebas que demuestren la capacidad efectiva.
- Los protocolos técnicos detallados de equipos, software base, sistemas propietarios, plataformas SaaS o servicios gestionados deben ser suministrados por los proveedores o fabricantes responsables.
- La recuperación puede requerir intervención de terceros, autorizaciones institucionales, ventanas de mantenimiento, recursos físicos o decisiones de seguridad.
- Ante indicios de ciberseguridad, la preservación de evidencia y la contención pueden prevalecer temporalmente sobre el restablecimiento inmediato.
- Las cuentas privilegiadas, contraseñas, llaves, tokens y secretos no se incluyen en este PCE; su custodia se gestiona mediante el registro institucional correspondiente y mecanismos de acceso restringido.
- Los servicios no inventariados, sin responsable técnico identificado o sin soporte vigente presentan una mayor incertidumbre de recuperación y deben ser tratados como brechas de gestión.

14 Pruebas y actualización

La Oficina Asesora de CTeI programará y realizará pruebas graduales del presente PCE, priorizando inicialmente la verificación documental, la revisión de contactos, inventario y respaldos de configuración, ejercicios de escritorio y pruebas técnicas controladas que no afecten la operación institucional.

Las pruebas de mayor impacto, tales como recuperación de hosts, restauración de máquinas virtuales, conmutación de almacenamiento o simulación de indisponibilidad del centro de datos, requerirán evaluación previa de riesgos, disponibilidad de ventana técnica, coordinación con proveedores y autorización del Jefe de la Oficina Asesora de CTeI.

Tipos mínimos de prueba:

Prueba	**Periodicidad orientativa**	**Evidencia**
Revisión de inventario, contactos, garantías y soportes	Anual o ante cambios relevantes	Lista de verificación y actualización del registro
Verificación de respaldo de configuraciones	Semestral y antes de cambios mayores	Bitácora, exportación, informe de herramienta o soporte de proveedor
Ejercicio de escritorio	Anual	Acta, escenario, decisiones, hallazgos y compromisos
Prueba técnica controlada	Anual o según criticidad	Informe técnico, tiempos, evidencias y validación
Prueba posterior a incidente relevante	Por evento	Informe de recuperación y acciones de mejora

El PCE deberá actualizarse como mínimo una vez al año y también cuando ocurran cambios de infraestructura, inventario, proveedor, contrato, garantía, licenciamiento, configuración relevante, arquitectura, mecanismos de respaldo, responsables, contactos, incidentes críticos, pruebas fallidas, hallazgos de auditoría o modificaciones al Plan de Contingencia para Recuperación de los Sistemas de Información.

15 Evidencias

Evidencia	Fuente o ubicación de custodia	Responsable
Registro del incidente o solicitud	KAÍA y, cuando aplique, correo institucional de contingencia	Mesa de ayuda y Profesional Especializado
Inventario técnico de infraestructura	Inventario institucional, anexo técnico y repositorio autorizado	Oficina CTeI
Bitácoras de monitoreo	Herramientas de monitoreo, reportes y capturas controladas	Personal técnico o proveedor
Registros de mantenimiento preventivo y correctivo	Formatos de mantenimiento, tickets, informes y soportes de proveedor	Profesional Universitario grado 8 de CTeI
Respaldos de configuración	Repositorio seguro, herramienta de respaldo o soporte de proveedor	Personal técnico o proveedor
Registros de respaldo y restauración	Herramienta de copias, bitácoras, tickets e informes	Personal técnico o proveedor
Informes de proveedor, garantía o soporte especializado	Expediente contractual, mesa de ayuda o repositorio autorizado	Supervisor contractual
Registro de incidentes de seguridad	Registro institucional y referencias cruzadas con KAÍA	Profesional Universitario grado 8 de CTeI
Registro de cuentas privilegiadas	Repositorio restringido y mecanismo institucional de custodia	Oficina CTeI
Informes de prueba y recuperación	Expediente de contingencia y repositorio documental institucional	Profesional Especializado grado 20 de CTeI
Registros de cambio — RFC	Mecanismo institucional de gestión de cambios	Profesional Especializado grado 20 de CTeI
Informe de continuidad y acciones de mejora	Expediente documental del proceso Gestión de TI	Jefe de CTeI y Profesional Especializado grado 20 de CteI

Control de Cambios

Versión	Fecha	Descripción del Cambio
1	29/10/2026	Creación del documento