1 OBJETO

Establecer los lineamientos, responsabilidades y acciones generales para responder, recuperar y restablecer de manera controlada los sistemas de información, servicios tecnológicos y componentes de infraestructura que los soportan, ante eventos que afecten o puedan afectar su disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, desempeño o acceso, con el propósito de reducir la interrupción de los servicios institucionales y preservar la información de la Corporación Autónoma Regional del Atlántico — CRA.

2 ALCANCE

El presente Plan aplica a los sistemas de información, servicios tecnológicos, infraestructura física y lógica, redes y comunicaciones, mecanismos de seguridad, almacenamiento, servicios de respaldo, plataformas de virtualización, servicios en nube, bases de datos, cuentas técnicas, licenciamiento y proveedores tecnológicos que estén bajo administración, supervisión, soporte o coordinación de la Oficina Asesora de Ciencia, Tecnología e Innovación de la CRA.

Comprende la identificación, valoración, activación, coordinación, contención, recuperación, restablecimiento, validación, comunicación, prueba, seguimiento, actualización y mejora de las acciones de contingencia requeridas ante eventos que afecten la prestación de los servicios TIC.

El plan constituye el marco tecnológico para la recuperación de los sistemas de información; no sustituye los procedimientos manuales, las decisiones operativas ni las responsabilidades de continuidad de los procesos misionales, estratégicos, de apoyo o de evaluación de la CRA.

3 TERMINOS Y REFERENCIAS

Término	Definición propuesta
Activación del plan	Decisión de aplicar formalmente este plan ante un evento cuya severidad, impacto o duración supera la atención ordinaria de soporte técnico
Contingencia	Situación no prevista o no deseada que altera o amenaza la operación normal de un sistema, servicio tecnológico o componente de infraestructura y exige acciones de respuesta o recuperación
Disponibilidad	Capacidad de un sistema, servicio o activo tecnológico de estar operativo y accesible cuando sea requerido
Incidente de seguridad	Evento o conjunto de eventos que compromete o puede comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información o de los recursos tecnológicos
Plan específico de contingencia	Documento operativo, por sistema de información o por servicio tecnológico, que detalla escenarios, recursos, responsables, pasos técnicos, validaciones y mecanismos de recuperación aplicables

Término	Definición propuesta
Protocolo de recuperación	Secuencia técnica detallada para responder, contener, recuperar, validar y restablecer un sistema, servicio o componente ante un escenario definido
Recuperación	Acciones dirigidas a restaurar la operación, configuración, conectividad, seguridad, funcionalidad o información de un sistema o servicio afectado
Restablecimiento	Retorno controlado del sistema o servicio a condiciones estables de operación, previa verificación técnica y, cuando aplique, funcional
RTO	Tiempo objetivo de recuperación: tiempo máximo definido o estimado para restablecer un servicio o sistema después de una interrupción
RPO	Punto objetivo de recuperación: máxima pérdida de información aceptable, medida en tiempo, entre el último dato recuperable y el momento del evento
Servicio tecnológico	Conjunto de capacidades tecnológicas entregadas para soportar procesos, usuarios o sistemas institucionales; puede depender de aplicaciones, infraestructura, redes, proveedores y personas
Sistema de información	Conjunto organizado de personas, procedimientos, datos, software, infraestructura y comunicaciones que permite capturar, procesar, almacenar, consultar o intercambiar información institucional

4 ROLES Y RESPONSABILIDADES

Rol	Responsabilidades
Jefe de la Oficina Asesora de CTeI	Autorizar, validar y ratificar la activación del plan y la aplicación de los protocolos de contingencia; supervisar y evaluar las tareas desarrolladas por el Profesional Especializado de CTeI y por los demás funcionarios y contratistas intervinientes; aprobar de manera previa y expresa la aceptación técnica de los planes específicos, la clasificación de brechas y, en general, toda decisión de fondo relacionada con la formulación, activación, ejecución, validación y cierre de las contingencias; orientar el escalamiento institucional; y gestionar las decisiones que superen la capacidad operativa ordinaria de TIC
Profesional Especializado de CTeI	Administrar y ejecutar operativamente el plan marco y proponer sus actualizaciones para aprobación del Jefe de la Oficina Asesora de CTeI; identificar y valorar eventos, y coordinar la aplicación de contingencias bajo la supervisión y autorización del Jefe de la Oficina; solicitar, revisar y articular los planes específicos de proveedores; verificar evidencias y consolidar informes, hallazgos y acciones de mejora, para conocimiento y decisión del Jefe de la Oficina; apoyar la contención, preservación de evidencias, análisis y recuperación cuando exista o se sospeche un incidente de seguridad. Proponer y mantener actualizados los criterios técnicos mínimos para los planes específicos; revisar su coherencia con el inventario, contratos, ANS, arquitectura y

Rol	Responsabilidades
	capacidades existentes; y presentar al Jefe de la Oficina Asesora de CTeI el concepto técnico y la recomendación correspondiente sobre la aceptación del plan específico o la necesidad de ajustes, la clasificación de brechas y la aplicabilidad de los procedimientos de recuperación verificada mediante pruebas o evidencias. La aceptación técnica de los planes específicos, la clasificación definitiva de brechas y, en general, toda decisión de fondo en esta materia son competencia privativa del Jefe de la Oficina Asesora de CTeI, quien podrá acoger, modificar o rechazar motivadamente la recomendación del Profesional Especializado. El Profesional Especializado de CTeI no podrá adoptar por sí mismo decisiones de fondo sobre la aceptación de planes específicos, la clasificación de brechas, la activación del plan ni la validación final de la recuperación.
Proveedor de sistemas, infraestructura, conectividad, nube, seguridad o soporte especializado	Elaborar, entregar, actualizar y ejecutar, cuando corresponda, el Plan Específico de Contingencia o Protocolo de Recuperación del sistema, servicio o componente bajo su responsabilidad, conforme a los requisitos mínimos definidos por la CRA, las condiciones efectivamente contratadas, la arquitectura e inventario tecnológico vigentes, los ANS aplicables y las recomendaciones del fabricante. El plan específico deberá identificar expresamente los recursos, licencias, accesos, respaldos, configuraciones, personal, dependencias, ventanas de intervención, tiempos estimados, limitaciones y prerrequisitos necesarios para su ejecución. Cualquier requisito que exceda el alcance contractual o la capacidad tecnológica disponible deberá reportarse como brecha técnica, sin presumirse como capacidad existente de la CRA
Supervisor del contrato	Verificar que el proveedor entregue, mantenga actualizado, pruebe y cumpla los planes específicos, protocolos, ANS, respaldos, medidas de recuperación y soportes exigibles contractualmente
Contratistas de apoyo de CTeI	Ejecutar actividades de diagnóstico, contención, recuperación, validación y documentación, conforme al alcance de sus funciones y al protocolo aplicable
Profesional Universitario Grado 8	Registrar el evento en KAÍA/GLPI, asignar, escalar, mantener trazabilidad y apoyar la comunicación de estado y cierre
Profesional responsable funcional del sistema	Informar la afectación funcional cuando corresponda y validar la recuperación desde la operación, cuando sea requerido
Usuarios	Reportar oportunamente fallas o comportamientos anómalos y atender las instrucciones de contingencia impartidas por la Oficina TIC

5 DESCRIPCIÓN

5.1 FORMULACIÓN Y VALIDACIÓN DE PLANES ESPECÍFICOS

Para cada sistema de información, servicio tecnológico o componente de infraestructura priorizado, deberá existir un Plan Específico de Contingencia o Protocolo de Recuperación. Dicho documento desarrollará el detalle técnico requerido para recuperar el activo o servicio ante los escenarios identificados.

Cuando el sistema, servicio o componente sea provisto, administrado, soportado o mantenido por un tercero, el proveedor deberá elaborar y mantener el plan específico, de conformidad con los requisitos técnicos mínimos establecidos en el presente Plan, los instrumentos contractuales, el inventario tecnológico, los ANS, las condiciones de operación y las capacidades realmente disponibles en la CRA.

El Profesional Especializado de CTeI revisará la consistencia técnica del plan específico y presentará su concepto y recomendación al Jefe de la Oficina Asesora de CTeI, a quien corresponde de manera privativa decidir y autorizar su aceptación. No se aceptarán procedimientos que dependan de recursos, configuraciones, licencias, infraestructura, personal, conectividad, respaldos, servicios en nube, credenciales, contratos o niveles de soporte que no se encuentren disponibles, contratados, documentados o formalmente previstos.

Cuando la recuperación requerida exceda las capacidades disponibles, el plan específico deberá identificar la brecha, el riesgo, el impacto, la alternativa temporal de operación, el responsable de su tratamiento y la recomendación técnica correspondiente. La identificación de una brecha no constituye por sí misma autorización de gasto ni compromiso de inversión.

5.1.1 Contenido mínimo obligatorio

El Plan Marco debe incluir una tabla de requisitos mínimos. El proveedor puede usar su propio formato, pero no puede omitir ninguno de estos componentes.

Componente exigido	Contenido mínimo verificable	Criterio de aceptación CRA
Identificación	Sistema, servicio, versión, proveedor, contrato u orden aplicable, responsable técnico y fecha de vigencia	Coincide con catálogo, inventario y contrato
Alcance	Activos, sedes, usuarios, integraciones, datos, componentes y servicios cubiertos	No deja por fuera dependencias esenciales
Escenarios	Fallas de hardware, software, red, conectividad, energía, seguridad, datos, proveedor, configuración o infraestructura, según aplique	Corresponden a riesgos y arquitectura real

Componente exigido	Contenido mínimo verificable	Criterio de aceptación CRA
Dependencias	Servidores, virtualización, almacenamiento, bases de datos, red, identidad, certificados, licencias, integraciones, respaldos y terceros	Verificables en inventario técnico
Prerrequisitos	Accesos, cuentas privilegiadas, herramientas, medios de respaldo, licencias, recursos físicos, conectividad, personal y ventanas de mantenimiento	Disponibles o registrados como brecha
Responsables	Ejecutor, escalamiento, soporte de segundo nivel, fabricante, supervisor y validación técnica	Roles y canales existentes
Activación	Eventos que disparan el uso del protocolo y severidad aplicable	Compatible con el Plan Marco
Contención	Acciones iniciales para limitar propagación, proteger información y preservar evidencia	Compatible con seguridad de la información
Recuperación	Pasos ordenados, reversibles cuando aplique, con puntos de decisión y condiciones de parada	Ejecutable sin conocimiento tácito no documentado
Seguridad	Preservación de evidencia, revisión de compromiso, control de accesos y recuperación segura	No restaura un entorno comprometido sin controles
Datos	Respaldo, ubicación, periodicidad, retención, último punto recuperable y validación de integridad, cuando aplique	Basado en evidencia real de respaldos
Comunicaciones	Contactos, canales, tiempos de aviso y escalamiento	Corresponde al directorio vigente
Validación	Pruebas técnicas, funcionalidad esencial, conectividad, acceso, integridad y criterios de retorno	Define qué significa “recuperado”
Tiempo de recuperación	Tiempo estimado, RTO objetivo o provisional, y supuestos	No contradice capacidad, ANS ni soportes
Restricciones y brechas	Recursos no disponibles, dependencias no cubiertas, riesgos residuales y contingencias manuales	Expresamente declaradas, no ocultas
Evidencias	Logs, tickets, capturas, reportes, actas, respaldo utilizado y resultados de prueba	Localizables y con responsable de custodia
Pruebas y revisión	Tipo de prueba, periodicidad, última prueba, resultado, hallazgos y fecha próxima	Prueba programable y sostenible

5.2 CRITERIOS DE ACTIVACIÓN

El presente Plan se activará cuando ocurra un evento que afecte o pueda afectar de manera significativa

la operación, disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, desempeño o acceso de uno o varios sistemas de información, servicios tecnológicos o componentes de infraestructura de la CRA, y cuya atención exceda el tratamiento ordinario previsto en el procedimiento de Soporte Técnico o requiera coordinación de recursos, proveedores, comunicaciones o mecanismos de recuperación especializados.

La activación del plan es una decisión privativa del Jefe de la Oficina Asesora de CTeI, quien podrá autorizarla a solicitud o recomendación del Profesional Especializado de CTeI. Una vez activado el plan por el Jefe de la Oficina, o bajo su autorización expresa, el Profesional Especializado de CTeI identificará el sistema, servicio o componente afectado y ejecutará, bajo la supervisión directa del Jefe de la Oficina, el plan específico de contingencia o protocolo de recuperación correspondiente. Cuando dicho sistema, servicio o componente se encuentre bajo responsabilidad de un proveedor, el protocolo será el entregado y mantenido por este, validado por el Jefe de la Oficina de CTeI, con el apoyo técnico del Profesional Especializado, y exigible a través de la supervisión contractual.

Si no existe protocolo específico o este resulta insuficiente para el evento, se aplicará la secuencia mínima de recuperación definida en el numeral 5.4, se escalará al proveedor o fabricante correspondiente y se registrará la elaboración, ajuste o complementación requerida como acción de mejora.

Se consideran criterios de activación, entre otros:

- Indisponibilidad no programada de un sistema de información o servicio tecnológico priorizado.
- Falla total o degradación severa de servidores, virtualización, almacenamiento, bases de datos, redes, conectividad, seguridad perimetral, correo, autenticación o servicios en nube.
- Pérdida, corrupción, borrado accidental, cifrado o inaccesibilidad de información institucional.
- Falla de procesos de respaldo, pérdida de medios de copia o imposibilidad de restaurar información requerida.
- Incidente de seguridad que requiera aislamiento, contención, recuperación, reconstrucción o restablecimiento controlado.
- Indisponibilidad o incumplimiento de un proveedor tecnológico que afecte el servicio.
- Evento eléctrico, físico, ambiental o de seguridad que afecte infraestructura tecnológica.

La decisión de activar debe basarse en el impacto, la duración estimada, los sistemas afectados, la existencia de alternativas y la necesidad de recuperar información o infraestructura. Todo evento debe registrarse en KAÍA/GLPI o, cuando esta herramienta no esté disponible, por correo institucional y registrarse posteriormente. El procedimiento de soporte técnico establece que las solicitudes recibidas deben quedar registradas en la mesa de ayuda.

5.3 CLASIFICACIÓN DE SEVERIDAD

Nivel	Criterio de clasificación	Protocolo o plan aplicable	Decisión y respuesta
Crítica	Interrupción total, compromiso grave de seguridad o afectación de infraestructura transversal, sistema crítico, información sensible o servicio de atención externa; no existe alternativa inmediata	Plan específico vigente del sistema o servicio; protocolo del proveedor; y, si no existe, secuencia mínima de este plan	Activación inmediata, escalamiento al jefe, proveedor, supervisor y seguridad; comunicación de estado hasta estabilización
Alta	Indisponibilidad o degradación severa de un sistema o servicio relevante; múltiples usuarios afectados; operación limitada o alternativa temporal insuficiente	Plan específico o protocolo técnico vigente; protocolo del proveedor cuando aplique	Activación coordinada, escalamiento técnico, verificación de recursos y seguimiento reforzado
Media	Afectación parcial, localizada o controlable con soporte ordinario, sin comprometer significativamente la operación institucional	Procedimiento de soporte técnico, manual técnico o protocolo de atención aplicable	Registro en mesa de ayuda, atención y análisis de recurrencia; escalar a contingencia si aumenta el impacto
Baja	Incidencia individual o de impacto reducido, sin riesgo relevante sobre información, operación o disponibilidad institucional	Procedimiento de soporte técnico	Atención, cierre y conservación de la trazabilidad en KAÍA

5.4 ESTRATEGIA DE RECUPERACIÓN

La estrategia de recuperación se definirá y aplicará de acuerdo con el tipo de evento, la severidad, el sistema o servicio afectado, la criticidad, la dependencia tecnológica, la información involucrada, los riesgos de seguridad, las condiciones de infraestructura, la disponibilidad de recursos, los compromisos de soporte y las capacidades efectivamente disponibles en la CRA o sus proveedores.

La recuperación podrá comprender, según corresponda, actividades de contención de seguridad; preservación de evidencia; reparación, reemplazo o reconfiguración de hardware; recuperación de servidores, virtualización, almacenamiento, bases de datos y aplicaciones; restauración de configuraciones; recuperación o redireccionamiento de conectividad y comunicaciones; gestión de identidad y accesos privilegiados; activación de soporte del proveedor; recuperación desde respaldos; utilización de recursos alternos; operación degradada o temporal; y validación del restablecimiento técnico y funcional.

Los criterios mínimos para seleccionar la estrategia son:

Criterio	Pregunta de decisión
Tipo y causa del evento	¿Se trata de falla de hardware, software, red, proveedor, energía, configuración, ciberseguridad, pérdida de datos o evento físico?
Alcance	¿Afecta un usuario, un sistema, múltiples servicios, una sede, infraestructura transversal o servicios externos?
Severidad y criticidad	¿Cuál es el impacto sobre la operación, la ciudadanía, los usuarios, la información y los servicios institucionales?
Seguridad	¿Es seguro restaurar, o primero se debe contener, investigar, cambiar credenciales, aislar activos o preservar evidencia?
Dependencias	¿Qué infraestructura, red, almacenamiento, identidad, licencia, certificado, servicio tercero o personal se requiere antes de recuperar?
Integridad y disponibilidad de información	¿Existe información afectada?, ¿hay respaldo válido?, ¿es posible verificar la integridad?, ¿cuál es el último punto recuperable?
Capacidad técnica disponible	¿Existen recursos locales, alternos, de nube, de reemplazo, de garantía o de proveedor para ejecutar la recuperación?
Obligaciones contractuales	¿Qué ANS, garantía, soporte, manuales, protocolos y responsabilidades son exigibles al proveedor?
Tiempo requerido	¿Cuál es el tiempo objetivo o estimado para recuperación y cuál es el tiempo real alcanzable?
Riesgo residual	¿La solución restablece plenamente el servicio o se requiere operación temporal, restricción de funcionalidades o acción posterior de mejora?

5.5 SECUENCIA DE RECUPERACIÓN

La siguiente secuencia constituye el mínimo obligatorio de coordinación, control y trazabilidad para la atención de eventos de contingencia. No reemplaza los planes específicos de contingencia, manuales técnicos, procedimientos de fabricante ni protocolos de recuperación entregados por los proveedores.

Para cada sistema, servicio o componente priorizado, la Oficina de CTeI deberá armonizar esta secuencia con el plan específico o protocolo técnico correspondiente, verificando que incluya los pasos de recuperación de hardware, software, infraestructura, conectividad, seguridad, datos y validación aplicables.

- Detectar el evento y registrar el caso en KAÍA o, si la plataforma está indisponible, en el medio alterno definido, para su registro posterior.
- Identificar el sistema, servicio, componente, sede, usuarios, proveedor y activos potencialmente afectados.
- Clasificar la severidad y recomendar al Jefe de la Oficina Asesora de CTeI si corresponde activar este plan, decisión que este último adoptará y autorizará.
- Informar al Jefe de la Oficina Asesora de CTeI y escalar a los responsables, proveedores, supervisores contractuales y seguridad de la información, según el caso.

- Consultar y aplicar el plan específico de contingencia, protocolo del proveedor, manual técnico o procedimiento de recuperación vigente.
- Contener el evento, proteger a las personas y preservar evidencia cuando exista sospecha de incidente de seguridad.
- Verificar dependencias, accesos privilegiados, licencias, respaldos, recursos alternos, soporte técnico, garantía y condiciones de recuperación.
- Ejecutar la recuperación conforme al protocolo específico y registrar las acciones realizadas, decisiones adoptadas, tiempos, responsables y evidencias.
- Verificar el restablecimiento técnico: infraestructura, conectividad, configuración, seguridad, accesos, integridad de componentes y funcionamiento esencial.
- Solicitar, cuando aplique, validación funcional del responsable del sistema o proceso usuario.
- Comunicar el estado de recuperación, restricciones conocidas, acciones pendientes y recomendaciones de uso.
- Proponer el cierre del incidente cuando se logre estabilidad operacional, se consoliden evidencias y se definan las acciones de mejora necesarias, cierre que requiere la verificación y autorización del Jefe de la Oficina Asesora de CTeI.
- Actualizar el plan específico, protocolo, registro de incidentes, inventario, riesgos, ANS, contrato o registro de cuentas privilegiadas, según los hallazgos.

5.6 COMUNICACIONES

Momento	Responsable	Destinatarios	Medio	Contenido mínimo
Detección	Quien detecta / Kaia	Profesional Universitario grado 8 de CTeI	Mesa de ayuda Kaia, teléfono o correo	Servicio afectado, hora, síntoma y usuarios impactados
Activación	Jefe de CTeI, con apoyo del Profesional Especializado grado 20 de CTeI	Jefe CTeI, Profesional Especializado grado 20 de CTeI, equipo técnico, proveedor y seguridad cuando aplique	Teléfono, correo y ticket	Severidad, alcance, medidas iniciales y responsables
Seguimiento	Profesional Especializado grado 20 de CTeI	Jefe CTeI	Correo, ticket o canal institucional	Estado, acciones, riesgos, requerimientos y siguiente actualización
Restablecimiento	Profesional Especializado grado 20 de CTeI	Jefe CTeI, Usuarios o responsables involucrados	Correo y ticket	Servicio restablecido, alcance, validaciones y recomendaciones

Momento	Responsable	Destinatarios	Medio	Contenido mínimo
Cierre	Profesional especializado CTeI	Jefe de CTeI, Profesional Universitario grado 8 de CTeI y responsables de los sistemas de información	Informe y ticket	Causa, duración, evidencias, hallazgos y acciones de mejora

5.7 PRUEBAS

Los planes específicos y protocolos de recuperación deberán ser probados de acuerdo con la criticidad del sistema o servicio, los compromisos contractuales, las ventanas operativas disponibles y las condiciones de seguridad. Cuando el proveedor sea responsable de un sistema, infraestructura o servicio, deberá participar en la prueba, entregar sus resultados y soportes, y ejecutar los ajustes derivados de los hallazgos dentro de las condiciones contractuales aplicables.

La Oficina de CTeI debe programar pruebas proporcionales y sostenibles:

Tipo de prueba	Propósito
Revisión documental	Confirmar vigencia de contactos, inventario, responsabilidades, protocolos y mecanismos de escalamiento
Ejercicio de mesa	Validar decisiones, clasificación, comunicaciones, activación y coordinación con proveedor
Prueba técnica controlada	Comprobar una restauración, recuperación de configuración, conmutación, restablecimiento de conectividad o procedimiento específico sin afectar la operación
Prueba de recuperación de sistema	Validar que el sistema, sus dependencias y sus funciones esenciales pueden recuperarse conforme al protocolo específico
Evento real	Tratar una contingencia real como fuente de evidencia, evaluación y mejora

5.8 ACTUALIZACIÓN Y MEJORA

El presente Plan y los planes específicos de contingencia o protocolos de recuperación deberán revisarse como mínimo una vez al año, así como después de incidentes críticos, pruebas, cambios significativos de infraestructura, software, conectividad, seguridad, proveedor, contrato, inventario, respaldo, cuentas privilegiadas o niveles de servicio.

Los hallazgos derivados de pruebas, incidentes, auditorías, incumplimientos de ANS, cambios o revisiones deberán documentarse, analizarse y tratarse mediante acciones de mejora, solicitudes de

cambio, ajustes operativos, requerimientos al proveedor, controles de seguridad o gestiones contractuales, según corresponda.

La Oficina TIC conservará la trazabilidad de las actualizaciones, resultados de prueba, decisiones, responsables y acciones de mejora.

6 REGISTROS

Registro	Finalidad	Responsable de generación o actualización	Frecuencia / evento
Plan específico de contingencia o protocolo de recuperación por sistema, servicio o componente	Instrucciones técnicas y operativas detalladas para contingencias particulares	Proveedor responsable; validación y custodia en CTeI	Según contrato, cambios, incidentes o prueba
Inventario de sistemas de información y recursos tecnológicos	Identificar activos, componentes, relaciones y responsables	Oficina de CTeI	Periódica y por cambio
Registro de incidentes y requerimientos de soporte	Trazabilidad operativa, escalamiento, tiempos y cierre	KAÍA	Por evento
Registros de respaldo y restauración	Evidenciar ejecución, éxito, fallas y pruebas de recuperación	Oficina de CTeI/ proveedor de copia de seguridad	Según esquema de respaldo y por prueba

7 Control de Cambios

Versión	Fecha	Descripción del Cambio
1	18/09/2026	Creación del documento