1 Objeto

Establecer las acciones de contingencia para detectar, clasificar, contener, investigar, erradicar, recuperar y restablecer de manera segura los sistemas de información, servicios tecnológicos, infraestructura, redes, comunicaciones y activos de información de la Corporación Autónoma Regional del Atlántico - CRA, ante incidentes de ciberseguridad o eventos tecnológicos graves que afecten o puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, desempeño o acceso a la información y a los recursos tecnológicos institucionales.

El presente PCE busca reducir la propagación e impacto de los incidentes, proteger la evidencia técnica, prevenir la reincidencia, orientar la coordinación de la Oficina Asesora de Ciencia, Tecnología e Innovación - CTeI con proveedores y responsables involucrados, y asegurar que el restablecimiento de los servicios se realice bajo condiciones verificadas de seguridad.

2 Alcance

El presente PCE aplica a los sistemas de información, aplicaciones, servidores, estaciones de trabajo, dispositivos móviles institucionales, equipos de red, firewall, WAF, servicios en nube, correo electrónico, bases de datos, repositorios documentales, herramientas de respaldo, servicios de autenticación, cuentas privilegiadas, registros de auditoría, servicios de telecomunicaciones y demás activos tecnológicos bajo administración, supervisión, soporte o coordinación de la Oficina Asesora de CTeI.

Comprende la detección, reporte, registro, clasificación, contención, preservación de evidencia, análisis técnico, erradicación, recuperación, validación, comunicación, cierre y mejora de incidentes de ciberseguridad o tecnológicos graves.

El PCE aplica tanto a eventos originados internamente como a los generados por terceros, proveedores, ataques externos, errores de configuración, fallas de actualización, uso indebido de privilegios, pérdida de activos, vulnerabilidades, malware o interrupciones de servicios con indicios de compromiso de seguridad.

No reemplaza las competencias de Control Interno Disciplinario, Jurídica, Gestión Humana, Comunicaciones, autoridades competentes ni los protocolos especializados de proveedores. Cuando la situación involucre responsabilidades de esas instancias, CTeI conservará la coordinación técnica y escalará conforme a las instrucciones del Jefe de la Oficina Asesora de CTeI y la normativa aplicable.

3 Escenarios de contingencia

Escenario	Ejemplos	Respuesta inicial esperada
Malware o ransomware	Cifrado de archivos, ejecución de código malicioso, propagación por red, mensajes	Aislar activos afectados, no reiniciar ni restaurar sin evaluación,

Escenario	Ejemplos	Respuesta inicial esperada
	de rescate, degradación masiva o comportamiento anómalo	preservar evidencia, escalar y activar recuperación segura
Compromiso de credenciales	Phishing, uso no autorizado de cuenta, inicio de sesión anómalo, pérdida de cuenta administrativa, filtración de contraseñas o MFA comprometido	Bloquear o suspender accesos, cambiar credenciales, revocar sesiones, revisar privilegios, preservar registros y evaluar alcance
Acceso no autorizado	Intentos o accesos exitosos sin autorización, escalamiento de privilegios, cuentas desconocidas, uso de cuentas genéricas o cambios no autorizados	Contener acceso, registrar evidencias, revisar trazabilidad, revocar privilegios y escalar según criticidad
Alteración o pérdida de información	Borrado, modificación indebida, corrupción, manipulación de documentos, bases de datos, configuraciones o archivos de auditoría	Preservar evidencia, detener propagación, determinar alcance, validar respaldos y recuperar de manera controlada
Exposición o fuga de información	Envío no autorizado, publicación accidental, acceso externo indebido, repositorio expuesto, configuración insegura o pérdida de medio	Restringir acceso, preservar evidencia, identificar datos y destinatarios, escalar a responsables institucionales y corregir exposición
Vulnerabilidad crítica	Vulnerabilidad activamente explotada, software obsoleto, fallo de seguridad descubierto, configuración débil, servicio expuesto o falta de parche	Evaluar exposición, aplicar mitigación temporal, restringir servicios, coordinar actualización y documentar riesgo residual
Ataque de red	DDoS, escaneo, fuerza bruta, tráfico anómalo, intento de intrusión, explotación de servicios expuestos o manipulación de DNS	Activar controles de red, bloquear o filtrar, escalar al proveedor, preservar logs y aplicar el PCE de Conectividad cuando aplique
Compromiso de infraestructura	Servidor, hipervisor, firewall, switch, WAF, almacenamiento o plataforma de respaldo comprometida	Aislar activo, proteger configuraciones y registros, evaluar afectación transversal, aplicar PCE de Infraestructura y recuperación controlada
Compromiso de aplicaciones web	Ataques a portal, SQL Injection, XSS, fuerza bruta, bots, DDoS, explotación de vulnerabilidades o alteración de sesión	Activar WAF, contener exposición, preservar registros, escalar al proveedor de aplicación y aplicar protocolo específico
Incidente asociado a proveedor	Acceso indebido de tercero, caída por error de proveedor, exposición en nube, incumplimiento de controles, soporte remoto inseguro o fuga desde plataforma externa	Suspender o limitar accesos, exigir respuesta y evidencia al proveedor, revisar obligaciones contractuales y escalar supervisión

Escenario	Ejemplos	Respuesta inicial esperada
Evento tecnológico grave	Indisponibilidad con indicios de ataque, alteración de configuración crítica, pérdida masiva de capacidad, daño simultáneo de múltiples activos o evento que exceda soporte ordinario	Activar coordinación de contingencia, evaluar seguridad antes de recuperar, escalar al Jefe de CTeI y aplicar PCE complementarios

4 Dependencias

Categoría	Dependencias que deben verificarse
Inventario y clasificación	Inventario de activos, sistemas críticos, usuarios, dueños funcionales, proveedores, clasificación de información y dependencias tecnológicas
Registros y monitoreo	Logs de servidores, aplicaciones, firewall, WAF, antivirus/EDR, correo, autenticación, red, bases de datos, nube, respaldos, monitoreo y auditoría
Seguridad perimetral	Firewall Fortigate FG 100F, WAF, reglas de acceso, VPN, segmentación, listas de bloqueo, certificados, DNS y controles de red disponibles
Herramientas de seguridad	Solución antivirus o EDR, consola de seguridad, FortiAnalyzer Cloud, mecanismos de análisis, alertas, escaneo de vulnerabilidades y herramientas de monitoreo
Accesos y privilegios	Registro de cuentas privilegiadas, custodios autorizados, MFA, cuentas de emergencia, acceso a consola, mecanismos de revocación y rotación de credenciales
Recuperación	Respaldos válidos, repositorios segregados, configuraciones exportadas, imágenes de servidores, procedimientos de restauración, licencias y recursos alternos
Personal y proveedores	Jefe CTeI, Profesional Especializado, personal técnico, proveedores de infraestructura, seguridad, WAF, conectividad, nube, aplicaciones, operadores y supervisores contractuales
Comunicaciones	KAÍA/GLPI, correo institucional, teléfonos y canales alternos; directorio actualizado de contactos y escalamiento
Información jurídica y administrativa	Contratos, ANS, garantías, obligaciones de seguridad, acuerdos de confidencialidad, procedimientos disciplinarios y lineamientos de tratamiento de datos personales
Evidencia digital	Repositorio de custodia, mecanismos de acceso restringido, sellado lógico, copias protegidas, registro de quién accede y criterios de conservación

5 Activación

Este PCE se activará cuando se detecte, reporte o exista sospecha razonable de un incidente de ciberseguridad o evento tecnológico grave que afecte o pueda afectar de manera significativa la información, los sistemas de información, la infraestructura, las comunicaciones, los accesos, los

servicios institucionales o la continuidad de la operación.

La activación podrá originarse en alertas de herramientas de seguridad o monitoreo, reportes de usuarios, hallazgos de auditoría, eventos de proveedores, registros de firewall, WAF, antivirus, correo, autenticación o infraestructura, incidentes registrados en KAÍA, notificaciones de terceros o análisis técnico de CTeI.

El Profesional Especializado realizará la clasificación inicial y coordinará las medidas de respuesta. Se informará de inmediato al Jefe de la Oficina Asesora de CTeI cuando el evento sea crítico, involucre información sensible o crítica, afecte múltiples sistemas o usuarios, genere indisponibilidad relevante, comprometa cuentas privilegiadas, suponga exposición externa, requiera activación de proveedores o pueda generar consecuencias institucionales, legales o reputacionales.

Si el evento corresponde a un incidente de menor impacto, se gestionará inicialmente por la mesa de ayuda y el procedimiento de soporte. Si aumenta su alcance, se confirma compromiso de seguridad o se requiere contención y recuperación coordinada, se activará el presente PCE.

6 Roles y contactos

Rol	Responsabilidades
Jefe de la Oficina Asesora de CTeI	Autorizar o ratificar decisiones críticas; definir escalamiento institucional; orientar comunicación de alto impacto; poner en conocimiento de instancias competentes cuando corresponda
Profesional Especializado	Coordinar la respuesta técnica; clasificar el incidente; ordenar o gestionar contención; articular proveedores; preservar trazabilidad; verificar recuperación; consolidar informe, hallazgos y acciones de mejora. Apoyar la valoración, contención, preservación de evidencia, evaluación de riesgos y definición de controles de seguridad requeridos.
Personal de apoyo técnico de CTeI	Detectar, registrar, apoyar diagnóstico, contener según instrucciones, conservar evidencias, ejecutar recuperación autorizada y documentar acciones
Proveedor de seguridad, infraestructura, WAF, nube, aplicación o soporte especializado	Ejecutar el protocolo técnico específico del servicio bajo su responsabilidad; apoyar análisis, contención, erradicación, restauración y entrega de evidencias; reportar actividades, hallazgos y recomendaciones
Supervisor contractual	Exigir intervención, evidencias, cumplimiento de ANS y obligaciones de seguridad; documentar incumplimientos y gestionar acciones contractuales cuando aplique
Mesa de ayuda	Registrar el incidente, asignar y escalar, conservar trazabilidad de comunicaciones y apoyar cierre del caso
Responsable funcional del sistema afectado	Confirmar afectación funcional, colaborar en la priorización y validar el restablecimiento cuando aplique

Rol	Responsabilidades
Usuarios, funcionarios y contratistas	Reportar oportunamente comportamientos sospechosos; no reiniciar, borrar, formatear o manipular un activo comprometido; seguir instrucciones de CTeI

7 Contención y seguridad

Ante cualquier incidente de seguridad, se deberán aplicar las siguientes reglas:

- Registrar el evento en KAÍA; si la herramienta está indisponible, registrar inicialmente por el canal alterno autorizado e incorporarlo posteriormente al registro oficial.
- Preservar la evidencia disponible: fecha, hora, alertas, capturas, registros, correos, direcciones de origen, archivos, cuentas, equipos, configuraciones, acciones observadas y personal interviniente.
- No reiniciar, apagar, formatear, borrar, restaurar, actualizar ni modificar el activo afectado sin valorar previamente el impacto sobre la evidencia, la propagación y la continuidad del servicio, salvo que exista riesgo inmediato para personas, infraestructura o expansión activa que exija aislamiento urgente.
- Aislar lógica o físicamente los activos, segmentos, cuentas, servicios, interfaces, VPN, sesiones o accesos comprometidos, procurando minimizar la propagación a otros sistemas.
- Suspender, bloquear, revocar o cambiar credenciales cuando exista sospecha de compromiso de cuentas, especialmente de cuentas privilegiadas; validar también las cuentas de proveedores con acceso remoto.
- Restringir temporalmente reglas de red, servicios expuestos, integraciones, cuentas, accesos remotos o componentes comprometidos cuando sea necesario para contener el evento.
- Mantener registros de toda acción de contención, con hora, responsable, justificación y resultado.
- Preservar copias de configuraciones, respaldos y registros de auditoría antes de realizar intervenciones que puedan modificarlos.
- Coordinar con proveedores únicamente por canales autorizados y limitar los privilegios otorgados al mínimo necesario y durante el tiempo estrictamente requerido.
- No restablecer un sistema, servicio, red o acceso hasta verificar que el vector de compromiso ha sido eliminado, mitigado o aceptado formalmente como riesgo residual.

8 Recuperación técnica

La recuperación técnica solo se iniciará después de las actividades mínimas de contención, preservación de evidencia y valoración de seguridad. La recuperación no debe convertirse en una reinstalación apresurada que borre rastros útiles o reincorpore activos aún comprometidos.
La secuencia mínima de recuperación será:

- Confirmar el activo, servicio, sistema, cuenta, red, información o componente afectado; identificar

su criticidad, dependencias y usuarios impactados.

- Determinar el tipo de incidente, posible vector de entrada, alcance técnico, evidencia disponible, servicios comprometidos y riesgo de propagación.
- Aplicar o solicitar el protocolo específico del proveedor, fabricante, aplicación, servicio de nube, WAF, firewall, antivirus o plataforma afectada.
- Erradicar o mitigar la causa identificada: eliminación de malware, bloqueo de indicadores, cierre de vulnerabilidad, actualización, cambio de contraseña, revocación de token, corrección de configuración, restricción de acceso, actualización de certificados o aislamiento de segmentos, según corresponda.
- Verificar accesos privilegiados, cuentas técnicas, integraciones, servicios remotos, reglas de firewall, credenciales de proveedor y configuraciones relacionadas con el evento.
- Recuperar el activo afectado mediante reconstrucción segura, instalación limpia, restauración de configuración validada, restauración desde respaldo limpio, reparación técnica, sustitución de componente o intervención de proveedor, según aplique.
- Aplicar actualizaciones, endurecimiento, controles de acceso, configuraciones seguras, segmentación, monitoreo y registros antes de reincorporar el activo a producción.
- Ejecutar pruebas técnicas controladas antes de reconectar el activo a la red institucional, habilitar accesos externos o restablecer la operación normal.
- Coordinar con el PCE de Infraestructura Tecnológica y Centro de Datos cuando sea necesario recuperar servidores, virtualización, almacenamiento, UPS, hardware o software base.
- Coordinar con el PCE de Conectividad, Redes y Comunicaciones cuando se requiera aislar o recuperar enlaces, VLAN, firewall, VPN, WAF, DNS, telefonía IP o comunicaciones institucionales.
- Registrar tiempos, responsables, decisiones, acciones, configuraciones aplicadas, recursos utilizados, evidencias y limitaciones.

9 Recuperación de información

La recuperación de información se realizará cuando el incidente haya afectado, pueda haber afectado o exija restaurar datos, archivos, bases de datos, configuraciones, registros de auditoría, correos, credenciales, certificados, imágenes de servidores, máquinas virtuales, repositorios o cualquier otro activo de información.

Ninguna información será restaurada desde respaldos o repositorios sin verificar, en la medida técnicamente posible, que el punto de recuperación seleccionado no esté comprometido por el mismo incidente y que el entorno de destino esté protegido contra una nueva afectación.

La recuperación de información debe comprender, según aplique:

- Identificación de información afectada, sistema de origen, propietario funcional, clasificación y alcance.
- Identificación del último respaldo, copia, réplica, versión, instantánea o registro confiable

disponible.

- Verificación de la integridad, legibilidad, completitud y vigencia del recurso de recuperación.
- Análisis de posible contaminación, cifrado, alteración, manipulación o compromiso del respaldo.
- Restauración en ambiente aislado o controlado, cuando técnicamente sea viable.
- Validación de archivos, bases de datos, documentos, configuraciones, registros y servicios asociados.
- Determinación de pérdida de información, período afectado y punto de recuperación alcanzado.
- Conservación de la evidencia de restauración y comunicación de limitaciones.
- Rotación de credenciales, certificados, tokens y secretos que hayan podido quedar expuestos, aun cuando se recuperen datos o sistemas.

10 Infraestructura y conectividad

Componente	Validaciones mínimas de seguridad
Servidores y virtualización	Estado de hardware, hipervisor, sistema operativo, parches, servicios habilitados, accesos administrativos, *hardening*, registros y ausencia de indicadores de compromiso
Almacenamiento y respaldos	Integridad, disponibilidad, permisos, versiones, separación del entorno afectado, evidencia de restauración y protección de repositorios
Red y segmentación	VLAN, rutas, ACL, firewall, DNS, VPN, reglas, puertos expuestos, tráfico anómalo, segmentación y aislamiento de activos comprometidos
Firewall y WAF	Políticas vigentes, reglas temporales, bloqueos, registros, certificados, protección contra ataques y ausencia de cambios no autorizados
Endpoints y estaciones	Estado de antivirus, parches, indicadores de infección, aislamiento, cuentas, servicios remotos y conectividad controlada
Cuentas y accesos	Usuarios, privilegios, MFA, credenciales de emergencia, sesiones activas, cuentas de proveedor, accesos remotos y registro de cuentas privilegiadas
Monitoreo y auditoría	Sincronización de hora, recepción de registros, alertas, logs de seguridad, retención, custodia y acceso restringido
Servicios externos y nube	Estado del proveedor, registros disponibles, controles aplicados, configuraciones, accesos, respaldos, contratos y ANS
Comunicaciones	Disponibilidad de canales seguros para coordinación, escalamiento con proveedor y notificación a responsables autorizados

11 Validación

Un activo, sistema, servicio o componente afectado por un incidente de ciberseguridad solo se considerará recuperado para retorno a operación cuando se verifique, según corresponda:

- Eliminación, contención o mitigación verificable del vector de ataque, vulnerabilidad, malware, acceso no autorizado o configuración insegura.

- Aplicación de actualizaciones, correcciones, parches, endurecimiento, segmentación, reglas de seguridad o controles compensatorios requeridos.
- Revocación, rotación o restablecimiento controlado de cuentas, contraseñas, tokens, certificados y accesos comprometidos.
- Integridad y disponibilidad de configuraciones, servicios, datos, respaldos y registros recuperados.
- Funcionamiento de controles de seguridad: antivirus, firewall, WAF, autenticación, MFA cuando aplique, registros, monitoreo y alertas.
- Ausencia de alertas críticas activas, tráfico anómalo persistente o indicadores conocidos de compromiso sin tratamiento.
- Pruebas de conectividad, funcionalidad esencial, acceso autorizado e integraciones requeridas.
- Validación técnica del Profesional Especializado responsable de Gestión de TI, con soporte del proveedor cuando aplique.
- Validación funcional por el responsable del sistema afectado, cuando la recuperación impacte procesos institucionales.
- Registro de restricciones, riesgos residuales, controles temporales y acciones pendientes.

12 Comunicaciones

Momento	Responsable	Destinatarios	Canal	Contenido mínimo
Reporte o detección	Usuario, técnico, proveedor o mesa de ayuda	Profesional Especializado / Universitario grado 8	KAÍA/GLPI, teléfono, correo o canal alterno autorizado	Activo afectado, hora, síntoma, alerta y datos del reportante
Activación	Profesional Especializado	Jefe CTeI, técnicos, proveedor, supervisor y seguridad según el caso	Teléfono, correo institucional y ticket	Severidad, alcance preliminar, medidas de contención y requerimientos
Escalamiento crítico	Jefe CTeI o delegado	Instancias institucionales competentes, según instrucciones	Canal institucional autorizado	Impacto, estado, acciones en curso y necesidad de decisión o apoyo
Seguimiento	Coordinador técnico	Jefe CTeI, equipo técnico y responsables definidos	Correo seguro, ticket o canal autorizado	Evolución, evidencias, servicios afectados, restricciones, riesgos y próximo reporte
Recuperación	Coordinador técnico	Jefe CTeI, mesa de ayuda, responsables funcionales y usuarios afectados	Correo y ticket	Servicios recuperados, alcance, validaciones, restricciones y recomendaciones

Momento	Responsable	Destinatarios	Canal	Contenido mínimo
Cierre	Profesional Especializado	Jefe CTeI, supervisor, proveedor y responsables involucrados	Informe, ticket y correo	Duración, causa preliminar, alcance, evidencias, decisiones, hallazgos y acciones de mejora

13 Restricciones

- La capacidad de detección, análisis, contención y recuperación depende de la disponibilidad efectiva de herramientas de seguridad, registros, respaldos, licencias, conectividad, proveedores, cuentas privilegiadas, personal técnico y soporte contratado.
- La CRA no debe prometer erradicación inmediata, recuperación total de datos o disponibilidad continua si no cuenta con evidencias de respaldo, monitoreo, soporte 24×7, recursos alternos o pruebas que demuestren esa capacidad.
- Algunos incidentes pueden requerir análisis especializado, apoyo de fabricante, proveedor de nube, operador de conectividad, firma de seguridad, autoridad competente o intervención institucional adicional.
- Las acciones de contención pueden ocasionar indisponibilidad temporal de usuarios, redes, sistemas, correo, VPN, servicios web o equipos; la contención prioriza evitar expansión y pérdida adicional.
- El PCE no sustituye protocolos de respuesta a incidentes de fabricantes, proveedores, plataformas SaaS, sistemas de información o servicios de seguridad administrada; estos deben ser exigidos, revisados y aplicados conforme a contratos y condiciones técnicas reales.
- La información necesaria para investigación puede estar incompleta si no existen registros suficientes, si los logs no se preservaron, si los activos no estaban sincronizados en tiempo o si el proveedor no entrega evidencias oportunamente.
- Las contraseñas, tokens, llaves privadas, códigos de recuperación y secretos no se incluyen en el PCE. Se administran a través del Registro de Cuentas y Claves Privilegiadas y mecanismos de custodia restringida.
- La determinación de responsabilidades disciplinarias, administrativas, contractuales, civiles o penales no corresponde a este PCE; este documento se limita a la respuesta y recuperación técnica.
- El PCE no reemplaza las obligaciones legales específicas sobre tratamiento de datos personales, notificación de incidentes o conservación de evidencia, cuando estas resulten aplicables.

14 Pruebas y actualización

La Oficina Asesora de CTeI realizará pruebas graduales del presente PCE, priorizando inicialmente ejercicios de escritorio, verificación de disponibilidad de contactos, revisión de registros, simulación de

notificación, bloqueo controlado de una cuenta no productiva, validación de mecanismos de aislamiento y pruebas de restauración segura en ambiente controlado.

Las pruebas que puedan afectar producción, servicios institucionales, redes, aplicaciones, correo, autenticación, firewall, WAF, datos o acceso de usuarios deberán programarse, evaluarse previamente, ejecutarse en ventana controlada y coordinarse con los proveedores responsables. Cuando el impacto potencial sea relevante, requerirán autorización del Jefe de la Oficina Asesora de CTeI.

Tipo de prueba	**Periodicidad orientativa**	**Evidencia**
Revisión de contactos, contratos, ANS, cuentas privilegiadas y protocolos de proveedor	Anual o ante cambio relevante	Lista de verificación y registro de actualización
Ejercicio de escritorio de ransomware, phishing o compromiso de cuenta	Anual	Acta, escenario, decisiones, tiempos de escalamiento y hallazgos
Verificación de registros, alertas y trazabilidad	Según herramienta	Reporte de monitoreo, eventos y evidencia de revisión
Prueba de aislamiento controlado	Anual o según criticidad	Bitácora de prueba, resultados, efectos y acciones
Prueba de restauración segura	Anual o junto con PCE de infraestructura	Informe técnico, respaldo utilizado, validaciones y hallazgos
Prueba de escalamiento con proveedor	Anual o según ANS	Registro de contacto, tiempos de respuesta y resultado
Evaluación posterior a incidente real	Por evento	Informe de incidente, lecciones aprendidas y acciones de mejora

El PCE deberá revisarse como mínimo una vez al año y cuando ocurran incidentes críticos, cambios de arquitectura, incorporación o retiro de servicios, cambios de proveedores, cambios de licencias o herramientas de seguridad, hallazgos de auditoría, modificaciones relevantes de configuraciones, pruebas fallidas, nuevas vulnerabilidades críticas o cambios en el Plan de Contingencia para Recuperación de los Sistemas de Información.

15 Evidencias

Evidencia	**Fuente o ubicación de custodia**	**Responsable**
Registro de incidente de seguridad	Registro institucional y referencia cruzada con KAÍA	Profesional Especializado
Ticket de atención, escalamiento y cierre	KAÍA o canal alterno autorizado para posterior registro	Profesional Universitario grado 8 y personal

Evidencia	Fuente o ubicación de custodia	Responsable
		técnico
Registros de auditoría y eventos	Firewall, WAF, FortiAnalyzer Cloud, antivirus, servidores, aplicaciones, correo, red, nube y herramientas de monitoreo	CTeI y proveedores según aplique
Evidencia técnica preservada	Repositorio restringido, expediente controlado o mecanismo de custodia definido	Profesional Especializado
Inventario de activos y dependencias	Inventario institucional, anexo técnico y repositorio autorizado	Oficina CTeI
Registro de cuentas y claves privilegiadas	Repositorio restringido y mecanismo de custodia institucional	Oficina CTeI
Informes de proveedor o fabricante	Expediente contractual, repositorio técnico y ticket asociado	Supervisor contractual y proveedor
Registros de cambios o RFC	Mecanismo institucional de gestión de cambios	Profesional Especializado
Registros de respaldo y restauración	Herramienta de copias, informes, bitácoras y tickets	CTeI y proveedor
Informes de análisis, contención y recuperación	Expediente de contingencia e incidentes de seguridad	Profesional Especializado
Evidencias de pruebas	Actas, bitácoras, capturas, resultados, tiempos y hallazgos	Oficina CTeI y proveedor
Informes de continuidad y acciones de mejora	Expediente del proceso Gestión de TI	Profesional Especializado y Jefe de CTeI
Comunicaciones institucionales autorizadas	Correo institucional, radicados o repositorio controlado	Jefe CTeI y responsable técnico

16 Control de Cambios

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