1 Objeto

Establecer las acciones de contingencia para responder, contener, recuperar y restablecer de manera controlada los servicios de conectividad, redes, comunicaciones y seguridad de red de la Corporación Autónoma Regional del Atlántico - CRA, ante eventos que afecten o puedan afectar la disponibilidad, estabilidad, seguridad, capacidad de comunicación o acceso a los servicios tecnológicos institucionales.

El presente PCE busca reducir la interrupción de la conectividad institucional, preservar la comunicación entre las sedes, asegurar el acceso a los sistemas de información y servicios tecnológicos priorizados, y orientar la coordinación de la Oficina Asesora de Ciencia, Tecnología e Innovación - CTeI con el personal técnico, proveedores de conectividad, contratistas, supervisores y demás responsables que intervengan en la recuperación.

2 Alcance

El presente PCE aplica a la infraestructura y servicios de conectividad, redes y comunicaciones bajo administración, supervisión, soporte o coordinación de la Oficina Asesora de CTeI de la CRA.

Comprende, según su existencia y aplicabilidad, los enlaces de Internet principal y de respaldo, equipos de borde, firewall, routers, switches, red LAN, LAN Extendida entre las sedes 1 y 2, red inalámbrica — WLAN, segmentación mediante VLAN, enlaces troncales, direccionamiento IP, enrutamiento, políticas de comunicación entre segmentos, DNS, DHCP, VPN, reglas de seguridad de red, plataformas de monitoreo, WAF, telefonía IP, troncal SIP, extensiones IP, mecanismos de calidad de servicio — QoS, configuraciones, licencias, respaldos de configuración, cuentas administrativas y servicios contratados a proveedores de telecomunicaciones.

Comprende la detección, clasificación, activación, diagnóstico, contención, escalamiento, recuperación, validación, comunicación, prueba, actualización y mejora de las acciones requeridas ante incidentes que comprometan los servicios de red y comunicaciones.

Este PCE no reemplaza los protocolos del operador de Internet, proveedor de telecomunicaciones, fabricante de equipos, proveedor de WAF, proveedor de telefonía IP o contratista especializado. Tales protocolos deberán ser aplicados y armonizados con este PCE cuando la recuperación dependa de servicios, equipos o configuraciones bajo su responsabilidad.

3 Escenarios de contingencia

Escenario	Ejemplos de eventos	Respuesta inicial esperada
Indisponibilidad de Internet principal	Caída total o degradación prolongada, pérdida de enlace, falla del operador, latencia crítica, pérdida de	Verificar estado del enlace, activar monitoreo, confirmar afectación, validar operación del canal de

Escenario	Ejemplos de eventos	Respuesta inicial esperada
	direccionamiento o interrupción del medio físico	respaldo y escalar al operador
Falla de canal de Internet de respaldo	Enlace alterno no disponible, fallo de configuración, incapacidad de conmutación o degradación del servicio de respaldo	Verificar parámetros, rutas, políticas de enrutamiento y estado del enlace; escalar al proveedor y registrar pérdida de resiliencia
Falla de balanceo o *failover*	El tráfico no conmuta, ruta incorrecta, política de prioridad errada, bucle de enrutamiento o configuración no actualizada	Detener cambios no controlados, revisar configuración respaldada, validar salud de enlaces y aplicar reversión o ajuste autorizado
Falla de equipos de red	Switch, router, firewall, punto de acceso, módulo, fuente de poder, interfaz, puerto, transceptor o cableado dañado	Aislar el componente, verificar energía y alarmas, identificar impacto, aplicar garantía, reemplazo, respaldo de configuración o soporte especializado
Pérdida de conectividad entre sedes	Falla de LAN Extendida, VLAN, enlace troncal, enrutamiento, VPN, equipos intermedios o proveedor de telecomunicaciones	Identificar punto de interrupción, validar equipos de borde y segmentación, aplicar contingencia local y escalar proveedor
Falla de red LAN o WLAN	Segmento sin conectividad, usuarios sin acceso, SSID caído, saturación, interferencia, falla de switch o AP, problema de VLAN o DHCP	Determinar alcance, revisar conectividad física y lógica, aislar segmento si procede y restablecer con base en configuración aprobada
Indisponibilidad de DNS, DHCP o servicios de red	Equipos sin resolución de nombres, falta de asignación IP, pérdida de conectividad por parámetros incorrectos o falla de servicio base	Verificar disponibilidad de servicios, configuraciones, dependencias y redundancia disponible; recuperar o escalar
Falla de VPN o accesos remotos	Usuarios autorizados sin acceso, túnel caído, error de autenticación, certificado vencido, cambio de IP pública o falla de configuración	Verificar conectividad base, estado del firewall, autenticación, certificados y políticas; aplicar reversión o escalar
Falla de telefonía IP o troncal SIP	Extensiones sin registro, llamadas entrantes o salientes fallidas, audio unidireccional, pérdida de troncal, falla de PBX o QoS	Validar red, telefonía IP, troncal SIP, reglas de firewall, QoS y proveedor de telefonía; activar mecanismos alternos de comunicación
Falla del WAF o seguridad perimetral	Aplicación web inaccesible, bloqueo indebido, caída de WAF, reglas erróneas, certificado vencido o alteración de política	Verificar si existe riesgo de seguridad, contener cambios, aplicar configuración validada y escalar al proveedor

Escenario	Ejemplos de eventos	Respuesta inicial esperada
		correspondiente
Incidente de ciberseguridad de red	Ataque de denegación de servicio, escaneo, tráfico anómalo, intrusión, cambio no autorizado, compromiso de credenciales o propagación de malware	Activar o consultar el PCE de Ciberseguridad antes de restablecer rutas, reglas, VLAN o accesos
Cambio fallido	Actualización, mantenimiento, ajuste de ruta, cambio de firewall, VLAN, regla, firmware o configuración que genere indisponibilidad	Suspender despliegue, conservar evidencia, restaurar configuración previa y aplicar gestión de cambios

4 Dependencias

Categoría	Dependencias que deben verificarse
Conectividad externa	Enlace principal, canal de respaldo, operador de Internet, direccionamiento IP público, DNS público, medios físicos, equipos de demarcación y soporte del proveedor
Equipos de red	Firewall, routers, switches de núcleo, distribución o acceso, puntos de acceso, controladores WLAN, transceptores, módulos, interfaces, fuentes y cableado
Red lógica	Direccionamiento IP, VLAN, enlaces *trunk*, tablas de enrutamiento, rutas estáticas o dinámicas, NAT, ACL, políticas de firewall, QoS, DNS, DHCP y VPN
Seguridad	Reglas de seguridad, segmentación, WAF, registros, listas de bloqueo, certificados, autenticación, cuentas privilegiadas, MFA cuando aplique y monitoreo de amenazas
Infraestructura física	Energía regulada, UPS, racks, cableado estructurado, fibra óptica, patch panels, climatización de sala técnica y acceso físico autorizado
Servicios habilitadores	Directorio o autenticación, NTP, DNS, DHCP, monitoreo, correo, herramientas de administración remota, repositorio de configuraciones y licencias
Telefonía IP	PBX, servidor de telefonía, troncal SIP, extensiones, red LAN/LAN Extendida, QoS, firewall, reglas de voz, direccionamiento y proveedor de telefonía
Respaldos de configuración	Copias vigentes de firewall, routers, switches, VLAN, WAF, VPN, PBX, controladores inalámbricos, rutas, reglas y políticas
Accesos administrativos	Cuentas privilegiadas, acceso de consola, VPN administrativa, mecanismos de custodia, contactos de fabricante y procedimientos de emergencia
Proveedores y contratos	Contratos, ANS, garantías, contactos, horarios, canales de escalamiento, obligaciones de soporte y protocolos técnicos aplicables
Información técnica	Inventario, diagramas de red, topología lógica, topología física, direccionamiento, configuraciones aprobadas, historial de cambios y bitácoras

5 Activación

Este PCE se activará cuando se presente o se identifique un evento que afecte o pueda afectar significativamente la conectividad institucional, la comunicación entre sedes, el acceso a sistemas de información, la telefonía IP, la seguridad perimetral o los servicios de red transversales, y cuya atención exceda la gestión ordinaria de soporte técnico o requiera coordinación de recursos, proveedores, mecanismos de failover, restauración de configuraciones, intervención especializada o comunicación a usuarios.

La activación podrá ser solicitada por personal técnico, mesa de ayuda, proveedor, responsable de seguridad de la información o cualquier funcionario que detecte el evento. El Profesional Especializado de CTeI realizará la valoración inicial, identificará el alcance y coordinará la respuesta. Informará al Jefe de la Oficina Asesora de CTeI cuando el evento sea crítico, afecte las dos sedes, involucre indisponibilidad simultánea de enlaces, afecte atención externa o telefonía institucional, implique un incidente de seguridad o requiera decisiones que superen la atención operativa ordinaria.

Cuando el evento corresponda a una falla individual, localizada o recuperable mediante soporte habitual, se gestionará inicialmente mediante el procedimiento de Soporte Técnico y se registrará en KAÍA. Si el impacto aumenta, involucra servicios transversales o se requiere recuperación coordinada, se escalará al presente PCE.

6 Roles y contactos

Rol	Responsabilidades
Jefe de la Oficina Asesora de CTeI	Autorizar o ratificar decisiones críticas; orientar comunicaciones institucionales de alto impacto; gestionar escalamiento cuando se requieran decisiones administrativas, contractuales o institucionales
Profesional Especializado grado 20 de CTeI	Coordinar la activación del PCE; valorar severidad y alcance; priorizar recuperación; verificar dependencias; coordinar técnicos, proveedores y supervisión; validar recuperación técnica y elaborar informe de cierre. Apoyar contención y análisis cuando exista o se sospeche ataque, acceso no autorizado, alteración de configuración, vulnerabilidad o compromiso de seguridad
Personal de apoyo técnico de CTeI	Detectar, registrar, diagnosticar, contener, ejecutar o acompañar acciones de recuperación, documentar cambios y escalar conforme al presente PCE
Proveedor de infraestructura de red y soporte especializado	Entregar y ejecutar los protocolos específicos de recuperación de equipos, configuraciones, LAN, WLAN, LAN Extendida, firewall, WAF, VPN, rutas, QoS y componentes bajo su responsabilidad; aportar evidencias, respaldos, diagnósticos y recomendaciones
Operador de conectividad o telecomunicaciones	Diagnosticar, atender y restablecer los enlaces, direccionamiento, troncal SIP u otros servicios contratados bajo su responsabilidad, conforme a las condiciones contractuales y ANS aplicables

Rol	Responsabilidades
Proveedor o soporte de telefonía IP	Atender fallas de PBX, troncal SIP, extensiones, configuración de voz, integración con red, QoS y demás componentes bajo su responsabilidad
Supervisor contractual	Verificar atención de proveedores, cumplimiento de ANS, obligaciones, garantías, entrega de evidencias y tratamiento de incumplimientos
Profesional Universitario grado 8	Registrar, clasificar, asignar, escalar y hacer seguimiento de tickets; apoyar la trazabilidad, comunicaciones y cierre
Responsable funcional afectado	Informar afectación operativa y validar, cuando aplique, que los servicios recuperados permiten continuar la operación

7 Contención y seguridad

Ante un evento de conectividad, red o comunicaciones, se deberán aplicar las siguientes acciones antes de realizar cambios de recuperación:

- Registrar el evento en KAÍA o, si esta plataforma está indisponible, en el canal alterno autorizado para posterior incorporación al registro oficial.
- Identificar el alcance: sedes, segmentos, servicios, usuarios, enlaces, equipos, configuraciones, direcciones, reglas, telefonía o aplicaciones afectadas.
- Verificar si el evento puede corresponder a un incidente de seguridad: tráfico anómalo, ataque de denegación de servicio, acceso indebido, modificación no autorizada, compromiso de cuenta privilegiada, infección, exfiltración o intento de intrusión.
- Cuando exista sospecha de ciberseguridad, activar o consultar el PCE de Ciberseguridad e Incidente Tecnológico Grave antes de revertir, restaurar o habilitar accesos, rutas, reglas, VLAN, VPN o equipos que puedan estar comprometidos.
- Suspender cambios no controlados y preservar la última configuración conocida como válida, los registros de eventos, capturas de monitoreo, bitácoras de firewall, datos del enlace y evidencia relevante.
- Aislar lógicamente segmentos, equipos, cuentas, interfaces, VPN o servicios afectados cuando sea necesario para contener propagación, acceso no autorizado o degradación del resto de la red.
- Verificar el estado de las cuentas administrativas, acceso a consola y mecanismos de custodia requeridos para intervenir, sin registrar contraseñas ni secretos en tickets de amplia visibilidad.
- Registrar todo cambio realizado durante la contingencia. Si genera una modificación permanente, debe formalizarse posteriormente mediante el mecanismo institucional de gestión de cambios o RFC, conservando la evidencia de la situación de emergencia.

8 Recuperación técnica

La recuperación técnica se realizará con base en el diagnóstico, el alcance de la afectación, la criticidad

de los servicios comprometidos, la disponibilidad de configuraciones respaldadas, los procedimientos específicos de proveedores y las condiciones de seguridad verificadas.

La secuencia mínima será:

- Confirmar el servicio, enlace, equipo, sede, segmento, configuración o plataforma de comunicaciones afectada y determinar los servicios dependientes.
- Verificar energía, estado físico, interfaces, alarmas, monitoreo, registros, enlaces, configuración vigente, cambios recientes y disponibilidad de soporte.
- Determinar la acción aplicable: conmutación a enlace de respaldo, corrección de ruta, reversión de cambio, sustitución de equipo, restauración de configuración, reinicio controlado, ajuste de VLAN, restablecimiento de VPN, reparación de cableado, atención del operador o escalamiento al fabricante.
- Validar disponibilidad de recursos: acceso administrativo autorizado, consola, respaldo de configuración, licenciamiento, equipo de reemplazo, garantía, conectividad alterna, herramientas de diagnóstico y soporte técnico.
- Aplicar el protocolo técnico específico del proveedor o fabricante para el componente afectado. Cuando el activo esté bajo administración o soporte de tercero, el proveedor deberá entregar y aplicar su plan específico de contingencia o protocolo de recuperación.
- Priorizar la recuperación en el siguiente orden, salvo que el diagnóstico justifique un orden diferente:
    - Energía, UPS y condiciones físicas requeridas.
    - Enlace de Internet o canal alterno de conectividad.
    - Firewall, router y equipos de borde.
    - Switches de núcleo y distribución.
    - LAN Extendida entre sedes y segmentación crítica.
    - Servicios de red habilitadores: DNS, DHCP, NTP, autenticación y administración remota.
    - WLAN institucional.
    - VPN y accesos remotos.
    - WAF, servicios expuestos y controles perimetrales.
    - Telefonía IP, PBX, troncal SIP y extensiones.
- Registrar decisiones, responsables, hora de inicio, acciones ejecutadas, configuraciones restauradas, recursos utilizados, resultados y restricciones pendientes.
- Si el restablecimiento no es viable con recursos propios o contratados, mantener la contingencia controlada, aplicar canales alternos de comunicación, escalar al proveedor y registrar la limitación para seguimiento contractual o acción de mejora.

9 Recuperación de información

La recuperación de información comprende la restauración, consulta o verificación de configuraciones, respaldos, inventarios, diagramas, direccionamiento IP, reglas de seguridad, políticas de enrutamiento, registros de eventos, licencias, certificados, perfiles de telefonía, parámetros de VPN y demás información técnica requerida para recuperar los servicios de red y comunicaciones.

Si la información técnica o configuración se encuentra alterada, eliminada, comprometida o no disponible, la recuperación se realizará desde la última copia validada, respaldo de configuración, repositorio controlado, exportación autorizada o soporte del proveedor, verificando previamente que no exista compromiso de seguridad.

Se deberán considerar, según aplique:

- Configuraciones respaldadas de firewall, router, switches, WAF, WLAN, VPN, PBX y dispositivos de borde.
- Tablas de direccionamiento IP, VLAN, enlaces troncales, rutas, NAT, ACL, QoS y reglas de seguridad.
- Certificados, dominios, parámetros de DNS, túneles VPN y configuraciones de autenticación.
- Licencias, archivos de respaldo, imágenes de firmware y documentación de versión.
- Registros de auditoría, monitoreo, eventos y cambios recientes.
- Inventario de equipos, interfaces, puertos, transceptores, módulos, enlaces y responsables.
- Contactos de operadores, fabricantes, garantías y contratos aplicables.

No deben incluirse contraseñas, tokens, llaves privadas ni secretos en el PCE. Su disponibilidad para recuperación debe gestionarse mediante el Registro de Cuentas y Claves Privilegiadas y el mecanismo de custodia restringida definido por CTeI.

10 Infraestructura y conectividad

Componente	Validaciones mínimas
Energía y ambiente	Energía estable, UPS funcional, equipos energizados, temperatura adecuada, cableado seguro, racks y condiciones físicas aptas
Internet principal y respaldo	Estado de enlaces, disponibilidad del operador, IP pública, latencia, pérdida de paquetes, capacidad, rutas y conmutación
Equipos de borde	Estado de firewall, router, interfaces WAN/LAN, NAT, rutas, licencias, VPN, registros, políticas y configuraciones
LAN y LAN Extendida	Switches, puertos, enlaces troncales, VLAN, direccionamiento, rutas, segmentación, comunicación entre sedes y estabilidad
WLAN	Controladores, puntos de acceso, SSID, autenticación, cobertura, capacidad, interferencia, VLAN y políticas de acceso
Servicios de red	DNS, DHCP, NTP, autenticación, administración remota, monitoreo, repositorios de configuración y licencias
Seguridad de red	Firewall, WAF, reglas, ACL, segmentación, certificados, listas de bloqueo, registros y ausencia de indicadores de compromiso
VPN y accesos remotos	Túneles, autenticación, certificados, políticas, direccionamiento y conectividad de usuarios autorizados
Telefonía IP	PBX, troncal SIP, extensiones, rutas de llamadas, QoS, firewall, flujo de audio,

Componente	Validaciones mínimas
	comunicación interna y externa
Monitoreo	Alertas, disponibilidad, desempeño, registros, visualización de enlaces y capacidad de diagnóstico

11 Validación

Un servicio de conectividad, red o comunicaciones se considerará recuperado cuando se haya verificado, según el alcance del evento:

- Estabilidad eléctrica, física y ambiental de los equipos intervenidos.
- Estado saludable de routers, firewall, switches, interfaces, controladores, AP, PBX u otros componentes afectados.
- Conectividad entre sedes, segmentos, servidores, usuarios y servicios requeridos.
- Disponibilidad del enlace principal o, cuando aplique, operación estable sobre el canal de respaldo.
- Funcionamiento de mecanismos de balanceo o *failover*, cuando estén configurados.
- Resolución DNS, asignación DHCP, sincronización NTP y servicios habilitadores necesarios.
- Integridad de VLAN, rutas, ACL, NAT, reglas de firewall, VPN, políticas de QoS y configuraciones restauradas.
- Funcionamiento de controles de seguridad, registros, monitoreo y accesos administrativos autorizados.
- Disponibilidad de telefonía IP, llamadas internas y externas, registro de extensiones y flujo de audio, cuando aplique.
- Ausencia de alertas críticas o indicadores de compromiso de seguridad no tratados.
- Validación técnica por el Profesional Especializado responsable de Gestión de TI y, cuando corresponda, por el proveedor y responsable funcional afectado.

La validación debe considerar que puede existir recuperación en modo degradado. Por ejemplo, el canal de respaldo puede restablecer acceso institucional básico, pero con menor capacidad que el enlace principal; esa condición debe comunicarse y registrarse, no presentarse como recuperación total.

12 Comunicaciones

Momento	Responsable	Destinatarios	Canal	Contenido mínimo
Detección	Usuario, técnico o mesa de ayuda	Profesional Especializado	KAÍA, teléfono o correo	Servicio, enlace, sede, equipo o segmento afectado; hora, síntomas y alcance observado
Activación	Profesional Especializado	Jefe CTeI, personal técnico, proveedor,	Teléfono, correo	Severidad, alcance inicial, servicios

Momento	Responsable	Destinatarios	Canal	Contenido mínimo
		operador, supervisor y seguridad cuando aplique	institucional y ticket	afectados, acciones de contención, protocolo aplicable y requerimientos
Seguimiento	Coordinador técnico	Jefe CTeI, responsables definidos y usuarios afectados según impacto	Correo, ticket o canal institucional autorizado	Estado, acciones ejecutadas, servicios disponibles, restricciones, tiempo estimado y próxima actualización
Recuperación parcial	Coordinador técnico	Responsables funcionales, mesa de ayuda y usuarios afectados	Correo y ticket	Servicio disponible en modo alterno o degradado, limitaciones, recomendaciones y acciones pendientes
Restablecimiento y cierre	Profesional Especializado	Jefe CTeI, supervisor, proveedor, mesa de ayuda y responsables involucrados	Informe, ticket y correo	Alcance recuperado, duración, causa preliminar, evidencias, restricciones, hallazgos y acciones de mejora

13 Restricciones

- La capacidad de recuperación depende de la disponibilidad real del enlace principal, canal de respaldo, operadores, equipos, configuraciones, garantías, licencias, personal técnico, soporte especializado y recursos existentes.
- El canal de respaldo puede permitir continuidad parcial o degradada; su capacidad no debe asumirse equivalente al enlace principal sin mediciones y pruebas.
- La CRA no controla directamente la infraestructura, los medios físicos, la provisión de direcciones públicas ni la atención de fallas atribuibles al operador de Internet; tales elementos deben escalarse conforme a contrato y ANS. El anexo técnico excluye expresamente del soporte de integración el suministro de Internet, la provisión de IP públicas, la infraestructura del operador y la atención de fallas atribuibles a este.
- La recuperación de equipos propietaria, WAF, firewall gestionado, telefonía IP, troncal SIP, nube o servicios de terceros depende de los protocolos y soporte suministrados por el proveedor o fabricante.
- Los tiempos de recuperación son estimados mientras no existan ANS específicos, RTO/RPO validados o resultados de pruebas que demuestren el desempeño efectivo.
- Los procedimientos no pueden asegurar continuidad absoluta ante desastres físicos, daño

simultáneo de enlaces, indisponibilidad de proveedores, ausencia de repuestos, obsolescencia, agotamiento de licencias o eventos de fuerza mayor.

- Ante sospecha de incidente de seguridad, las acciones de aislamiento, contención, preservación de evidencia y análisis pueden limitar temporalmente la reconexión o restablecimiento de servicios.
- Las contraseñas, tokens, llaves privadas, configuraciones completas de seguridad y demás secretos no se incluyen en este PCE; se administran mediante registros y mecanismos restringidos de custodia.
- Los cambios de emergencia deben registrarse y regularizarse posteriormente en el proceso de gestión de cambios, sin normalizar intervenciones no documentadas.

14 Pruebas y actualización

La Oficina Asesora de CTeI realizará pruebas graduales de los mecanismos de contingencia de conectividad, redes y comunicaciones, priorizando verificaciones documentales, revisión de contactos, respaldo de configuraciones, monitoreo de enlaces, ejercicios de escritorio y pruebas técnicas controladas de conmutación, restauración o recuperación.

Las pruebas que puedan afectar usuarios, enlaces, telefonía IP, servicios institucionales o seguridad perimetral deberán programarse en ventana técnica, coordinarse con proveedores y contar con autorización del Jefe de la Oficina Asesora de CTeI cuando corresponda.

Tipo de prueba	**Periodicidad orientativa**	**Evidencia**
Revisión de inventario, topología, contactos, contratos y ANS	Anual o ante cambio relevante	Lista de verificación y registro de actualización
Verificación de respaldo de configuraciones	Semestral y antes de cambios mayores	Bitácora, exportación controlada, reporte de herramienta o informe de proveedor
Verificación del canal de respaldo y monitoreo de enlaces	Semestral	Reporte de estado, disponibilidad, alarmas e incidentes
Prueba de *failover* o balanceo	Anual o según ventana operativa	Acta, mediciones, resultados de conmutación, restricciones y acciones
Prueba de conectividad entre sedes y servicios críticos	Anual	Informe técnico, resultados de LAN Extendida, VLAN, VPN, DNS, DHCP y validación
Prueba de telefonía IP y troncal SIP	Anual o según contrato	Registro de llamadas, extensiones, audio, QoS, resultados y hallazgos
Ejercicio de escritorio por caída de enlace o incidente de red	Anual	Acta, escenario, decisiones, comunicaciones y acciones de mejora
Prueba posterior a incidente relevante	Por evento	Informe de recuperación, lecciones aprendidas y actualización del PCE

El PCE se actualizará al menos una vez al año y cuando se presenten cambios significativos en enlaces, equipos de red, firewall, WAF, VLAN, rutas, telefonía IP, contratos, proveedores, topología, configuraciones, seguridad, respaldos, responsables, contactos, incidentes críticos, pruebas fallidas o hallazgos de auditoría.

15 Evidencias

Evidencia	Fuente o ubicación de custodia	Responsable
Registro de incidente o requerimiento	KAÍA y, cuando sea necesario, correo institucional o canal alterno autorizado	Profesional Universitario grado 8
Inventario de equipos de red y comunicaciones	Inventario institucional, anexo técnico y repositorio autorizado	Oficina CTeI
Diagramas físico y lógico de red	Repositorio técnico controlado	Oficina CTeI
Direccionamiento, VLAN, rutas y configuraciones aprobadas	Repositorio técnico de acceso restringido	Profesional Especializado y proveedor responsable
Respaldos de configuraciones	Herramienta de respaldo o repositorio seguro	Personal técnico o proveedor
Bitácoras de monitoreo de enlaces, equipos y servicios	Herramientas de monitoreo, reportes y capturas controladas	Personal técnico o proveedor
Informes mensuales de canal de respaldo	Expediente contractual y repositorio de Gestión de TI	Supervisor contractual y proveedor
Registros de cambio o RFC	Mecanismo institucional de gestión de cambios	Profesional Especializado
Informes de operadores y proveedores	Expediente contractual, mesa de ayuda o repositorio autorizado	Supervisor contractual
Registro de incidentes de seguridad	Registro institucional y referencia cruzada con KAÍA/GLPI	Oficina CTeI
Registro de cuentas privilegiadas	Repositorio restringido y mecanismo de custodia institucional	Oficina CTeI
Informes de prueba, conmutación o recuperación	Expediente de contingencia y repositorio documental institucional	Profesional Especializado
Informes de continuidad y acciones de mejora	Expediente del proceso Gestión de TI	Profesional Especializado y Jefe de CTeI

16 Control de Cambios

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