BIBLIOTECA
ACCCF

03
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de respuesta a ransomware: contención, evidencia y continuidad del negocio

Primeros minutos, preservación, erradicación, recuperación y aprendizaje

Responder con rapidez sin destruir la información que permite comprender el incidente, proteger a las personas y volver a operar con controles verificables.

Coordinación editorial · Jocsan Laguna

Consejo Americano de Ciberseguridad y Cómputo Forense · 2026

Guía técnica general. Ejemplos y cifras de demostración son ficticios.

Contenido

Índice navegable. Los títulos enlazan a su ubicación dentro del documento.

Presentación: la crisis no elimina el método . . . 4

Capítulo 1. Primeros quince minutos . . . 4

1.1 Abrir el expediente antes de abrir archivos . . . 4

1.2 Apagar, desconectar o mantener . . . 5

Capítulo 2. Alcance, propagación y prioridades . . . 6

2.1 El equipo visible no es todo el incidente . . . 6

2.2 Prioridad por servicio y no por ruido . . . 6

Capítulo 3. Preservación durante la contención . . . 6

3.1 Memoria, disco, registros y estado . . . 7

3.2 Registros antes de suspender cuentas o reinstalar . . . 7

3.3 Evidencia de la nota y del canal de contacto . . . 7

Capítulo 4. Investigación: origen, persistencia y exfiltración . . . 8

4.1 Cronología con incertidumbre visible . . . 8

4.2 Hipótesis de entrada y persistencia . . . 9

4.3 Exfiltración: ausencia de prueba y prueba de ausencia . . . 9

Capítulo 5. Erradicación y decisión sobre rescate . . . 9

5.1 Erradicar la causa y no solamente el síntoma . . . 9

5.2 Pagar o no pagar: decisión documentada, no impulso . . . 10

5.3 Comunicación y obligaciones . . . 10

Capítulo 6. Recuperación y continuidad . . . 10

6.1 Seleccionar y validar el punto de recuperación . . . 11

6.2 Recuperación por etapas . . . 11

6.3 Reconciliación de información y aprendizaje . . . 11

Anexo A. Marco jurídico y registros sectoriales . . . 12

Anexo B. Formatos de respuesta . . . 13

B.1 Cronología del incidente . . . 13

B.2 Matriz de decisión de contención 13

B.3 Registro de adquisición 13

B.4 Criterios de salida de recuperación 14

Anexo C. Ejercicio y lista de verificación 14

C.1 Ejercicio de mesa con datos ficticios 14

C.2 Lista breve antes de cerrar 15

Presentación: la crisis no elimina el método

Cuando los archivos dejan de abrir y una pantalla exige un rescate, la primera reacción suele ser apagar todo, borrar lo que parece infectado y restaurar cualquier respaldo. Esas acciones pueden reducir daño en un contexto y destruir evidencia en otro. También pueden devolver a producción una persistencia que nadie revisó. El trabajo no consiste en escoger entre velocidad y prueba: consiste en preservar lo necesario mientras se limita el daño, con una persona responsable de cada decisión.

Este manual utiliza dos líneas paralelas desde el inicio. La primera protege personas, servicios y continuidad. La segunda conserva fuentes, decisiones y evidencia. No se permite que la segunda paralice una acción urgente de seguridad, ni que la primera borre sin registro la posibilidad de comprender qué pasó. Cada acción debe contestar quién la autorizó, con qué información, qué cambió y qué riesgo introdujo.

NIST SP 800-61 Rev. 3 organiza la respuesta en preparación, detección, respuesta, recuperación y mejora continua. NIST SP 800-86 aporta la relación entre recolección, examen, análisis e informe. La respuesta deja de ser una lista de botones cuando se documentan alcance, herramientas, resultados y límites. Un archivo cifrado demuestra cifrado; no demuestra por sí solo cuándo comenzó el acceso, si hubo exfiltración o quién lo hizo.[12]

> **Regla rectora**
>
> Protege primero a las personas. Después, contén con el menor daño razonable, preserva lo que pueda desaparecer y no prometas que estás limpio porque el sistema volvió a encender.

Capítulo 1. Primeros quince minutos

1.1 Abrir el expediente antes de abrir archivos

La primera persona que detecta el problema registra fecha, hora y zona, qué vio, en qué equipo, quién lo reportó y qué acciones ya ocurrieron. No necesita diagnosticar. Debe evitar abrir la nota de rescate con programas desconocidos, ejecutar adjuntos o seguir enlaces para “comprobar si es real”. Se fotografía o registra el mensaje sin interactuar con él y se conserva el objeto original cuando sea posible.

Se designa un coordinador de incidente y un canal de comunicación fuera de los sistemas potencialmente comprometidos. El directorio incluye responsable técnico, continuidad, jurídico, privacidad, comunicación, seguros y contactos de proveedores. Si el correo corporativo puede estar afectado, no se utiliza para compartir indicadores, credenciales o informes sensibles. Las decisiones verbales se anotan con hora y responsable.

Pregunta inicial	Registro mínimo	Por qué cambia la siguiente decisión
¿Hay personas o servicios críticos en riesgo?	Servicio, dependencia y consecuencia inmediata.	La contención prioriza vida y seguridad sobre evidencia.
¿Qué se observó exactamente?	Mensaje, extensión, comportamiento, activo y hora.	Distingue una alarma de una hipótesis.

Pregunta inicial	Registro mínimo	Por qué cambia la siguiente decisión
¿Sigue propagándose?	Equipos, segmentos, recursos y actividad observada.	Determina aislamiento y urgencia.
¿Qué puede desaparecer?	Memoria, sesiones, registros, enlaces y respaldos.	Prioriza preservación antes de cambios.
¿Quién decide y comunica?	Coordinador, autoridad, canal y suplencia.	Evita acciones contradictorias y rumores.

1.2 Apagar, desconectar o mantener

No existe una respuesta universal. Apagar puede detener procesos y, al mismo tiempo, eliminar memoria, sesiones y claves necesarias para analizar o recuperar. Desconectar de red puede limitar propagación y exfiltración sin borrar volatilidad, pero también puede activar una conducta prevista por el atacante o interrumpir un servicio crítico. Mantener encendido permite observar y adquirir en vivo, pero puede seguir alterando datos y expandiendo el daño.

La decisión se fundamenta en estado, propagación, servicio, cifrado, datos volátiles, herramientas y autoridad. Si hay capacidad para adquirir en vivo, se evalúa antes de apagar. Si no la hay, se documenta esa limitación y se elige la contención menos destructiva compatible con la seguridad. Un primer respondedor no debe improvisar memoria forense si no está capacitado; puede fotografiar estado, aislar según el procedimiento y escalar.

Decisión excepcional

Si una vida o servicio esencial depende del sistema, la preservación probatoria no se usa como argumento para demorar la protección. Se registra la necesidad, las alternativas consideradas y la evidencia que pudo conservarse antes y después.



Figura 1. Contener es elegir qué se protege primero. No existe una orden universal de apagar o desconectar Reconstrucción editorial; no constituye evidencia real.

Capítulo 2. Alcance, propagación y prioridades

2.1 El equipo visible no es todo el incidente

Una terminal con archivos cifrados puede ser el último eslabón de una cadena que comenzó semanas antes en otra cuenta. El mapa incluye identidades, VPN, correo, servidores, hipervisores, copias, proveedores, dispositivos personales autorizados para trabajo, sistemas de administración y servicios en la nube. La ampliación se hace con evidencia y no con la frase “todo está comprometido”, que puede producir apagones innecesarios y ocultar prioridades.

Se construye una matriz de activos con criticidad, propietario, estado, posible compromiso, dependencia, fuente de registros y decisión. Un equipo puede estar infectado, otro simplemente inaccesible porque un switch fue aislado y otro sano pero dependiente de un servidor detenido. El informe distingue esos estados para no presentarlos como una única infección confirmada.

Estado	Evidencia requerida	Decisión documentada
Confirmado	Artefacto, ejecución, registro o cifrado verificable en el activo.	Contener y preservar según prioridad.
Sospechoso	Indicador relacionado, sin confirmación suficiente.	Vigilar, aislar selectivamente o adquirir.
Afectado por dependencia	Servicio detenido por otra acción o sistema.	Recuperar dependencia sin etiquetarlo como infectado.
Sin indicios en el alcance	Consulta, filtros, período y fuentes revisadas.	No declarar limpio fuera de esa cobertura.
Desconocido	Falta de acceso, registros o inventario.	Asignar responsable y límite de conclusión.

2.2 Prioridad por servicio y no por ruido

La matriz de continuidad identifica procesos esenciales, tiempo máximo tolerable de interrupción, datos mínimos para operar, dependencias, responsables y rutas manuales temporales. Un servidor que produce muchas alertas puede ser menos prioritario que un directorio del que dependen todos. Se decide qué restaurar primero por impacto real, no por qué archivo apareció primero en la nota.

Los equipos de respuesta y continuidad trabajan con una misma cronología, pero con entregables distintos. Seguridad necesita saber qué persistencia existe; continuidad necesita saber qué versión es recuperable y qué dependencias tiene. La reconciliación evita que se restaure un sistema que volverá a conectar con el origen del incidente o que se mantenga apagado un servicio sano por desconocimiento.

Caso ficticio

Una empresa detecta cifrado en el servidor de documentos. La nómina no está cifrada, pero no funciona porque depende del mismo directorio. El equipo no etiqueta nómina como infectada: registra una afectación por dependencia. La recuperación prioriza identidad y registros antes de reconectar los servicios.

Capítulo 3. Preservación durante la contención

3.1 Memoria, disco, registros y estado

La preservación se prioriza por volatilidad y capacidad de responder preguntas. Memoria puede contener procesos, conexiones, claves o fragmentos de sesión; disco conserva archivos y artefactos; los registros explican eventos; la configuración muestra cómo estaba conectado el sistema. No todo caso requiere adquisición completa de cada activo. Se selecciona lo que puede discriminar origen, propagación, persistencia, exfiltración y recuperación.

Cada adquisición identifica fuente, método, herramienta y versión, fecha y zona, autoridad, cobertura, salida, errores y verificación. La salida se abre antes de darla por válida. Un archivo que existe pero no puede leerse no es evidencia útil. Las incidencias se conservan en el expediente, incluida una adquisición incompleta o una herramienta incompatible. La repetición genera otro objeto relacionado, no borra el primer intento.[34]

3.2 Registros antes de suspender cuentas o reinstalar

Antes de deshabilitar una cuenta se exportan registros de inicio de sesión, enrolamiento de factores, cambios de recuperación, reglas de correo, delegaciones, tokens y actividad administrativa disponible. Antes de reinstalar, se preserva imagen, configuración, registros, tareas y artefactos pertinentes. Estas acciones pueden ser imposibles en una emergencia; se anota qué se perdió y por qué, en lugar de inventar una secuencia ideal.

La retención puede rotar mientras se debate el alcance. Se solicita preservación al proveedor con período, cuentas, campos, zona, formato nativo, diccionario, filtros y limitaciones. La entrega se conserva con EML completo, cuerpo, encabezados y adjuntos. Si el proveedor declara hash para cada archivo, se comprueba localmente y se anota cualquier diferencia sin modificar la fuente.[5]

3.3 Evidencia de la nota y del canal de contacto

La nota de rescate se conserva como objeto: captura, archivo original si existe, ubicación, nombre, fecha de observación, formato y relación con el equipo. El texto puede contener afirmaciones falsas sobre exfiltración, vigilancia o tiempo de acceso. Se trata como declaración del atacante, no como hecho probado. Los identificadores de pago y contacto se registran sin hacer transacciones ni seguir instrucciones.

Objeto	Registro necesario	Error evitado
Nota de rescate	Objeto original, ubicación, fecha, relación y contenido literal.	Tratar su texto como confesión técnica.
Archivo cifrado	Muestra controlada, nombre, tamaño, estado previo y copia preservada.	Abrir muchos archivos y alterar el escenario.
Correo del incidente	EML, adjuntos, encabezados, fecha y receptor.	Guardar solo una captura del mensaje.
Cuenta de soporte	Rol, permisos, actividad y exportación.	Compartir acceso o ampliar el incidente.
Respaldo	Fecha, versión, cobertura, ubicación y estado de acceso.	Conectarlo sin evaluar contaminación.

Seguridad de laboratorio

Las muestras no se ejecutan en equipos personales ni redes de producción. El análisis dinámico requiere entorno aislado, objetivo, autorización, control de red y registro. Para la primera respuesta suele bastar preservar y escalar.

Fuentes que no deben desaparecer con la contención

ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Cada adquisición declara cobertura y límite

Fuente	Qué puede responder	Precaución
Memoria	Procesos, claves, conexiones y sesiones.	Adquisición en vivo justificada y validada.
Registros	Eventos antes, durante y después del cifrado.	Zona, rotación, integridad y cobertura.
Nota de rescate	Canal, afirmaciones y cronología.	No ejecutar archivos ni enlaces asociados.
Respaldo	Punto de recuperación y antigüedad.	No conectar antes de evaluar contaminación.
Nube y correo	Exfiltración, reglas y acceso del atacante.	Exportar antes de suspender la cuenta.

La figura explica decisiones y relaciones; no representa evidencia de un caso real.

Figura 2. Fuentes que no deben desaparecer con la contención. Cada adquisición declara cobertura y límite Reconstrucción editorial; no constituye evidencia real.

Capítulo 4. Investigación: origen, persistencia y exfiltración

4.1 Cronología con incertidumbre visible

La cronología conserva cada fecha literal, zona, fuente, precisión y conversión. Un registro UTC, una computadora desfasada y un correo local no se ordenan como si compartieran reloj sin explicar la conversión. La primera detección no es necesariamente el primer acceso. La fecha de modificación de un archivo no demuestra cuándo se ejecutó el cifrador; puede indicar la escritura de su resultado.

Se separan eventos observados, declarados por una persona, calculados e inferidos. La inferencia no se viste de registro. Si no existe una fuente para una etapa, se escribe “no acreditada en el alcance”. La ausencia de registros puede deberse a rotación, configuración, filtro o eliminación, no necesariamente a que el evento no ocurrió.

4.2 Hipótesis de entrada y persistencia

Las hipótesis pueden incluir credenciales robadas, vulnerabilidad expuesta, correo malicioso, proveedor, dispositivo externo o una combinación. El análisis compara cada una con fuentes que podrían debilitarla: autenticación, cambios de factor, reglas, procesos, tareas, servicios, cuentas nuevas, conexiones y actividad de administración. La explicación elegida es la compatible con más hechos y menos contradicciones, no la más espectacular.

Hipótesis	Fuente que confirma o debilita	Límite de la conclusión
Cuenta legítima comprometida	Sesiones anómalas, factor, dispositivo, recuperación y geografía aproximada.	Cuenta usada no identifica persona.
Vulnerabilidad pública	Versión, exposición, registros, prueba controlada y fecha de parche.	Presencia de vulnerabilidad no demuestra explotación.
Correo malicioso	EML, adjuntos, telemetría de apertura y ejecución.	Recepción no demuestra ejecución.
Proveedor comprometido	Acceso remoto, roles, cambios y correlación temporal.	Relación contractual no prueba vector.
Persistencia	Cuentas, tareas, servicios, claves, reglas y artefactos.	No erradicar solo el archivo visible.

4.3 Exfiltración: ausencia de prueba y prueba de ausencia

Para evaluar exfiltración se revisan conexiones, destinos, volumen, compresión, sincronización en nube, correo, reglas, servicios de transferencia, registros de proxy, DNS cuando esté disponible y declaraciones del atacante como hipótesis separada. Un volumen alto puede ser respaldo o actividad legítima; la falta de tráfico puede significar ausencia de registros, cifrado no inspeccionado o un canal no incluido.

La conclusión distingue: evidencia de transferencia, indicios compatibles, datos insuficientes o ausencia observada dentro de una cobertura definida. No se afirma “no hubo exfiltración” solo porque el firewall no la muestra. Tampoco se acepta “publicaremos tus datos” como prueba de que los datos salieron. Si se localiza una muestra publicada, se documenta sin difundirla ni descargar información innecesaria.

> **Redacción defendible**
>
> “No se observaron transferencias asociadas con el incidente en los registros de proxy comprendidos entre estas fechas y con estos campos. La cobertura no incluye canales cifrados no inspeccionados, otros proveedores ni períodos anteriores; por tanto, la ausencia total de exfiltración no puede afirmarse.”

Capítulo 5. Erradicación y decisión sobre rescate

5.1 Erradicar la causa y no solamente el síntoma

La erradicación incluye cuentas, métodos de recuperación, reglas, accesos remotos, persistencia, vulnerabilidades, secretos y rutas de proveedor. Cambiar una contraseña no basta si permanecen tokens, sesiones o claves. Eliminar el cifrador no elimina el punto de entrada. Las medidas se verifican con fuentes y pruebas, y se registran efectos sobre la operación.

Si no se conoce la causa, se declara. La organización puede elegir reconstruir desde un entorno confiable en lugar de “limpiar” sobre el mismo sistema. La decisión se basa en riesgo y evidencia, no en una apariencia de ahorro. Un sistema reinstalado recibe nueva configuración, credenciales y monitoreo; no se devuelve al mismo estado que permitió el incidente.

5.2 Pagar o no pagar: decisión documentada, no impulso

La decisión de pago pertenece a la organización y a sus asesores jurídicos, aseguradores y autoridades competentes. Debe considerar legalidad, sanciones, origen y destino de fondos, capacidad de continuidad, protección de personas, posibilidad de nuevas extorsiones y ausencia de garantía de recuperación. Este manual no recomienda pagar ni contactar con el atacante; ofrece la estructura para que la decisión no dependa de una sola persona bajo presión.

Factor	Pregunta que debe responderse	Evidencia para decidir
Legalidad	¿Existe prohibición, sanción o restricción aplicable?	Análisis jurídico actualizado y canal de aprobación.
Continuidad	¿Hay otra ruta viable y cuánto tarda?	Pruebas de respaldo, alternativas y costo de interrupción.
Recuperación	¿Qué se promete y qué puede comprobarse?	Ninguna garantía verbal; evaluación técnica y límites.
Riesgo humano	¿Hay amenaza adicional o datos sensibles?	Prioridad de seguridad y protección de afectados.
Repetición	¿Qué incentivo o exposición queda?	Riesgo documentado y plan posterior.
Autoridad	¿Quién puede decidir y comunicar?	Quórum, registro y canal único autorizado.

5.3 Comunicación y obligaciones

La evaluación de notificación distingue clientes, titulares de datos, reguladores, seguros, socios y autoridad. Cada jurisdicción y contrato tiene umbrales y plazos distintos. La información técnica se prepara de manera que permita explicar hechos, incertidumbre y medidas sin revelar detalles que aumenten el daño. La comunicación pública no se adelanta a la preservación ni convierte una sospecha en anuncio de causa.

En México, las instituciones de crédito tienen obligaciones específicas de investigación y aviso de incidentes, registros y conservación dentro de las disposiciones aplicables; en Perú, la SBS exige preservación y análisis forense a entidades supervisadas; en Argentina, la Comunicación A 8280 aborda respuesta y reporte final en su régimen. No se exportan esos plazos a toda organización ni a otro país.[6][7][8]

> **No fabricar certeza**
>
> El parte ejecutivo puede decir qué se sabe, qué se hace y qué falta por determinar. No necesita escoger entre pánico y tranquilidad artificial. Necesita una cronología defendible y responsables claros.

Capítulo 6. Recuperación y continuidad

6.1 Seleccionar y validar el punto de recuperación

El respaldo más reciente puede contener persistencia o archivos dañados; el más antiguo puede perder operaciones legítimas. Se comparan fecha, cobertura, integridad, acceso, historial y compatibilidad. Se preserva el respaldo original y se trabaja sobre copia controlada en un entorno aislado. Las llaves se entregan por canal separado y no se escriben en el acta.

La validación incluye que la copia abre, contiene los objetos esperados, puede montarse, presenta coherencia de versiones y no exhibe indicadores conocidos de compromiso. No demuestra que sea totalmente limpia; demuestra que superó las pruebas definidas. Si la copia tiene errores, se decide si esos errores afectan el objetivo y se conserva su detalle.

6.2 Recuperación por etapas

Se comienza por servicios mínimos en aislamiento, con datos ficticios o cuentas de prueba. Después se prueban identidad, permisos, aplicaciones, integración, lectura y escritura, exportación y monitoreo. Solo entonces se autoriza una ampliación gradual. La red de producción no se utiliza como laboratorio de primera recuperación.

Etapa	Criterio de aceptación	Evidencia
Infraestructura mínima	Componentes y versiones verificados, sin persistencia conocida.	Inventario y configuración.
Datos	Archivos legibles, cobertura y relación correctas.	Muestra, manifiesto y conteo.
Aplicación	Funciones y permisos operan con cuentas ficticias.	Casos de prueba y resultados.
Integración	Dependencias autorizadas responden sin rutas no previstas.	Registros y conexiones.
Observación	No aparece actividad anómala en el período definido.	Alertas, consultas y límites.
Salida	Responsable acepta riesgo residual y siguiente revisión.	Acta de salida y monitoreo.

6.3 Reconciliación de información y aprendizaje

Puede ser necesario reconstruir operaciones creadas entre el último respaldo íntegro y la detección. Se concilian registros externos, comprobantes, correos, mensajes y documentos de terceros sin alterar la fuente. Las diferencias se anotan y no se rellenan con estimaciones disfrazadas de datos reales.

La lección aprendida cambia el procedimiento: nuevas reglas de retención, autenticación resistente al phishing, segmentación, copias inmutables, pruebas de restauración, directorio, limitación de privilegios o ejercicios. Si el incidente termina con una presentación pero ningún comportamiento cambia, la siguiente crisis repetirá la misma secuencia.

Criterio de cierre

Recuperar es volver a operar con evidencia de que los controles funcionan y con una explicación honesta de lo que sigue desconocido. El cierre incluye personas, sistemas, datos, proveedores y revisión posterior.



Figura 3. Restaurar no equivale a recuperar confianza. La salida se comprueba por etapas y con criterios de aceptación Reconstrucción editorial; no constituye evidencia real.

Anexo A. Marco jurídico y registros sectoriales

El incidente puede involucrar evidencia electrónica, protección de datos, contratos, obligaciones financieras y reglas de continuidad. Estas funciones se analizan por separado. Una norma sectorial no crea una obligación universal y un plazo de retención no autoriza a conservar todo indefinidamente. Revisión documental al 10 de noviembre de 2026; el expediente real requiere verificar vigencia, sujeto, materia y canal.

Jurisdicción	Fuentes funcionales	Límite de uso
México	CCom 89–94 y 1205; CFPC 210-A / CNPCF 348–350 según transición; CNBV 316 Bis serie para entidades comprendidas; LFPDPPP para datos personales.	Separar documento electrónico, proceso, banca y privacidad. Revisar declaratoria CNPCF.
Perú	Reglamento IOFE; CPC 188–197; SBS 504-2021 y 2286-2024 para entidades supervisadas.	No atribuir a Ley 27269 un régimen documental completo ni copiar plazos CNBV.
Chile	Ley 19.799; RAN 20-7, 20-8, 20-10 según entidad y servicio.	No confundir continuidad, externalización e incidentes.
Argentina	Ley 25.506; CCyC 318–319; BCRA A 7783 y A 8280.	Plazos y sujetos propios; autenticación no equivale a autorización.
Colombia	Ley 527; CPACA para actuaciones administrativas; normativa SFC por confirmar en su numeral específico.	No inventar requisitos de incidentes de una circular no leída.
Ecuador	Ley 67; LOPDP; régimen del sistema de pago cuando corresponda.	La notificación y conservación dependen del tratamiento y sector.

Jurisdicción	Fuentes funcionales	Límite de uso
España / UE	eIDAS; LEC 326 y 384; RGPD; RD-ley 19/2018 para servicios de pago.	Distinguir documento, proceso, privacidad y operaciones no autorizadas.

Fuentes de la tabla: [9][10][11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27]

Para una solicitud de registros se especifica función, período, referencia, campos, formato, zona y método de entrega. El objetivo no es pedir todos los servidores, sino los eventos que pueden contestar preguntas concretas. La cadena de custodia conserva quién entrega, quién recibe, qué objeto contiene, cómo se verifica y qué limitaciones existen.

Anexo B. Formatos de respuesta

B.1 Cronología del incidente

Campo	Registro exigido	Control
Evento	Observado, declarado, calculado o inferido.	No mezclar categorías.
Fecha literal y zona	Texto original, conversión y precisión.	No sobrescribir fuente.
Activo y fuente	Objeto, sistema, identificador y ubicación.	Trazabilidad hasta el manifiesto.
Acción y responsable	Qué ocurrió, quién decidió y quién ejecutó.	Autoridad y evidencia.
Resultado	Salida, errores y cambios de estado.	No esconder incidencias.
Siguiente comprobación	Pregunta abierta y responsable.	Evitar cierre prematuro.

B.2 Matriz de decisión de contención

Ficha ficticia de decisión

```
Incidente: DEMO-RANSOM-2026-001
Activo y servicio: [identificador, función, dependencias]
Estado observado: [pantalla, procesos, red, cifrado]
Opciones evaluadas: [apagar, aislar red, mantener, suspender cuenta]
Riesgo para personas y continuidad: [prioridad]
Volatilidad y evidencia en riesgo: [memoria, registros, sesiones]
Decisión y autoridad: [acción, persona, fecha y zona]
Preservación previa: [objeto, método y salida]
Cambio producido: [estado final y efecto colateral]
Pendiente: [qué no se pudo preservar o confirmar]
Revisión: [responsable y siguiente hora de evaluación]
```

B.3 Registro de adquisición

Manifiesto técnico

```
ID de fuente / adquisición: DEMO-SRV-001 / A01
Autoridad y alcance: [documento y exclusiones]
Estado inicial: [fotografías y observación]
Objetivo y cobertura: [memoria, imagen, lógica, exportación]
Herramienta y validación: [versión, entorno y prueba]
Inicio / fin con zona: [valores literales]
Salida: [archivos, formato y tamaño]
Integridad: [algoritmo y objeto exacto]
Incidencias: [errores y cobertura faltante]
Verificación: [apertura, relación y revisión]
Custodia: [resguardo, acceso y transferencias]
```

B.4 Criterios de salida de recuperación

Comprobación	Sí / no / no aplica	Evidencia y observación
Respaldo preservado antes de usar	[ ]	Identificador y custodia.
Datos legibles y cobertura coherente	[ ]	Muestra y conteo.
Cuentas y factores reconstruidos	[ ]	Sin sesiones antiguas.
Persistencia evaluada	[ ]	Fuentes y límites.
Funciones e integraciones probadas	[ ]	Casos ficticios.
Monitoreo y responsable asignado	[ ]	Alertas y revisión.
Comunicaciones ejecutadas	[ ]	Versiones y destinatarios.
Riesgo residual aceptado	[ ]	Firma y fecha de responsable.

Anexo C. Ejercicio y lista de verificación

C.1 Ejercicio de mesa con datos ficticios

Se simula una empresa con tres servidores, dos cuentas administrativas, respaldo nocturno y un proveedor de correo. A las 08:12 se reporta cifrado en documentos; a las 08:16 otro equipo presenta la misma extensión; a las 08:20 se descubre una regla de reenvío en una cuenta. El equipo debe decidir aislamiento, primeras adquisiciones, contacto con proveedor, evaluación de datos y ruta de recuperación, sin ejecutar ningún archivo.

La evaluación se basa en calidad de decisiones y registros: si el equipo restaura sin preservar, pierde la oportunidad de explicar el reenvío; si suspende la cuenta antes de exportar, documenta el límite; si deja un servicio crítico sin alternativa, debe justificarlo. Al final se revisan decisiones en vez de premiar la actuación más rápida.

C.2 Lista breve antes de cerrar

Pregunta	Resultado esperado
¿Las personas están protegidas?	Prioridades y servicios esenciales atendidos.
¿Se conservó la evidencia volátil prioritaria?	Objetos, métodos y límites registrados.
¿Se evaluaron origen, persistencia y exfiltración?	Hipótesis y fuentes, sin absolutos.
¿Las decisiones de rescate y comunicación fueron autorizadas?	Quórum, fundamento y versiones.
¿La recuperación fue probada?	Datos, funciones, accesos y observación.
¿Qué cambió para la próxima vez?	Control real, responsable y validación.

Cierre

La calma no consiste en decir que todo está bien. Consiste en saber qué se está haciendo, con qué evidencia, quién decide y qué queda por comprobar.

Referencias citadas

Cada número remite a la fuente consultada en el cuerpo. La fecha general de revisión documental es el 10 de noviembre de 2026; el uso en un expediente exige comprobar la versión aplicable al hecho, materia, sujeto y jurisdicción.

[1] NIST SP 800-61 Rev. 3 (abril de 2025). Recomendaciones de respuesta a incidentes integradas en CSF 2.0: preparación, detección, respuesta, recuperación y mejora. Sustituye la revisión 2. Fuente oficial en línea

[2] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Guía metodológica, no legislación ni garantía de admisibilidad. Fuente oficial en línea

[3] ISO/IEC 27037:2012. Directrices para identificación, recolección, adquisición y preservación de evidencia digital. Edición confirmada por ISO como vigente. Fuente oficial en línea

[4] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Guía metodológica, no legislación ni garantía de admisibilidad. Fuente oficial en línea

[5] RFC Editor. RFC 5322, Internet Message Format: estructura del mensaje, encabezados y cuerpo. Es una referencia técnica para preservar y comprender correo electrónico, no una prueba automática de identidad humana. Fuente oficial en línea

[6] Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis, 316 Bis 1, 316 Bis 10 a 17: comprobantes, cifrado, acceso, incidentes, incidencias, bitácoras y revisiones. Fuente oficial en línea

[7] Perú. SBS 504-2021, artículos 12.6.g, 15 y 17.3–17.4: preservación, reporte y análisis forense, registros de enrolamiento, autenticación y operaciones. Fuente oficial en línea

[8] Argentina. BCRA Comunicación A 8280: respuesta y recuperación ante ciberincidentes; reporte final dentro de cinco días corridos posteriormente a contención, recuperación y resolución. Fuente oficial en línea

[9] Código de Comercio de México, artículos 89–94 y 1205: neutralidad, atribución, escrito, original, integridad, accesibilidad y admisión de mensajes de datos. Compilación oficial. Fuente oficial en línea

[10] Código Federal de Procedimientos Civiles, artículo 210-A: fiabilidad del método, atribución, accesibilidad e integridad de la información electrónica. Código abrogado por decreto de 07-06-2023, sujeto al régimen gradual de transición. Fuente oficial en línea

[11] Código Nacional de Procedimientos Civiles y Familiares, artículos 348–350. Compilación con reforma del 15-01-2026. La aplicación es gradual y depende de declaratorias. Fuente oficial en línea

[12] Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis, 316 Bis 1, 316 Bis 10 a 17: comprobantes, cifrado, acceso, incidentes, incidencias, bitácoras y revisiones. Fuente oficial en línea

[13] Perú. Reglamento de la IOFE, DS 052-2008-PCM, artículos 3 y 4: exigencia y admisión de documentos electrónicos firmados digitalmente. Fuente oficial en línea

[14] Perú. Código Procesal Civil, artículos 188–197 y 245.5: finalidad, legalidad, medios, carga, valoración y fecha por medios técnicos. Fuente oficial en línea

[15] Perú. SBS 504-2021, artículos 12.6.g, 15 y 17.3–17.4: preservación, reporte y análisis forense, registros de enrolamiento, autenticación y operaciones. Fuente oficial en línea

[16] Chile. Ley 19.799 sobre documentos electrónicos y firma electrónica, artículos 1–5: equivalencia, escrito, firma simple/avanzada, fecha y valor probatorio. Fuente oficial en línea

[17] Chile. Recopilación Actualizada de Normas, capítulos 20-7, 20-8 y 20-10: externalización, incidentes operacionales, seguridad de la información y ciberseguridad. Fuente oficial en línea

[18] Argentina. Ley 25.506 de Firma Digital, artículos 1 y 5–9: documento digital, carga al invocar firma electrónica desconocida y presunciones delimitadas. Fuente oficial en línea

[19] Argentina. Código Civil y Comercial, artículos 318–319: correspondencia por cualquier medio y ponderación de confiabilidad de soportes y procedimientos técnicos. Fuente oficial en línea

[20] Argentina. BCRA Comunicación A 8280: respuesta y recuperación ante ciberincidentes; reporte final dentro de cinco días corridos posteriormente a contención, recuperación y resolución. Fuente oficial en línea

[21] Colombia. Ley 527 de 1999, artículos 5–13, 16–25 y 28: mensajes de datos, escrito, original, integridad, admisibilidad, conservación, envío, recepción y firma digital. Fuente oficial en línea

[22] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, artículos 2, 6–8, 10–16: equivalencia, escrito, original, conservación, procedencia, envío, recepción y firma electrónica. Fuente oficial en línea

[23] Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artículos 10, 37–44: principios, medidas de seguridad, protección desde el diseño, riesgos y tratamiento ante incidentes. Fuente oficial en línea

[24] Reglamento (UE) 910/2014 eIDAS, artículos 25–26 y 46: no discriminación de firmas electrónicas y documentos por su formato, firma avanzada y efectos de firma cualificada. Fuente oficial en línea

[25] España. Ley de Enjuiciamiento Civil, artículos 326 y 384: documentos privados, impugnación, instrumentos para archivar, conocer o reproducir datos, examen, custodia y sana crítica. Fuente oficial en línea

[26] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea

[27] España. Real Decreto-ley 19/2018, artículos 45, 66 y 67: restitución por operaciones no autorizadas, gestión de riesgos y notificación inmediata de incidentes graves. Fuente oficial en línea

Aviso editorial: guía técnica general y material educativo. No constituye asesoría legal, dictamen pericial ni autorización para acceder a sistemas o información. Los ejemplos y cifras de demostración son ficticios; las figuras son reconstrucciones editoriales.