CASO PRÁCTICO PARA AUDITORÍA, PRIVACIDAD, RIESGO Y CUMPLIMIENTO

Las primeras 24 horas de un ataque de ransomware

Por Stephan · 9 de noviembre de 2026

CASO FICTICIO

Logística Vantoria, sus sistemas, sus horarios y sus cifras se han creado para este ejercicio. Las obligaciones legales y las recomendaciones técnicas se citan por separado.

A las 02:10, el equipo de guardia de Vantoria recibe una alerta de cifrado masivo. Antes de que amanezca tendrá que aislar servidores, proteger pruebas y explicar por qué se han detenido los pedidos. Al terminar el día deberá decidir si puede reanudar parte de la operación mientras sigue abierta la investigación.

El caso está pensado para quienes aprueban esas decisiones, evalúan sus riesgos o revisan el expediente después. La cronología separa los hechos de las hipótesis y el registro D-07 muestra qué se sabía al autorizar la recuperación.

Tres decisiones en las primeras horas

• **Quién aísla.** El plan define quién puede aislar un equipo y quién autoriza interrumpir un servicio crítico. NIST SP 800-61 Rev. 3, §§ 2.2–2.3.

• **Qué se conserva.** Priorice la memoria y los registros que puedan sobrescribirse. Aísle los sistemas afectados de inmediato y reserve el apagado para cuando no pueda desconectarlos de la red. CISA, parte 2, pasos 1, 2 y 9.

• **Quién autoriza recuperar.** En Vantoria, Operaciones y Seguridad aprueban juntas la recuperación de un sistema crítico. El plan fija los criterios y TI ejecuta. NIST CSF 2.0, RS.MA-05.

La empresa y su plan

Vantoria es una distribuidora con sede en América Latina y una filial en España. Tiene 900 empleados, 120 en la filial. El caso sigue dos servidores de archivos (FS-01 y FS-02), un servidor de salto (SALTO-01), el sistema de pedidos y facturación (ERP-01) y el servidor de copias en línea (BK-01). También hay una copia inmutable en la nube con retención bloqueada durante 14 días.

La sección 4.2 del plan faculta al analista de guardia para aislar un equipo individual y avisar en 15 minutos. Aislar un segmento o un servicio crítico exige autorización de la directora de seguridad (CISO), previa consulta con el responsable del servicio. La sección 6.1 exige aprobación conjunta para recuperar un sistema crítico y confirmación de la líder de respuesta de que se han cumplido los criterios aplicables.

01 / CRONOLOGÍA

De la primera alerta al aviso a Jurídica

Todas las horas del caso corresponden a la sede. El martes a las 02:10 empieza el ejercicio. La hora en que el equipo detecta el cifrado y la hora en que tuvo constancia de una brecha de datos se registran por separado.

Hora	Hecho confirmado	Hipótesis o incógnita	Decisión o acción
02:10	La herramienta de detección en equipos (EDR) alerta de renombrados masivos en FS-01. Aparece una nota de rescate.	FS-01 podría ser el único equipo afectado.	**D-01.** El analista aísla FS-01 por EDR y avisa a la líder de respuesta dentro del plazo del plan.
02:25	Hay archivos cifrados en FS-02 y SALTO-01.	El atacante podría tener credenciales privilegiadas.	**D-02.** El analista aísla ambos equipos y actualiza a la líder por teléfono.
02:52	ERP-01 comparte la red virtual (VLAN) de servidores. El equipo todavía no observa cifrado en el ERP.	El atacante podría alcanzar ERP-01.	**D-03.** La CISO consulta a Operaciones y autoriza aislar la VLAN desde el conmutador. Los pedidos se detienen.
03:30	Se declara un incidente de severidad 1.	El correo corporativo podría estar bajo vigilancia.	**D-04.** El comité se reúne por canales alternativos y activa a la firma forense.
03:50–04:05	Se exportan los registros del cortafuegos, que retiene siete días de datos.	Todavía se desconoce cuánto abarca el incidente.	**D-05.** Se preserva la evidencia. La firma comienza a capturar memoria y después obtiene imágenes de disco de los tres equipos.
06:00	Registros históricos de la VPN muestran un acceso externo de svc-inventario, sin autenticación multifactor, nueve días antes. En FS-01 se borraron instantáneas.	La cuenta pudo ser la vía de entrada.	El equipo amplía la búsqueda de persistencia y comienza a rastrear sesiones activas y credenciales relacionadas.
08:00	Se borró el catálogo de BK-01. Existe una copia inmutable del domingo a las 23:00.	La copia podría contener cambios posteriores a la intrusión.	Operaciones pide restaurar. La líder de respuesta mantiene en espera la solicitud mientras se verifica la copia.
10:30	FS-02 transfirió 38 GB a un servicio de almacenamiento el lunes a las 23:40. En el servidor se ejecutó rclone.	Aún se desconoce el contenido de la transferencia.	Se avisa a Jurídica y a la delegada de protección de datos (DPD) de la filial.

02 / CRONOLOGÍA

De la brecha de datos al primer pedido

Hora	Hecho confirmado	Hipótesis o incógnita	Decisión o acción
11:00	El inventario y la revisión de FS-02 confirman que el cifrado dejó inaccesibles expedientes de 120 empleados de la filial española.	Sigue sin conocerse si los expedientes se copiaron.	**D-06.** Jurídica y la DPD documentan la constancia de la brecha. El responsable evalúa el riesgo e inicia la preparación de la notificación.
12:30	La junta pide una decisión sobre el rescate.	Sigue abierto el análisis de obligaciones sectoriales.	El comité decide no pagar, avisa a la aseguradora y denuncia el ataque. Contacta al CSIRT de referencia para apoyo.
15:02	La cuenta svc-inventario queda deshabilitada.	Podría haber otras cuentas o sesiones comprometidas.	La CISO restringe la VPN a un grupo de emergencia con autenticación multifactor y ordena revocar las sesiones de la cuenta afectada.
18:00	El análisis de la copia de SALTO-01 confirma que incluye una herramienta de acceso remoto no autorizada, instalada ocho días antes.	Falta descartar persistencia en otros equipos.	Se excluye esa copia de la recuperación de SALTO-01, se bloquea el archivo identificado y se amplía la búsqueda de actividad relacionada.
21:40	La copia de datos de archivos supera la revisión inicial. ERP-01 supera pruebas previas de integridad y de pedidos en la red de recuperación.	Podría persistir actividad fuera del entorno validado. La conciliación ampliada del ERP sigue pendiente.	**D-07.** Operaciones y la CISO aprueban una vuelta limitada a la operación, con monitoreo y criterios de suspensión.
23:30	ERP-01 vuelve a aceptar pedidos mediante un acceso controlado a la red de recuperación.	Continúa el seguimiento de persistencia y de integridad.	Se registra el resultado y se fija la próxima revisión del comité para el miércoles a las 09:00.

Balance a las 24 horas · miércoles, 02:10

Se conservaron la memoria y las imágenes de los tres equipos cifrados. La cuenta sospechosa está deshabilitada, la copia de SALTO-01 quedó excluida y el ERP opera con acceso limitado. El responsable del tratamiento envió una notificación inicial a la autoridad competente durante el martes y dejó constancia de los datos pendientes.

Pendientes. El miércoles, Finanzas ampliará la conciliación del ERP a las 10:00 y la firma forense informará sobre el acceso inicial y el contenido de la transferencia a las 12:00. Jurídica revisa en paralelo el régimen sectorial. La llamada al CSIRT queda registrada por separado.

03 / CONTENCIÓN Y EVIDENCIA

Quién aísla y qué debe quedar en el expediente

Autorizar el aislamiento

El plan debe asignar autoridad para aislar un equipo, interrumpir un segmento y retirar de servicio un sistema crítico. También debe identificar al suplente, el tiempo de escalamiento y las facultades del proveedor externo. Si varios sistemas parecen afectados, valore el aislamiento desde el conmutador y coordine la respuesta por un canal alternativo. NIST SP 800-61 Rev. 3, §§ 2.2–2.3 · CISA, parte 2, paso 1.

PRUEBA DE AUDITORÍA

Compare D-03 con la sección 4.2 del plan. Busque la hora, la recomendación de la líder de respuesta, la consulta a Operaciones y evidencia de la aprobación de la CISO. Una llamada puede quedar respaldada por el registro contemporáneo y su confirmación posterior, según lo que exija el plan.

Conservar evidencia durante la contención

• **Datos volátiles.** Tras aislar los equipos, preserve la memoria y los registros de corta retención. Si la única vía de contención es apagar un equipo, documente qué datos volátiles pueden perderse. CISA, parte 2, pasos 1, 2 y 9.

• **Artefactos del incidente.** Obtenga imágenes de una muestra representativa de equipos, exporte los registros pertinentes de EDR, VPN, cortafuegos, proxy e identidad, y tome instantáneas de volúmenes en la nube cuando corresponda. Conserve la nota de rescate, una copia y muestras de archivos cifrados. CISA, parte 2, pasos 1 y 9.

• **Cadena de custodia.** Registre quién recogió cada elemento, cuándo, su origen, dónde se guardó y quién lo recibió. Calcule y conserve un hash de los archivos o imágenes cuando corresponda. Limite el acceso a la evidencia, que puede contener datos personales. NIST CSF 2.0, RS.AN-06 y RS.AN-07.

EVIDENCIA DEL CASO

E-02 es la copia de la nota de rescate. E-03 es la exportación del cortafuegos de las 03:50. E-04 a E-09 son las capturas de memoria y las imágenes de disco. La firma documenta cada adquisición y calcula SHA-256 para los archivos resultantes. El acceso a los registros históricos de VPN permite investigar eventos anteriores al período de retención del cortafuegos.

Privacidad también lleva su propio registro. El responsable documenta los hechos, efectos y medidas correctivas de toda brecha de datos personales, incluida la decisión sobre la notificación. RGPD, art. 33.5.

04 / RECUPERACIÓN

Qué hay que comprobar antes de volver a operar

En Vantoria, Operaciones y Seguridad autorizan juntas la recuperación y TI la ejecuta. El plan identifica qué debe comprobar la líder de respuesta y cómo se deja constancia de los riesgos pendientes. NIST recomienda definir y aplicar criterios para iniciar la recuperación, considerando la evidencia disponible y la interrupción que puede causar la propia recuperación. NIST SP 800-61 Rev. 3, tabla 3, RS.MA-05.

Criterios de decisión

• **Contención suficiente.** Cierre las vías de entrada identificadas, revoque accesos comprometidos y busque persistencia. Si el acceso inicial sigue bajo investigación, documente esa incertidumbre y cómo se separará la operación recuperada del entorno afectado.

• **Copias verificadas por sistema.** Compare la fecha de la copia con el primer indicio de intrusión. Compruebe integridad, analice indicadores de compromiso y haga una restauración de prueba cuando proceda. La inmutabilidad protege la copia de modificaciones durante su retención. El contenido puede incluir cambios que el atacante hizo antes. NIST CSF 2.0, RC.RP-03.

• **Evidencia preservada.** Termine la adquisición de los elementos que se perderían durante la reconstrucción o registre qué falta y por qué.

• **Entorno y servicio validados.** Use una red de recuperación segregada y limite sus conexiones. Verifique la integridad técnica y las funciones esenciales del servicio antes de admitir tráfico operativo. CISA, parte 2, recuperación · NIST CSF 2.0, RC.RP-05.

• **Seguimiento.** Registre quién acepta el riesgo, quién verifica cada pendiente y cuándo se detiene el servicio o se reabre la decisión.

LA COPIA DEL DOMINGO

A las 08:00 la empresa sabía que la copia existía y que había ocurrido un acceso remoto sospechoso nueve días antes. A las 18:00 confirmó que la copia de SALTO-01 contenía la herramienta no autorizada. Por eso reconstruyó SALTO-01 desde una imagen verificada y evaluó por separado la copia de los datos de archivos.

A las 21:40, Vantoria autorizó una reanudación parcial del ERP después de validar su integridad y probar el flujo de pedidos. El entorno recuperado admitió únicamente conexiones autorizadas y el resto de la red siguió aislado. La recuperación parcial fue una decisión documentada del caso. El cierre del incidente requería su propia evaluación. CISA, parte 2, erradicación y recuperación.

05 / NOTIFICACIÓN

Qué plazos corren en paralelo

RGPD · la constancia de la brecha inicia el cómputo

El responsable del tratamiento debe avisar a la autoridad de control competente sin dilación indebida y, cuando sea posible, en un máximo de 72 horas desde que tiene constancia de la brecha, salvo que sea improbable que exista un riesgo para los derechos y libertades de las personas. Si faltan datos, puede aportarlos por fases. Si se supera el plazo, debe explicar el retraso. Cuando sea probable un alto riesgo, el artículo 34 prevé también la comunicación sin dilación indebida a las personas afectadas, con las excepciones de su apartado 3. RGPD, arts. 33–34 · AEPD, notificación a la autoridad · AEPD, comunicación a las personas afectadas.

Se tiene constancia cuando existe un grado razonable de certeza de que el incidente ha comprometido datos personales. El cifrado puede causar una brecha de disponibilidad aunque el equipo aún desconozca si se copiaron los archivos. CEPD, Directrices 9/2022, apartados 20–23 y 32–35.

D-06 / MARTES, 11:00

El equipo confirma que el cifrado dejó inaccesibles los expedientes de 120 empleados. Jurídica y la DPD registran la evidencia y la hora de constancia. El responsable valora conjuntamente la pérdida de disponibilidad y la posible exposición, y presenta una notificación inicial ese mismo martes. Las 72 horas se cumplen el viernes a las 11:00, en la misma referencia horaria del caso. El análisis sobre los 38 GB y sobre el posible alto riesgo continúa en paralelo.

España · alcance y canal sectorial

El artículo 23 de NIS2 establece para las entidades comprendidas una alerta temprana en 24 horas y una notificación en 72 horas desde que tienen constancia de un incidente significativo, con reglas específicas para determinados servicios. El informe final se presenta, por regla general, en un mes desde la notificación del incidente. Este cómputo se evalúa por separado del RGPD. Directiva (UE) 2022/2555, art. 23.

En julio de 2026, la Comisión Europea anunció que llevaría a España ante el Tribunal de Justicia por no haber notificado medidas de transposición. En el ejercicio, Jurídica consulta el BOE y comprueba si resultan aplicables el Real Decreto-ley 12/2018, el Real Decreto 43/2021 o alguna norma sectorial o posterior. El caso deja pendiente la calificación de la filial y el umbral de reporte sectorial. Comisión Europea, INFR(2024)0270 · BOE, RDL 12/2018 · BOE, RD 43/2021.

América Latina · identificar primero el país

La sede del caso carece de una jurisdicción concreta. Antes de fijar un plazo para esa sede, identifique el país, el sector, el responsable del tratamiento, la autoridad competente y el hecho que inicia el cómputo.

06 / REGISTRO DE DECISIONES

D-07 · reanudar los pedidos con acceso limitado

Campo	Entrada del registro
Identificación	D-07 · martes, 21:40, hora de la sede · 19 h 30 min desde la primera alerta.
Decisión solicitada	Reanudar la toma de pedidos en ERP-01 y autorizar la restauración de archivos en servidores nuevos.
Opciones	A. Reabrir la red original y restaurar todo esa noche. B. Recuperar el ERP y los archivos en un entorno segregado y reconstruir SALTO-01 desde una imagen verificada. C. Esperar el informe forense completo, estimado en tres días.
Hechos y evidencia	La cuenta sospechosa está deshabilitada (E-11). Las pruebas previas del ERP y del flujo de pedidos se superaron (E-14). La copia de SALTO-01 contenía la herramienta no autorizada (E-17). La copia de datos de archivos superó el análisis inicial (E-19).
Hipótesis y verificación	Persistencia fuera del entorno validado: informe preliminar de la firma forense el miércoles a las 12:00. Alteraciones fuera del conjunto de pruebas iniciales del ERP: conciliación ampliada de Finanzas el miércoles a las 10:00.
Riesgo de actuar	Reinfección o errores en pedidos. La red segregada, el acceso restringido, la vigilancia del EDR y la conciliación de Finanzas reducen la exposición.
Riesgo de esperar	Los pedidos están detenidos desde las 02:52. Operaciones estima que cada día sin el ERP impide despachar a unos 300 clientes.
Propone y confirma	La líder de respuesta propone la opción B y confirma el cumplimiento de los criterios de recuperación aplicables.
Autorizan	El director de Operaciones, responsable del ERP, y la CISO, según la sección 6.1 del plan.
Consultados	Firma forense, Jurídica y Dirección Financiera.
Informados	Dirección General, aseguradora y DPD de la filial.
Evidencia conservada	Memoria e imágenes de FS-01, FS-02 y SALTO-01 (E-04 a E-09) y registros de validación y contención. La hoja de custodia identifica las adquisiciones y sus hashes cuando corresponden.
Decisión y hora	B, aprobada a las 21:40. Operaciones y Seguridad aceptan el riesgo residual para el alcance aprobado. A expone la red original y utilizaría una copia descartada. C prolonga la interrupción.
Condición de suspensión	Un indicador de compromiso en el entorno recuperado o una discrepancia material en pedidos, facturas o cobros detiene la reanudación y devuelve la decisión al comité.
Registra	Analista de GRC, responsable del registro de decisiones.

El registro permite reconstruir la decisión tal como se tomó: qué evidencia se tenía, qué seguía pendiente y quién asumió el riesgo de actuar.

07 / EJERCICIO DE MESA

Plantilla imprimible del registro de decisiones

Use una copia por decisión. Añada la referencia de zona horaria y mantenga los identificadores de evidencia vinculados al expediente del incidente.

1. N.º de entrada	**2. Fecha, hora y zona horaria**
3. Decisión solicitada	**4. Opciones consideradas**
5. Hechos y referencias de evidencia	**6. Hipótesis, responsables y plazo de verificación**
7. Riesgo de actuar	**8. Riesgo de esperar**
9. Persona que propone	**10. Persona que autoriza y sección del plan**
11. Personas consultadas	**12. Personas informadas**
13. Evidencia preservada antes de actuar	**14. Decisión, alcance y hora**
15. Condición para revisar o suspender	**16. Persona que registra**

08 / ENTREVISTA Y PORTAFOLIO

Practique la decisión de las 08:00

PREGUNTA DE ENTREVISTA

Dos servidores de archivos están cifrados. Operaciones quiere restaurarlo todo desde la copia del domingo. Usted representa a Riesgo o Cumplimiento. ¿Qué evidencia necesita para apoyar la decisión, quién puede aprobarla y en qué condiciones se detendría la recuperación?

Una buena respuesta identifica la autoridad según el plan, distingue la fecha de la intrusión de la del cifrado, pide evidencia de contención y verificación de la copia, y separa las pruebas previas al retorno de las verificaciones que pueden continuar después. Debe mencionar la preservación de evidencia y las obligaciones de notificación que corren en paralelo.

Para un portafolio, elija un sistema y escriba media página del plan que delegue autoridad. Complete tres registros, uno para aislar, otro para preservar evidencia y otro para recuperar. En cada entrada incluya al menos un hecho con su fuente, una hipótesis con responsable y plazo, y una condición de escalamiento.

Fuentes primarias y guías

CISA y socios. Guía de #StopRansomware, edición en español, parte 2.

NIST SP 800-61 Rev. 3. Respuesta a incidentes, secciones 2.2 y 2.3 y tabla 3.

NIST Cybersecurity Framework 2.0. Edición en español.

Reglamento (UE) 2016/679. Artículos 4.12, 33 y 34.

Comité Europeo de Protección de Datos. Directrices 9/2022, apartados 20 a 23 y 32 a 35.

AEPD. Notificación de brechas de datos personales a la autoridad de control.

AEPD. Comunicación de brechas de datos personales a los interesados.

Directiva (UE) 2022/2555 (NIS2). Artículos 23 y 41.

Comisión Europea. Procedimiento de infracción INFR(2024)0270, julio de 2026.

BOE. Real Decreto-ley 12/2018, artículo 19.

BOE. Real Decreto 43/2021, capítulo IV y anexo.

Lecturas relacionadas

CS-014 Ransomware · CS-007 La cadena de ataque · CS-002 La tríada CIA · AI Assurance Engineering Skills Map, proyecto 4 (en inglés)