



La Primera Hora.

Lo que su empresa hace en los primeros sesenta minutos de un incidente cibernético.



Por qué la primera hora decide el costo de los meses siguientes

Este documento fue solicitado en el sitio de Zamak por alguien de su empresa, o le llegó reenviado. Describe lo que una empresa hace en la primera hora de un incidente cibernético y por qué esa hora decide cuánto tiempo queda detenida la operación, cuánto paga y qué se dirá de ella. Fue escrito para que lo lea quien decide, no solo quien opera, y puede reenviarse sin ningún contexto adicional.

Un ataque de ransomware rara vez comienza en el momento en que se percibe. La intrusión llega antes de la alerta, muchas veces por una credencial robada o un correo de phishing; el atacante se mueve por la red, copia datos y solo entonces cifra los sistemas. Cuando llega la alerta, el reloj que importa es el de la respuesta.

En esa hora se deciden tres cosas al mismo tiempo: cuánto tiempo queda detenida la operación, cuánto paga la empresa (en rescate, en recuperación, en multas y en contratos) y qué se dirá de ella por parte de clientes, prensa y reguladores.

La CISA, agencia de ciberseguridad de Estados Unidos, recomienda como primera acción identificar los sistemas afectados y aislarlos de inmediato, apagando un equipo solo cuando no sea posible desconectarlo de la red. El NIST, en el SP 800-61 Rev. 3 de 2025, trata la respuesta a incidentes como parte de la gestión de riesgo de la empresa, y no como tarea aislada de TI. Este playbook aplica ambas orientaciones en lenguaje de negocio.

La primera hora no es técnica. Es de decisión.

Cómo usar este documento

HOY

Léalo una vez, con calma. Nombre quién hace qué en la página 4 y complete los cuatro números en la página 5.

JUNTO AL TELÉFONO

Imprímalo, recorte la tarjeta de la página 7 y déjela con quien decide. Ese día, nadie busca un archivo.

EL DÍA DEL INCIDENTE

Abra la página 3 y siga la columna de los minutos. Una decisión por línea, sin saltar ninguna.

DESPUÉS

Lleve la página 6 a la dirección: cinco preguntas y una lista para cerrar antes de la próxima vez.



Los sesenta minutos, paso a paso

Una decisión por línea. El reloj comienza cuando alguien percibe que algo está mal, no cuando el problema se confirma.

MINUTO	QUÉ OCURRE	QUIÉN	POR QUÉ
0-5	Desconectar, sin borrar Desconectar de la red los sistemas afectados, sin borrar ni formatear nada. Apagar solo si no se puede desconectar.	Quien esté frente al sistema, con el proveedor de TI y seguridad	Interrumpe la propagación y preserva lo que la investigación va a necesitar.
5-15	Declarar el incidente Un responsable, un canal de comunicación fuera de los sistemas afectados, un registro con la hora de cada decisión.	La dirección ejecutiva	Sin un dueño, cada área decide sola y la empresa pierde tiempo y prueba.
15-30	Preservar Confirmar que los respaldos están aislados e intactos; congelar imágenes de los sistemas afectados; nada se reinicia para ver si vuelve.	Proveedor de TI y seguridad	Reiniciar puede destruir evidencia que la investigación necesita.
30-45	Llamar a los cuatro números Proveedor de TI y seguridad, aseguradora cibernética, asesoría legal y autoridad competente.	La dirección ejecutiva y finanzas	Las pólizas suelen exigir aviso rápido; las leyes de protección de datos fijan plazos; la autoridad orienta y registra.
45-55	Una sola voz La dirección define lo que la empresa dice a empleados y clientes; nadie especula ni publica en redes sociales.	Dirección y comunicación	La reputación se decide por la consistencia de lo que se dice en las primeras horas.
55-60	Decidir la hora siguiente Alcance conocido, plan de continuidad activado, quién habla con los clientes y cuándo.	Todos los responsables, en una reunión corta	Convierte la reacción en plan y devuelve a la empresa el control del reloj.



Quién hace qué

Nómbrelos hoy. Ese día, nadie tiene tiempo de discutir roles. Cada rol tiene un titular y un suplente.

ROL	RESPONDE POR	TITULAR · SUPLENTE
Quien decide	Declara el incidente, autoriza gastos y apagados, habla por la empresa. Normalmente el socio, el CEO o el director general.	TITULAR SUPLENTE
Quien contiene	Aísla, preserva evidencia y conduce la recuperación. El proveedor de TI y seguridad, con la TI interna cuando la hay.	TITULAR SUPLENTE
Quien notifica	Activa a la aseguradora, la asesoría legal y la autoridad; controla los plazos legales de notificación. Legal y finanzas.	TITULAR SUPLENTE
Quien comunica	Escribe y entrega el mensaje único a empleados y clientes. Comunicación o RR. HH., bajo la palabra de quien decide.	TITULAR SUPLENTE
Quien registra	Anota la hora de cada decisión y de cada contacto en papel o en un canal fuera de los sistemas afectados. Cualquier persona de confianza.	TITULAR SUPLENTE

La hora va bien cuando

- ◆ Hay un solo responsable y todos saben quién es.
- ◆ Los sistemas afectados están fuera de la red y nadie reinició nada.
- ◆ Los cuatro números ya fueron llamados y la hora de cada llamada está anotada.

La hora va mal cuando

- ◆ Tres personas deciden cosas distintas al mismo tiempo.
- ◆ Alguien reinició o formateó un sistema para ver si vuelve.
- ◆ Un cliente se enteró del incidente antes que la dirección.



Lo que nunca hay que hacer

- X Pagar por impulso.** La CISA y el FBI no recomiendan pagar el rescate: el pago no garantiza que los datos se descifren ni que dejen de filtrarse.
- X Reiniciar o formatear para ver si vuelve.** Destruye evidencia y puede activar la siguiente fase del ataque.
- X Borrar registros y correos sospechosos.** Son la prueba que la investigación y la aseguradora van a necesitar.
- X Publicar antes de saber.** Un mensaje público sin alcance conocido se vuelve titular y no se retira.
- X Negociar solo.** Cualquier contacto con el atacante pasa por el área legal y la aseguradora.

Los cuatro números

Complételos hoy y déjelos junto al teléfono de quien decide.

Proveedor de TI y seguridad

Quien aísla, preserva y recupera. Si la respuesta es lo vemos en el momento, es el primer número que hay que resolver.

EMPRESA

.....

NOMBRE

.....

TELÉFONO 24 H

.....

Aseguradora cibernética

La póliza suele fijar un plazo de aviso e indicar a los proveedores de respuesta. Revise el suyo.

ASEGURADORA

.....

N.º DE PÓLIZA

.....

TELÉFONO DE SINIESTROS

.....

PLAZO DE AVISO

.....

Asesoría legal

Las leyes de protección de datos, como las leyes estatales en Estados Unidos y la LGPD en Brasil, fijan plazos y obligaciones de notificación.

ESTUDIO

.....

NOMBRE

.....

TELÉFONO

.....

Autoridad competente

En Estados Unidos, el FBI recibe denuncias por el IC3; en Brasil, la unidad policial especializada en delitos cibernéticos.

ORGANISMO

.....

CANAL

.....

TELÉFONO

.....

La versión de una página para la dirección

Cinco preguntas que la dirección puede hacer hoy, antes de cualquier incidente, y cómo se ve una buena respuesta.

- 1 ¿Quién decide en la primera hora, y quién decide si esa persona no está disponible?
Dos nombres, por escrito, conocidos por toda la dirección.
- 2 ¿Cuántas horas puede quedar detenida la operación antes de convertirse en pérdida irreversible o noticia?
Un número por área crítica, y un plan de continuidad para cada una.
- 3 ¿Dónde está el respaldo, está aislado de la red, y cuándo fue la última recuperación realmente probada?
Una copia inmutable, fuera del alcance del atacante, con la fecha de la última prueba de recuperación.
- 4 ¿Quién habla por la empresa, y qué dice, en las primeras horas?
Un portavoz y un mensaje base aprobado antes de necesitarlo.
- 5 ¿Qué contratos, pólizas y leyes exigen aviso, y en cuánto tiempo?
Una lista con los plazos, revisada por legal y finanzas.

Antes de la próxima vez

- | | |
|--|--|
| ☐ Respaldo inmutable, aislado de la red, con recuperación probada y fechada | ☐ Detección y respuesta en todos los endpoints, no solo antivirus |
| ☐ Autenticación de múltiples factores en correo, acceso remoto y administración | ☐ Plan de respuesta con nombres, suplentes y un canal fuera de los sistemas |
| ☐ Póliza cibernética leída: plazos de aviso y proveedores exigidos | ☐ Un ensayo por año: una hora, en la mesa, con quienes deciden |

Tarjeta de bolsillo

Recórtela y déjala junto al teléfono de quien decide.



La Primera Hora.



0 - 5	5 - 15	15 - 30	30 - 45	45 - 55	55 - 60
Desconectar, sin borrar	Declarar el incidente	Preservar	Llamar a los cuatro números	Una sola voz	Decidir la hora siguiente

Cuatro números: proveedor de TI y seguridad · aseguradora · legal · autoridad

Cómo Zamak prepara la primera hora

Para las empresas que Zamak atiende, la primera hora comienza antes del incidente: detección y respuesta en todos los endpoints, copias de respaldo inmutables con recuperación que puede probarse, y atención en español, inglés y portugués, en el alcance que cada empresa contrata. Para empresas con TI propia, Zamak trabaja al lado del equipo como centro de operaciones y de seguridad.

Al servicio de empresas que no pueden detenerse. Microsoft Solutions Partner y Addee (N-able) Elite Group, operando con herramientas de defensa y de respaldo cuyos fabricantes están certificados en SOC 2 Type II, ISO 27001, HIPAA y PCI-DSS.

→ Conversar con un especialista de Zamak

https://www.zamakt.com/es_419/appointment

→ Calcular cuánto cuesta una hora detenida en su operación

https://www.zamakt.com/es_419/tools/downtime-calculator

→ Compartir este playbook con su dirección

https://www.zamakt.com/es_419/resources/first-hour

Fuentes: [NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management \(abril de 2025\)](#) · [CISA y FBI, #StopRansomware Guide y Ransomware Response Checklist](#)

Material educativo de Zamak Technologies. No reemplaza un plan de respuesta a incidentes diseñado para su empresa, trabajo que Zamak conduce al contratar.



Saving time, money & business reputation.

Sesenta minutos. Seis
decisiones. Una voz.



PLAYBOOK GRATUITO · ESPAÑOL · ENGLISH · PORTUGUÊS

ZAMAKT.COM/ES_419/RESOURCES/FIRST-HOUR