



O que a sua empresa faz nos primeiros sessenta minutos de um incidente cibernético.

EDIÇÃO PARA QUEM DECIDE · PORTUGUÊS



Por que a primeira hora decide o custo dos meses seguintes

Este documento foi pedido no site da Zamak por alguém da sua empresa, ou chegou até você encaminhado. Ele descreve o que uma empresa faz na primeira hora de um incidente cibernético e por que essa hora decide quanto tempo a operação fica parada, quanto ela paga e o que vai ser dito sobre ela. Foi escrito para ser lido por quem decide, não só por quem opera, e pode ser encaminhado sem nenhum contexto adicional.

Um ataque de ransomware raramente começa na hora em que é percebido. A invasão vem antes do alerta, muitas vezes por uma credencial roubada ou um e-mail de phishing; o atacante se move pela rede, copia dados e só então cifra os sistemas. Quando o alerta chega, o relógio que importa é o da resposta.

Nessa hora, três coisas são decididas ao mesmo tempo: quanto tempo a operação fica parada, quanto a empresa paga (em resgate, em recuperação, em multas e em contratos) e o que vai ser dito sobre ela por clientes, imprensa e reguladores.

A CISA, agência de cibersegurança dos Estados Unidos, recomenda como primeira ação identificar os sistemas afetados e isolá-los imediatamente, desligando um equipamento apenas quando não for possível desconectá-lo da rede. O NIST, no SP 800-61 Rev. 3 de 2025, trata a resposta a incidentes como parte da gestão de risco da empresa, e não como tarefa isolada da TI. Este playbook aplica as duas orientações em linguagem de negócio.

A primeira hora não é técnica. É de decisão.

Como usar este documento

HOJE

Leia uma vez, com calma. Nomeie quem faz o quê na página 4 e preencha os quatro números na página 5.

AO LADO DO TELEFONE

Imprima, recorte o cartão da página 7 e deixe com quem decide. No dia, ninguém procura arquivo.

NO DIA DO INCIDENTE

Abra na página 3 e siga a coluna dos minutos. Uma decisão por linha, sem pular.

DEPOIS

Leve a página 6 à diretoria: cinco perguntas e uma lista para fechar antes da próxima vez.



Os sessenta minutos, passo a passo

Uma decisão por linha. O relógio começa quando alguém percebe que algo está errado, não quando o problema é confirmado.

MINUTO	O QUE ACONTECE	QUEM	POR QUÊ
0-5	Desconectar, sem apagar Desconectar da rede os sistemas afetados, sem apagar nem formatar nada. Desligar só se não der para desconectar.	Quem estiver na frente do sistema, com o parceiro de TI e segurança	Interrompe a propagação e preserva o que a investigação vai precisar.
5-15	Declarar o incidente Um responsável, um canal de comunicação fora dos sistemas afetados, um registro com a hora de cada decisão.	A liderança executiva	Sem um dono, cada área decide sozinha e a empresa perde tempo e prova.
15-30	Preservar Confirmar que os backups estão isolados e intactos; congelar imagens dos sistemas afetados; nada é reiniciado para ver se volta.	Parceiro de TI e segurança	Reiniciar pode destruir evidências de que a investigação precisa.
30-45	Ligar para os quatro números Parceiro de TI e segurança, seguradora cibernética, assessoria jurídica e autoridade competente.	A liderança executiva e o financeiro	Apólices costumam exigir aviso rápido; leis de proteção de dados fixam prazos; a autoridade orienta e registra.
45-55	Uma só voz A liderança define o que a empresa diz a funcionários e clientes; ninguém especula nem publica em redes sociais.	Direção e comunicação	A reputação é decidida pela consistência do que é dito nas primeiras horas.
55-60	Decidir a hora seguinte Escopo conhecido, plano de continuidade acionado, quem fala com clientes e quando.	Todos os responsáveis, em uma reunião curta	Transforma reação em plano e devolve à empresa o controle do relógio.

Quem faz o quê

Nomeie hoje. No dia, ninguém tem tempo de discutir papéis. Cada papel tem um titular e um suplente.



PAPEL	RESPONDE POR	TITULAR · SUPLENTE
Quem decide	Declara o incidente, autoriza gastos e desligamentos, fala pela empresa. Normalmente o sócio, o CEO ou o diretor-geral.	TITULAR SUPLENTE
Quem contém	Isola, preserva evidência e conduz a recuperação. O parceiro de TI e segurança, com a TI interna quando houver.	TITULAR SUPLENTE
Quem notifica	Aciona seguradora, assessoria jurídica e autoridade; controla prazos legais de notificação. Jurídico e financeiro.	TITULAR SUPLENTE
Quem comunica	Escreve e entrega a mensagem única a funcionários e clientes. Comunicação ou RH, sob a palavra de quem decide.	TITULAR SUPLENTE
Quem registra	Anota a hora de cada decisão e de cada contato em papel ou em um canal fora dos sistemas afetados. Qualquer pessoa de confiança.	TITULAR SUPLENTE

A hora está indo bem quando

- ◆ Há um só responsável e todos sabem quem é.
- ◆ Os sistemas afetados estão fora da rede e ninguém reiniciou nada.
- ◆ Os quatro números já foram acionados e o horário de cada ligação está anotado.

A hora está indo mal quando

- ◆ Três pessoas decidem coisas diferentes ao mesmo tempo.
- ◆ Alguém reiniciou ou formatou um sistema para ver se volta.
- ◆ A primeira notícia do incidente chegou a um cliente antes de chegar à diretoria.



O que nunca fazer

- X Pagar por impulso.** A CISA e o FBI não recomendam pagar o resgate: o pagamento não garante que os dados sejam decifrados nem que deixem de vazar.
- X Reiniciar ou formatar para ver se volta.** Destrói evidência e pode ativar a próxima fase do ataque.
- X Apagar registros e e-mails suspeitos.** São a prova de que a investigação e a seguradora vão precisar.
- X Publicar antes de saber.** Uma mensagem pública sem escopo conhecido vira manchete e não volta.
- X Negociar sozinho.** Qualquer contato com o atacante passa pelo jurídico e pela seguradora.

Os quatro números

Preencha hoje e deixe ao lado do telefone de quem decide.

Parceiro de TI e segurança

Quem isola, preserva e recupera. Se a resposta for a gente vê na hora, é o primeiro número a resolver.

EMPRESA

.....

NOME

.....

TELEFONE 24H

.....

Seguradora cibernética

A apólice costuma fixar um prazo de aviso e indicar os fornecedores de resposta. Confira o da sua.

SEGURADORA

.....

Nº DA APÓLICE

.....

TELEFONE DE SINISTRO

.....

PRAZO DE AVISO

.....

Assessoria jurídica

Leis de proteção de dados, como a LGPD no Brasil e as leis estaduais nos Estados Unidos, fixam prazos e obrigações de notificação.

ESCRITÓRIO

.....

NOME

.....

TELEFONE

.....

Autoridade competente

Nos Estados Unidos, o FBI recebe denúncias pelo IC3; no Brasil, a delegacia especializada em crimes cibernéticos.

ÓRGÃO

.....

CANAL

.....

TELEFONE

.....

A versão de uma página para a diretoria

Cinco perguntas que a diretoria pode fazer hoje, antes de qualquer incidente, e o que uma resposta boa parece.

- 1** Quem decide na primeira hora, e quem decide se essa pessoa não estiver disponível?
Dois nomes, por escrito, conhecidos por toda a liderança.
- 2** Quantas horas a operação pode ficar parada antes de virar prejuízo irreversível ou notícia?
Um número, por área crítica, e um plano de continuidade para cada uma.
- 3** Onde está o backup, ele está isolado da rede, e quando foi a última recuperação testada de verdade?
Cópia imutável, fora do alcance do atacante, com data do último teste de recuperação.
- 4** Quem fala pela empresa, e o que diz, nas primeiras horas?
Um porta-voz e uma mensagem base aprovada antes de precisar.
- 5** Quais contratos, apólices e leis exigem aviso, e em quanto tempo?
Uma lista com os prazos, revisada pelo jurídico e pelo financeiro.

Antes da próxima vez

- | | |
|---|---|
| ☐ Backup imutável, isolado da rede, com recuperação testada e datada | ☐ Detecção e resposta em todos os endpoints, não só antivírus |
| ☐ Autenticação de múltiplos fatores em e-mail, acesso remoto e administração | ☐ Plano de resposta com nomes, suplentes e canal fora dos sistemas |
| ☐ Apólice cibernética lida: prazos de aviso e fornecedores exigidos | ☐ Um ensaio por ano: uma hora, à mesa, com quem decide |

Cartão de bolso

Recorte e deixe ao lado do telefone de quem decide.



A Primeira Hora.



0 - 5	5 - 15	15 - 30	30 - 45	45 - 55	55 - 60
Desconectar, sem apagar	Declarar o incidente	Preservar	Ligar para os quatro números	Uma só voz	Decidir a hora seguinte

Quatro números: parceiro de TI e segurança · seguradora · jurídico · autoridade

Como a Zamak prepara a primeira hora

Para as empresas que a Zamak atende, a primeira hora começa antes do incidente: detecção e resposta em todos os endpoints, cópias de backup imutáveis com recuperação que pode ser testada, e atendimento em português, inglês e espanhol, no escopo que cada empresa contrata. Para empresas com TI própria, a Zamak trabalha ao lado da equipe como centro de operações e de segurança.

A serviço de empresas que não podem parar. Microsoft Solutions Partner e Addee (N-able) Elite Group, operando com ferramentas de defesa e de backup cujos fabricantes são certificados em SOC 2 Type II, ISO 27001, HIPAA e PCI-DSS.

→ Conversar com um especialista da Zamak

<https://www.zamakt.com/appointment>

→ Calcular quanto custa uma hora parada na sua operação

<https://www.zamakt.com/tools/downtime-calculator>

→ Compartilhar este playbook com a sua diretoria

<https://www.zamakt.com/resources/first-hour>

Fontes: [NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management \(abril de 2025\)](#) · [CISA e FBI, #StopRansomware Guide e Ransomware Response Checklist](#)
Material educativo da Zamak Technologies. Não substitui um plano de resposta a incidentes desenhado para a sua empresa, trabalho que a Zamak conduz na contratação.



Saving time, money & business reputation.

Sessenta minutos. Seis
decisões. Uma voz.



PLAYBOOK GRATUITO · PORTUGUÊS · ENGLISH · ESPAÑOL

ZAMAKT.COM/RESOURCES/FIRST-HOUR