CIPHRAVERSE

CIPHRAVERSE WHITE PAPER

One-Page Incident Response Plan

A security incident does not wait for a convenient moment. If nobody has decided in advance who does what, the first hours get lost arguing instead of acting. This document is the one-page template your company needs before an incident happens, not during one.

Decisions made in advance, not during

Four questions need a written answer before an incident: who has the authority to declare one officially, who can authorise disconnecting a system or server from the network, who talks to customers and suppliers if something needs to be communicated externally, and who calls the cyber insurance provider and the company lawyer. Write a name and a backup next to each question. Without names, every decision stalls while each person waits for someone else to make it.

The contact list, on paper

If the incident affects email or the network, you will not be able to look up a phone number on the computer. Print a list with direct numbers for your IT provider, the insurer, the lawyer, the police, and the two or three internal people who need to know first. Keep a physical copy in a drawer, not only in the cloud.

The first hour

- Contain the problem without destroying evidence: disconnect the machine from the network, do not switch it off or reinstall it.
- Write down the exact time of every action and who took it, on paper or in a separate document.
- Do not wipe or reinstall anything until someone with technical judgement authorises it.
- Activate the contact list and notify whoever needs to decide the next steps.

Personal data and an annual rehearsal

Assess as soon as possible whether the incident affected personal data belonging to customers or employees. Article 33 of the GDPR requires notifying the data protection authority within 72 hours if it did, and the AEPD's Asesora Brecha tool helps decide whether your case requires it. Finally, rehearse this plan once a year with your team: the first time it gets read cannot be in the middle of a real incident.