
Digeat N.2 - 19 Giugno 2024

# I documenti “non digitali” come argine per la sicurezza

*Di Cesare Gallotti*

## Abstract

Nel 2014, l’autorevole NIST, US National Institute of Standards and Technology, pubblicò il NIST Cybersecurity Framework (CSF) per fornire alle organizzazioni un punto di riferimento per la sicurezza dei sistemi informatici o, più in generale, dei sistemi digitali. È quindi possibile tracciare una data da quando si cominciò a parlare sempre più di “ciber-sicurezza” e sempre meno di “sicurezza informatica” e di “sicurezza delle informazioni”. In realtà il termine “ciber-sicurezza” è in uso da molto prima, più spesso con scrittura inglese (“cyber-security”) o mista (“cyber-sicurezza”). Questo per il valido motivo che è necessario occuparsi non solo dei sistemi informativi, ossia, intuitivamente, quelli usati per elaborare documenti, ma anche dei cosiddetti *sistemi operativi*, che controllano gli impianti industriali, gli impianti di distribuzione di acqua, gas ed elettricità, i dispositivi di automazione della casa o di appartamenti, eccetera. Infatti sono noti diversi incidenti che li hanno coinvolti, come il blocco, nel 2016, di un sistema di termoregolazione in un condominio finlandese, il blocco, nel 2021, di un impianto di trattamento dell’acqua in Florida, l’accesso non autorizzato, nel 2023, ai sistemi di ABB in Svizzera. Questa attenzione alle ciber-minacce, per contro, ha ridotto quella verso i documenti non digitali, peraltro ancora molto importanti, non solo perché usati per trattare informazioni critiche, ma perché possono essere essi stessi una misura di sicurezza.

## Indice



I documenti non digitali sono molto importanti e possono essere essi stessi una misura di sicurezza.

## Il valore dei documenti non digitali

La scrittura ha circa 10.000 anni e, tranne che negli ultimi 20, ha usato supporti non digitali: pietra, tavolette di argilla, fogli di papiro, pelli, fogli di carta.

> Ancora oggi è più pratico leggere alcuni testi in formato cartaceo, per la possibilità di guardare quasi contemporaneamente più pagine o di sottolineare e prendere appunti a margine immediatamente riconoscibili. I libri cartacei non hanno funzionalità che possono distrarre il lettore e di sicuro non presentano problemi legati alla batteria.

Nelle scuole, dopo anni di **positivismo digitale**, sono molti i casi di ritorno ai supporti cartacei. Sono anche molte le riflessioni in merito alla validità degli investimenti in strumenti digitali (come le LIM, lavagne interattive multimediali) che forse **non hanno portato a reali miglioramenti nella didattica e dell'imposizione di strumenti digitali a minori non consapevoli dei rischi**, per non parlare, spesso, dei genitori.

È importante considerare anche **il fattore temporale dei documenti non digitali**, **legato alla loro validità**. Innanzi tutto, bisogna riflettere sul fatto che hanno dimostrato una notevole resistenza al passare del tempo, caratteristica tutta da dimostrare per i formati digitali. Inoltre, un documento firmato a mano ha valore anche dopo molti anni, a meno di non perderlo.

Un documento firmato digitalmente deve essere **sottoposto a verifiche periodiche** per evitare che la sottoscrizione perda di valore perché basata su tecnologie obsolete e vulnerabili. Da ricordare che anche i documenti firmati digitalmente possono essere persi, sia perché archiviati male sia per malfunzionamenti ai sistemi informatici.

## I documenti non digitali come misure di sicurezza

> È possibile usare i documenti digitali come misura di sicurezza. La fisicità del documento presenta alcune caratteristiche intrinseche tali da rendere meno efficienti gli attacchi, rispetto a quelli condotti in ambito digitale.

La prima caratteristica è **ovviamente la necessità di dover essere fisicamente dove si trovano gli obiettivi**. Questo richiede soldi per viaggiare e allenamento fisico e mentale per avvicinarsi all'obiettivo, eludere telecamere e personale di vigilanza.

La seconda, collegata alla precedente, riguarda **mezzi e strumenti non reperibili facilmente**. Certamente si possono reperire molti strumenti sui vari negozi, leciti e illeciti, online e fisici, ma i costi sono più elevati rispetto ai software disponibili anche gratuitamente, non tutti sono facilmente reperibili e i tempi di consegna possono essere imprevedibili.

La terza riguarda **l'impatto psicologico dell'attaccante**: un conto è nascondersi dietro una tastiera, un altro è mettersi in gioco in prima persona. L'effetto "filtro" è ben noto, soprattutto quando si parla di "leoni da tastiera", ossia persone che intervengono in modo aggressivo e maleducato nei dibattiti online perché il filtro del canale informatico fa perdere la percezione di umanità nelle altre persone ( questo perché non le si vede e non si attivano i neuroni a specchio). Accanto a questo bisogna ricordare che aggredire fisicamente un'altra persona o attaccare un sito per rubare o distruggere documenti è molto più pericoloso perché le reazioni dell'altra parte possono essere molto violente.

Infine, la presenza fisica **fa perdere l'anonimato** che è molto più semplice da mantenere nel mondo digitale.

Questi quattro elementi rendono più difficili gli attacchi sia da parte di aggressori esterni (che devono quindi intrufolarsi in un sito fisico, permanerci e poi uscirci), ma anche da interni, che possono essere sempre notati, anche quando copiano o fotografano documenti riservati.

Anche l'alterazione di un documento è solitamente identificabile, ma è necessario ricordare che sono molti i falsi in circolazione e, quindi, il supporto non digitale non mette al riparo da questa minaccia.

**Il documento cartaceo può quindi essere usato in esclusiva e per alcune occasioni**. Uno degli esempi più noti, avvolto da un alone di mistero, è quello della segretissima ricetta della Coca Cola, che non sembra essere su alcun supporto digitale.

## La sicurezza dei documenti non digitali

Negli Anni Novanta fu pubblicata la **BS 7799**, norma britannica che presentava controlli di sicurezza per le informazioni, in formato digitale e non digitale. Oggi quella norma è nota nelle sue versioni **ISO/IEC 27001** (requisiti per un sistema di gestione per la sicurezza delle informazioni) e **ISO/IEC 27002** (controlli per la sicurezza delle informazioni).

Già all'epoca erano disponibili riferimenti autorevoli per la sicurezza informatica, ma la BS 7799 non voleva limitarsi al digitale, perché i processi di gestione delle informazioni vanno considerati nel loro insieme: **le informazioni potrebbero essere ben protette in formato digitale, ma vulnerabili se stampate o dette a voce ad altri**. A questo proposito è interessante il caso del dossier compilato da Mitrokhin, un membro del KGB che copiava ogni giorno piccole parti di informazioni, disponibili presso le sedi super protette del KGB e, tornato a casa, le nascondeva.

La BS 7799 proponeva controlli per l'archiviazione sicura dei documenti non digitali (con riferimenti anche al controllo della temperatura e dell'umidità degli archivi e degli accessi fisici), per la distruzione di ogni tipo di supporto, per la gestione, in termini di classificazione ed etichettatura, di tutte le informazioni, per la disponibilità per tutti i formati, eccetera. Questo approccio è stato ereditato dalle ISO/IEC 27001 e ISO/IEC 27002.

Altre norme sono state elaborate per i formati non solo digitali, come la ISO 15489 sulla gestione degli archivi. La norma ISO/IEC 21964 (Destruction of data carriers) è dedicata alla distruzione dei supporti fisici.

La normativa sulla protezione dei dati (e in particolare il GDPR), infine, non distingue tra protezione dei dati in formato digitale e non. Questo vuol dire che vanno assicurati livelli di sicurezza equivalenti alle medesime informazioni, anche se su supporti diversi, non solo a quelle in formato digitale. Questo richiede attenzione anche quando si cambia il formato delle informazioni, per esempio quando si digitalizzano documenti cartacei e quando si stampano quelli digitali, perché ne va assicurato lo stesso livello di riservatezza, integrità e disponibilità.

## Conclusioni

Questo articolo ha voluto riflettere sul fatto che è possibile usare il formato non digitale per aumentare, in alcuni casi, il livello di sicurezza delle informazioni e/o la loro fruibilità. La spinta alla digitalizzazione, pertanto, non sempre porta miglioramenti e va quindi promossa con attenzione.

---

**Note**

NIST

Con riguardo agli incidenti menzionati nell'abstract:

- Finlandia, 2016
- Florida, 2021
- Svizzera, 2023