

QUADERNO III

L'EREDITÀ DIGITALE

Memoria, accesso e successione nell'era della proprietà digitale

Ciò che non può essere compreso
non può essere trasmesso davvero.



FLORIANO RIGHETTI

L'Eredità Digitale

Quaderni di Custodia Digitale · Quaderno III

Floriano Righetti

Edizione definitiva · settembre 2026

© 2026 Floriano Righetti

Tutti i diritti riservati.

florianorighetti.ch

Questo quaderno ha finalità culturali e informative. Non costituisce consulenza finanziaria, legale, fiscale o d'investimento. Le indicazioni vanno valutate rispetto agli strumenti e alle circostanze concrete.

Non inserire segreti reali nei modelli del libro. I documenti compilati restano riservati anche quando non contengono credenziali. Le scene narrative sono esempi illustrativi.

Testo e riferimenti verificati il 12 settembre 2026.

ESTRATTO GRATUITO

Capitolo 3: Il segreto e le istruzioni (pp. 16-20).

Il testo e la numerazione delle pagine riproducono l'edizione integrale. L'indice presenta il libro completo: i capitoli non inclusi in questa anteprima non sono collegati.

La pagina finale rimanda alla scheda del quaderno sul sito dell'autore.

Indice

Nota al lettore.....	4
Prologo	5
1 Quando il proprietario non risponde	8
2 Che cosa si eredita davvero.....	12
3 Il segreto e le istruzioni.....	16
4 Famiglia, eredi e persone fidate.....	21
5 Aziende e continuità operativa.....	27
6 La procedura di attivazione.....	33
7 Trasmettere senza consegnare troppo presto	39
Scenari di continuità	45
Chiusura.....	48
Glossario minimo	50
Appendice operativa.....	52
Fonti e approfondimenti.....	68
Nota di chiusura della trilogia	69

Nota al lettore

Questo terzo quaderno chiude la trilogia iniziale dei Quaderni di Custodia Digitale. Il primo quaderno, *La Custodia*, ha posto una domanda: chi controlla davvero l'accesso? Il secondo, *La Proprietà Digitale*, ha chiesto che cosa significhi possedere qualcosa che non si può toccare. Questo quaderno porta entrambe le domande nel punto più umano e più fragile: che cosa accade quando il proprietario non può più agire?

Il tema principale è la successione dopo la morte. Accanto a essa, il quaderno esamina l'incapacità temporanea e la continuità aziendale: situazioni che possono interrompere gli stessi accessi, ma non attribuiscono gli stessi diritti. Una malattia, un'assenza o un conflitto non aprono una successione. Per ciascun caso occorrono presupposti, persone autorizzate e limiti distinti.

Il problema riguarda wallet, domini, email, cloud, archivi familiari, licenze, account social e sistemi di lavoro. Alcuni fornitori prevedono procedure per decesso o recupero; altri richiedono percorsi diversi. La preparazione collega queste possibilità senza presumere che un unico account o documento possa risolverle tutte.

La frase guida è semplice: ciò che non può essere compreso non può essere trasmesso davvero. Nel digitale, infatti, consegnare un oggetto non basta sempre. Un telefono bloccato non è accesso. Un hardware wallet senza contesto non è patrimonio leggibile. Una seed phrase senza istruzioni può essere tanto pericolosa quanto inutile. Un account aziendale senza ruoli chiari può creare conflitto. Una cartella cifrata senza chiave può diventare memoria perduta.

Preparare l'eredità digitale non significa consegnare tutto oggi. Significa costruire una strada legittima per domani. Una strada che separi contesto e segreto, informazione e potere, memoria e accesso, diritto e capacità tecnica. Una strada che protegga il presente senza tradire il futuro.

3 Il segreto e le istruzioni

Il falso conforto della lista dei segreti

L'errore più pericoloso dell'eredità digitale è credere che tutto si risolva scrivendo i segreti. Password, seed phrase, PIN, codici di recupero, chiavi, frasi, file, combinazioni. Mettere tutto in un documento, in una busta, in una cartella, in un messaggio, in un foglio. Sembra la soluzione più diretta: se domani non posso parlare, qualcuno troverà ciò che serve.

Il segreto dà potere. Chi possiede una seed phrase può forse controllare un wallet. Chi possiede una master password può forse entrare in un password manager. Chi possiede codici e accessi può forse raggiungere account, dati, asset, documenti. Consegnare segreti significa consegnare possibilità operative, e nel digitale la possibilità operativa può essere irreversibile, invisibile e difficile da contestare dopo il fatto.

D'altra parte, non lasciare nulla può essere altrettanto distruttivo. Il segreto assoluto protegge il presente e può tradire il futuro. Una chiave che nessuno troverà mai non è più sicurezza. È perdita programmata. Una procedura che vive solo nella memoria del proprietario non è discrezione. È dipendenza biologica. Un patrimonio digitale completamente muto non è custodito. È sepolto.

Contesto e segreto

Il contesto deve essere recuperabile dalle persone appropriate. I segreti devono restare protetti fino a un uso autorizzato.

Il contesto dice che cosa esiste, perché conta, quale categoria ha, chi può aiutare, quali errori evitare, quali passaggi non improvvisare. Il segreto permette di agire. Confondere i due livelli crea problemi opposti. Se il contesto è nascosto come un segreto, il futuro non capirà. Se il segreto è esposto come contesto, il presente diventa vulnerabile.

Sapere che esiste un wallet non significa poterlo svuotare. Sapere che esiste un archivio cifrato non significa poterlo aprire subito. Sapere che un dominio è importante non significa poterlo trasferire. Sapere quale professionista contattare non significa avere accesso diretto ai beni. Questa separazione è la differenza tra preparare e consegnare troppo presto.

I cinque livelli

Possiamo immaginare cinque livelli. Il primo livello è l'esistenza: qualcuno deve sapere che certi beni digitali importanti esistono. Il secondo è il contesto: qualcuno deve sapere perché contano e a quale categoria appartengono. Il terzo è l'istruzione: qualcuno deve sapere quali passaggi seguire e quali errori evitare. Il quarto è il segreto: chiavi, password, codici, seed, accessi. Il quinto è l'autorizzazione: le condizioni in cui il segreto può essere usato legittimamente.

I livelli possono essere separati tra documenti, luoghi e persone, se la struttura resta sostenibile. Una busta sigillata segnala un'eventuale apertura ma non impedisce materialmente al detentore di leggere il contenuto. Istruzioni e vincoli giuridici vanno distinti dai controlli tecnici: scrivere «aprire solo dopo» non rende una chiave inutilizzabile prima.

Documenti, istruzioni e potere dormiente

Il documento di contesto descrive categorie, titolarità da verificare, priorità, account radice, contatti e azioni da evitare. Non deve contenere password, seed phrase o codici di recupero. Resta comunque riservato: nomi di servizi, patrimoni, ubicazioni e persone possono aiutare un attaccante.

Un buon documento di contesto può dire: esistono wallet e asset digitali; non inserire mai parole di recupero online; non chiedere aiuto su forum pubblici; non formattare dispositivi; contattare questa persona o questo professionista; verificare prima la legittimità; distinguere asset personali e aziendali; cercare istruzioni sigillate in un certo luogo. Non apre la porta. Impedisce di aprire quella sbagliata.

Il documento di istruzione è più operativo. Può indicare una sequenza: mettere al sicuro dispositivi, recuperare documenti, identificare account critici, contattare ruoli, verificare condizioni, aprire eventuali buste o depositi solo con persone autorizzate, documentare ogni azione. Anche qui, non è detto che debba contenere segreti diretti. Può indicare dove e come accedervi secondo condizioni stabilite.

I segreti richiedono strumenti e procedure adeguati al loro tipo. Le password possono essere gestite in un sistema cifrato con un recupero verificato; seed phrase e chiavi destinate alla custodia offline non vanno fotografate o trascritte in servizi online per comodità. Il progetto deve considerare sia chi possa accedere alle copie sia chi possa recuperarle legittimamente.

L'autorizzazione è il livello più trascurato. Quando può essere usato un segreto? Da chi? Con quale verifica? In presenza di quale evento? Con quale supervisione? Per fare cosa? Un segreto senza autorizzazione crea ambiguità. Chi lo trova potrebbe pensare di poter agire. Chi lo custodisce potrebbe essere tentato, accusato, confuso o sovraccaricato. Una buona procedura non lascia al segreto il compito di decidere quando essere usato.

Un percorso semplice può comprendere un inventario riservato, istruzioni di recupero e referenti informati. Se un gestore di password offre accesso di emergenza, occorre verificarne disponibilità, condizioni, attesa e poteri concessi: non tutti i servizi lo prevedono e non sostituisce il titolo giuridico per agire.

L'eccesso di complessità può essere pericoloso quanto l'assenza di procedura. Se le istruzioni sono troppo difficili, gli eredi le ignoreranno o le interpreteranno male. Se richiedono strumenti che nessuno possiede, resteranno teoria. Se coinvolgono troppe persone senza ruoli chiari, genereranno conflitto. Se sono troppo tecniche, diventeranno opache. Una procedura di eredità digitale deve essere abbastanza robusta da proteggere e abbastanza semplice da essere seguita in un momento difficile.

Bisogna scrivere per persone sotto stress. Questa è una regola pratica. Chi leggerà le istruzioni potrebbe essere nel lutto, in ospedale, in una crisi aziendale, in conflitto familiare, sotto pressione economica. Non leggerà come un tecnico calmo in laboratorio. Leggerà cercando di non sbagliare. Le istruzioni devono essere ordinate, sobrie, prive di ambiguità inutili, capaci di dire anche quando fermarsi.

Quando non procedere

Non procedere se non è chiara la legittimità. Non procedere se manca una persona indicata. Non procedere se un sito chiede una seed phrase. Non procedere se non si è certi della rete o dell'indirizzo. Non procedere se il bene potrebbe essere aziendale e non personale. Non procedere se il contenuto è sensibile e non riguarda chi lo sta aprendo. Non procedere se una decisione può essere irreversibile e il quadro legale non è chiaro.

Questo tipo di frasi può sembrare prudente fino all'eccesso, ma nel digitale l'irreversibilità è spesso nascosta dentro interfacce ordinarie. Un click può cancellare. Una firma può trasferire. Un cambio password può bloccare altri accessi. Un export può esporre dati. Un trasferimento può essere definitivo.

Una vendita può generare obblighi. Una chiusura account può perdere prove.

Il problema della buona volontà è che agisce. Vuole aiutare, risolvere, recuperare, sistemare. Ma senza contesto, la buona volontà può distruggere. Un familiare può cancellare file privati pensando di rispettare la privacy e perdere documenti necessari. Un socio può trasferire asset per metterli al sicuro e creare un conflitto. Un tecnico può forzare un accesso e violare limiti. Un erede può vendere token senza capire che rappresentano altro. La procedura serve a rallentare la buona volontà fino a farla diventare azione legittima.

Persone, ruoli e manutenzione

Persona fidata non significa persona adatta a ogni funzione. Fiducia personale, competenza tecnica e autorizzazione sono qualità distinte. Un socio può avere poteri sui servizi aziendali senza averne sul patrimonio privato; un tecnico può assistere senza decidere la destinazione dei beni.

Questa separazione non è freddezza. È protezione delle relazioni. Quando i ruoli sono confusi, le persone possono essere accusate, sovraccaricate o tentate. Quando i ruoli sono chiari, ciascuno sa cosa deve sapere, cosa può fare e dove deve fermarsi. La chiarezza riduce conflitto.

Il documento di contesto può quindi indicare ruoli senza consegnare potere. Può dire: per questioni tecniche, contattare questa persona; per questioni legali, rivolgersi a questo professionista; per beni aziendali, coinvolgere questo ruolo; per archivi familiari, parlare con questi familiari; per wallet, non agire senza verifica. La mappa non apre i forzieri. Evita che gli eredi cerchino le chiavi nel posto sbagliato.

Nel caso delle aziende, la distinzione tra contesto e segreto è ancora più importante. Un fondatore può non voler condividere ogni chiave durante la vita operativa, ma l'azienda deve sapere quali asset critici esistono e quali procedure si attivano in emergenza. Domini, DNS, repository, cloud, licenze, wallet, account pubblicitari, marketplace: non possono dipendere solo dalla memoria di una persona. Il documento di contesto aziendale può essere accessibile a ruoli autorizzati senza contenere segreti diretti.

Nel caso familiare, invece, il contesto deve proteggere dal panico e dalla curiosità. Non tutto deve essere letto subito. Non ogni archivio deve essere aperto. Non ogni account personale deve diventare pubblico. L'eredità digitale include anche privacy postuma, rispetto della memoria e selezione.

Lasciare istruzioni può significare dire: questo archivio è personale, non aprirlo se non per necessità; questo altro contiene documenti importanti; questo account va chiuso; questo profilo può essere memorializzato.

Documento vivo

Quando cambia una relazione, aggiornare i nominativi non basta se sono già stati condivisi segreti. Occorre verificare deleghe, sessioni e credenziali; se una chiave privata è stata esposta, non si può ritirarne la copia cancellando un nome dal documento. La messa in sicurezza richiede un intervento adatto al sistema e agli asset controllati.

Il documento di contesto dovrebbe avere data, versione e indicazione di validità. Una procedura vecchia può essere più pericolosa di nessuna procedura, perché dà sicurezza falsa. Se indica persone non più appropriate, luoghi cambiati, account chiusi, asset trasferiti, strumenti obsoleti, può orientare male proprio quando serve chiarezza.

La manutenzione dell'eredità digitale non deve essere continua, ma periodica. Dopo eventi importanti: matrimonio, separazione, nascita, morte, vendita aziendale, aumento di patrimonio, nuovo wallet, cambio provider, uscita di un socio, trasferimento di domicilio, cambio di professionista, nuove licenze, nuovo dominio. Ogni evento che cambia relazioni dovrebbe interrogare la procedura.

Una procedura operativa non sostituisce testamento, mandato, poteri societari o altri titoli richiesti. Deve essere coerente con questi documenti e con i limiti di accesso ai dati. La verifica professionale riguarda anche gli atti apparentemente semplici quando incidono su diritti altrui.

Ma la verifica professionale ha bisogno di materia. Un consulente può aiutare meglio se esiste una mappa. Un notaio può ragionare meglio se i beni sono identificati. Un tecnico può intervenire meglio se sa quali strumenti sono rilevanti. Una famiglia può evitare panico se sa chi contattare. Preparare contesto non è sostituire la legge. È permettere alla legge, alla tecnica e alla famiglia di non partire dal buio.

La lettura continua

L'Eredità Digitale

Floriano Righetti · Quaderno III

Hai letto un estratto dell'edizione definitiva di settembre 2026. Nella scheda del quaderno trovi la presentazione del volume e gli aggiornamenti sulla sua disponibilità.

SCOPRI IL QUADERNO

florianorighetti.ch/it/quaderni/eredita-digitale

Sette quaderni, un percorso

Custodia, proprietà digitale, eredità, chiavi private, wallet, cold storage e fiducia.

[Esplora la collana completa](#)