

81+

SICURISSIMO OS

LA TUA AZIENDA. SEMPRE SOTTO CONTROLLO.

I 7 BLACK HOLES DELLA GESTIONE AZIENDALE

Dove evapora tutto il tuo utile netto

CAUSE • ESEMPI REALI • CHECKLIST • SOLUZIONI



DOSSIER STRATEGICO GRATUITO

STRUMENTI PRATICI PER UNA PMI PIÙ FORTE

MENO CAOS
PIÙ TEMPO
PIÙ MARGINE
PIÙ LIBERTÀ

Perché questo ebook esiste SICURISSIMO OS parte da un problema semplice: l'azienda possiede dati, persone, documenti, software e processi, ma raramente qualcuno possiede nello stesso momento una vista completa, aggiornata e verificabile di tutto.

Il dossier allegato descriveva sette buchi neri con forte focus cantieri e appalti: fornitori, scadenze, registri dispersi, cambio gestionale, micro-gestione, direzione e margini. Questa edizione li trasforma in un modello universale per PMI e professionisti di ogni settore.

NON È UN EBOOK SULLA SOLA SICUREZZA. È UNA MAPPA DEI PUNTI IN CUI TEMPO, DENARO, CONOSCENZA,

RESPONSABILITÀ E DECISIONI SI PERDONO.

Lo schema globale di SICURISSIMO OS Sorgenti → PIPELINE81+ → PROOF81+ → Neuralog → Digital Twin → Cortex → Control Tower. Nessun cerchio con linee sovrapposte: il dato attraversa una catena leggibile e verificabile.

- PIPELINE81+ ingerisce, classifica e normalizza.
- PROOF81+ conserva Evidence, qualità, certezza e freshness.
- Neuralog costruisce memoria e relazioni.
- Digital Twin rappresenta la realtà aziendale.
- Cortex analizza e propone.
- Control Tower mostra KPI, alert, workflow e azioni.

Come funzionano moduli e workflow Mycelium collega moduli autonomi tramite capability ed eventi. Operations, compliance, economics e knowledge restano domini separati ma coordinati. Questo riduce il rischio di creare un monolite ingestibile.

EVENTO → OWNER → REGOLA → AZIONE → EVIDENCE → ESITO → APPRENDIMENTO

Il funnel operativo: dal caos all'azione Prima visibilità, poi verifica, poi contesto. L'automazione viene dopo. Il sistema non deve trasformare una chat, una foto o un nome file in verità senza un livello di prova adeguato.

7W81+: il contesto obbligatorio Ogni problema, scadenza, documento, costo o decisione deve rispondere a: PERCHÉ, COSA, COME, DOVE, QUANDO, PER CHI, CON CHI. È il filtro che impedisce task senza scopo, alert senza owner e KPI senza decisione.

BLACK HOLE #1 · FORNITORI & ACQUISTI

Riconciliazione cieca

PROBLEMI REALI

- Ordini, DDT, fatture e pagamenti non allineati • Prezzi o quantità incoerenti • Duplicati e note credito scollegate • Costi attribuiti alla commessa sbagliata • Fornitori critici e dipendenze invisibili

LE 7W

7W x 7 BLACK HOLES							
Fornitori	✓	✓	✓	✓	✓	✓	✓
Scadenze	✓	✓	✓	✓	✓	✓	✓
Conoscenza	✓	✓	✓	✓	✓	✓	✓
Software	✓	✓	✓	✓	✓	✓	✓
Tempo	✓	✓	✓	✓	✓	✓	✓
Direzione	✓	✓	✓	✓	✓	✓	✓
Margine	✓	✓	✓	✓	✓	✓	✓
	Perché	Cosa	Come	Dove	Quando	Per chi	Con chi

- Perché: evitare che differenze e duplicati diventino costo.
- Cosa: ordini, listini, DDT, fatture, pagamenti, banca.
- Come: three-way match, anomaly detection, Evidence, human review.
- Dove: ERP, email, Sdl/export, magazzino/cantiere, banca.
- Quando: ordine, consegna, fattura, scadenza, pagamento.
- Per chi: acquisti, amministrazione, commessa, direzione.
- Con chi: fornitore, banca, magazzino, consulenti.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

BLACK HOLE #2 · SCADENZE & OBBLIGHI

Una data non è compliance

PROBLEMI REALI

• Sicurezza e formazione • INPS/INAIL e lavoro • Fisco e camerale • Privacy e cyber • Autorizzazioni, ambiente, assicurazioni, asset

LE 7W

- Perché: sapere cosa si applica davvero.
- Cosa: obbligo, fonte, documento, Evidence, rischio.
- **Come: MATRIX81+ → LEX81 → PROOF81+ → Alert.**
- Dove: azienda, sede, cantiere, territorio, ente.
- Quando: statico, condizionale, periodico, evento, continuo.
- Per chi: impresa, lavoratori, clienti, PA.
- Con chi: owner interno, professionista, ente competente.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

BLACK HOLE #3 · CONOSCENZA DISPERSA

L'azienda non sa dove sa

PROBLEMI REALI

• File introvabili e duplicati • Foto scollegate dal contesto • Email, PEC e chat non collegate a oggetti • Know-how nelle persone • NAS, PC, USB e cloud separati

LE 7W

- Perché: ridurre ricerca e dipendenza dalle persone.
- Cosa: file, messaggi, immagini, documenti, metadati.
- Come: Source Twin + Knowledge Map + Neuralog.
- Dove: server, NAS, PC, cloud, app autorizzate.
- Quando: ingest, modifica, evento, richiesta.
- Per chi: chi deve trovare e usare la conoscenza.
- Con chi: owner del dato e soggetti autorizzati.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

BLACK HOLE #4 · SOFTWARE ISOLATI

Cambiare tutto non è una strategia

PROBLEMI REALI

• Doppio inserimento • Export/import manuali • Lock-in • Workflow separati dalla memoria • AI confinata a una chat

LE 7W

- Perché: evitare che le persone facciano da ponte.
- Cosa: ERP, contabilità, paghe, HSE, DMS, BI, banche.
- Come: Connector81 + Mycelium + API/eventi.
- Dove: sistemi esistenti on-premise o cloud.
- Quando: collegare prima; sostituire solo se utile.
- Per chi: PMI che non vogliono ripartire da zero.
- Con chi: vendor, IT, consulenti, owner di processo.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

BLACK HOLE #5 · TEMPO & MICRO-GESTIONE

Il telefono diventa workflow

PROBLEMI REALI

• Telefonate di verifica • Solleciti ripetuti • Riunioni per ricostruire lo stato • Rapportini incompleti • Ricerca manuale delle prove

LE 7W

- Perché: liberare attenzione manageriale.
- Cosa: richieste, task, owner, stati, deadline.
- Come: WORK81 + Event81 + Alert81 + Cortex.
- Dove: ufficio, cantiere, reparto, PWA.

• **Quando: evento → owner → azione → esito.**

- Per chi: direzione, coordinatori, team.
- Con chi: chi esegue, approva, controlla, viene informato.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

BLACK HOLE #6 · DIREZIONE AL BUIO

Dati senza sintesi

PROBLEMI REALI

- Report tardivi • KPI manuali • Anomalie scoperte tardi • Priorità confuse • Decisioni senza fonte

LE 7W

- Perché: concentrare l'attenzione su ciò che conta.
- Cosa: KPI, rischi, cash, scadenze, capacity, eccezioni.
- Come: Control Tower + Executive81 + Cortex.
- Dove: dashboard web/PWA e briefing.
- Quando: eventi + rollup giornalieri/settimanali.
- Per chi: imprenditore, direzione, responsabili.
- Con chi: owner dei processi e revisori.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

BLACK HOLE #7 · MARGINE, CASH & BANCHE

Fatturato ≠ utile ≠ cassa

PROBLEMI REALI

- Costi non attribuiti • Crediti scaduti • Debiti imminenti • Movimenti bancari non riconciliati • Pricing senza margine minimo

LE 7W

- Perché: vedere redditività e liquidità reale.
- Cosa: costi, ricavi, fatture, crediti, debiti, banca.
- Come: Cost81 + Cash81 + Profit81 + Forecast81.
- Dove: commessa, cliente, servizio, conto, centro di costo.

• **Quando: preventivo → costo → fattura → cash → forecast.**

- Per chi: direzione, amministrazione, commerciale.

- Con chi: clienti, fornitori, banca, consulenti.

SICURISSIMO non promette che il problema sparisca da solo: rende visibile la catena, assegna owner, collega Evidence e trasforma l'eccezione in workflow.

Le 12 famiglie di problemi

FAMIGLIA

PROBLEMA

CAPABILITY

1. Caos informativo

ricerca, duplicati, versioni, know-how FILESYSTEM81+ · Neuralog

2. Software isolati

export/import, doppio inserimento, lock-in Mycelium · Connector81

3. Compliance 360

obblighi e scadenze multi-dominio

MATRIX81+ · LEX81 · PROOF81+

4. Operations

task, rapportini, commesse, eventi WORK81 · Event81

5. Procurement

fornitori, DDT, ordini, fatture Procurement · Cash Chain

6. Finanza

crediti, debiti, banca, forecast Cash81 · Forecast81

7. Marginalità

costi reali e profitto per causa Cost81 · Profit81

8. Persone

ruoli, competenze, owner, key person People/Role DNA

9. Asset

mezzi, macchine, impianti, software Asset81 · Maintenance

10. Direzione

KPI, priorità, anomalie, report Control Tower · Executive81

11. AI affidabile

contesto, permessi, hallucination Cortex · PROOF81+

12. Decision→Action

decisioni senza follow-up Mycelium · Workflow · Audit I 7 Black Holes sono il linguaggio commerciale. Le 12 famiglie sono il modello operativo. MATRIX81+ collega i due livelli.

Company Health: non un solo numeretto Il radar è un esempio di come SICURISSIMO può mostrare equilibrio e fragilità tra domini. La torta è un esempio di analisi del tempo perso: i valori sono dimostrativi e devono essere sostituiti dai dati reali dell'azienda.

- Health Score con Evidence insufficiente = UNKNOWN, non un numero inventato.
- Maslow aziendale: prima sopravvivenza/liquidità e sicurezza, poi crescita.
- Life Wheel aziendale: cash, clienti, persone, operations, compliance, asset, data, cyber, qualità, crescita, leadership.

Comparazione: non sostituire, orchestrare

FAMIGLIA

FORTE SU

LIMITE TIPICO

RUOLO IN SICURISSIMO

ERP / contabilità Transazioni, amministrazione Contesto operativo spesso separato Fonte economica integrata HSE / compliance Verticalità normativa Non copre tutta l'azienda Capability specialistica DMS / cloud Archivio e collaborazione Non interpreta il business Sorgente della Knowledge Map BI / dashboard Visualizzazione KPI Dipende da dati già puliti Read model della Control Tower Automation Trigger e workflow Memoria/ontologia limitate Esecuzione tramite Mycelium AI assistant Sintesi e linguaggio Contesto/permission non sempre completi Cortex con Evidence IL POSIZIONAMENTO PIÙ FORTE NON È 'SIAMO MEGLIO DI TUTTI'. È: COLLEGHIAMO CIÒ CHE GIÀ FUNZIONA E

AGGIUNGIAMO IL COMPANY BRAIN.

Per chi è SICURISSIMO OS • PMI e studi professionali con documenti, scadenze e informazioni sparse.

- Aziende che usano già più software e non vogliono ricominciare da zero.
- Imprese con commesse, cantieri, sedi, mezzi, fornitori o processi distribuiti.
- Direzioni che vogliono una Control Tower e un Digital Twin progressivo.
- Organizzazioni che vogliono AI con fonti, Evidence, permessi e audit.
- Aziende che vogliono collegare compliance, operations, economics e knowledge.

PER CHI NON È

- Chi cerca una promessa di rischio zero, zero multe o profitto garantito.
- Chi vuole che l'AI prenda decisioni sensibili senza policy o controllo umano.
- Chi non è disposto a collegare o rendere accessibili in modo autorizzato le proprie sorgenti.
- Chi pretende risultati senza qualità dei dati, owner di processo e verifica.
- Chi vuole sostituire professionisti legali, fiscali, del lavoro o tecnici con una chat.

Le obiezioni più difficili È troppo complesso.

L'architettura può essere complessa; l'esperienza deve essere semplice: Control Tower, ricerca, workflow, scadenze, Cortex.

Devo cambiare gestionale?

No come requisito iniziale. Connect-before-replace: si collega prima, si sostituisce solo dove genera valore.

E i miei dati?

Il modello prevede tenant isolation, permessi, audit e connector read-only di default dove applicabile.

L'AI può sbagliare?

Sì. Per questo fatti, dichiarazioni, inferenze e azioni restano separati e PROOF81+ governa la certezza.

Quanto tempo fa risparmiare?

Va misurato. Il dossier allegato usa 15 ore/settimana come promessa commerciale; questa edizione lo tratta come ipotesi da verificare sul processo reale.

Sostituisce consulenti?

No. Organizza dati, Evidence e workflow; le decisioni professionali riservate restano ai soggetti competenti.

Check-up in 12 domande • Ordini, DDT, fatture e pagamenti vengono riconciliati senza ricostruzioni manuali?

- Sai quali scadenze sono realmente applicabili e perché?
- Sai dove si trova ogni documento critico e qual è la versione valida?
- Email, PEC, foto e chat autorizzate sono collegate a clienti, commesse o asset?
- Conosci il costo reale di una commessa o servizio?
- Vedi crediti scaduti, debiti imminenti e cash forecast insieme?
- Ricevi un briefing affidabile su cosa richiede decisione?
- Se manca una persona chiave, la conoscenza resta accessibile?
- Puoi risalire dalla decisione alla fonte del dato?
- Puoi distinguere un fatto verificato da una dichiarazione?
- Sai chi è owner di ogni problema importante?
- I software che usi condividono contesto senza doppio inserimento?

3 O PIÙ 'NO' = NON SIGNIFICA CHE DEVI COMPRARE SUBITO. SIGNIFICA CHE HAI ABBASTANZA ATTRITO DA

GIUSTIFICARE UNA DIAGNOSI.

Piano operativo: 7 giorni per vedere il caos

QUANDO

COSA FARE

Giorno 1 Mappa server, NAS, PC, cloud, gestionali, banche, email e canali autorizzati.

Giorno 2 Segna i tre Black Holes che assorbono più tempo, denaro o attenzione.

Giorno 3 Assegna owner, fonte primaria ed Evidence a ogni problema.

Giorno 4 Misura duplicati, telefonate, ricerche, ritardi e riconciliazioni manuali.

Giorno 5 Scegli un vertical slice end-to-end, per esempio ordine → DDT → fattura → pagamento.

Giorno 6 Definisci 5 KPI e 5 alert che servono davvero alla Direzione.

Giorno 7 Automatizza solo ciò che ha superato il verifier e confronta prima/dopo.

PARTIRE PICCOLO. MISURARE. VERIFICARE. POI SCALARE.

La trasformazione: prima vs dopo

AREA

PRIMA

DOPO SICURISSIMO

Documenti Ricerca per cartelle e persone Ricerca per oggetto, relazione, Evidence Scadenze Agenda e memoria Applicabilità + owner + prova + alert Fornitori Controllo manuale tardivo Catena ordine-DDT-fattura-pagamento Software Silos e doppio inserimento Connector + Mycelium Direzione Report e telefonate Control Tower + briefing Cash Estratti e fogli separati Cash Chain + riconciliazione + forecast

AI

Chat generica Cortex permission-aware con Proof

Il prossimo passo Se ti sei riconosciuto in tre o più Black Holes, la domanda non è 'quale altro software devo comprare?'. La domanda è: quali sorgenti, persone, processi e decisioni stanno oggi compensando manualmente la frammentazione? SICURISSIMO OS è progettato per diventare il layer intelligente sopra l'azienda esistente: collega, verifica, ricorda, controlla, prevede e trasforma eccezioni in azioni governate.

TROVA CIÒ CHE È DISPERSO. COLLEGA CIÒ CHE È ISOLATO. VERIFICA CIÒ CHE È INCERTO. RICORDA CIÒ CHE DI

DALLE PERSONE. CONTROLLA CIÒ CHE OGGI SCOPRI TROPPO TARDI.

Visita sicurissimo.online e valuta il piano di attivazione più adatto. La prova gratuita, i prezzi e le funzionalità effettivamente disponibili devono essere verificati sul portale al momento dell'attivazione.

FORNITORI: DAL COSTO INVISIBILE AL CONTROLLO

Il problema non è soltanto la fattura sbagliata. È l'impossibilità di ricostruire rapidamente la catena che ha generato quel costo. Ordine, consegna, DDT, fattura, pagamento e movimento bancario devono poter essere letti come un unico episodio economico.

Quando questa catena è spezzata, l'azienda paga in tempo amministrativo, contestazioni tardive e margini di commessa poco affidabili. La riconciliazione deve quindi essere un processo continuo e verificabile, non un controllo occasionale a fine mese.

COSA DEVE FARE SICURISSIMO OS

- collegare ordine, DDT, fattura e pagamento;
- segnalare quantità, prezzi e duplicati incoerenti;
- attribuire il costo alla commessa corretta;
- richiedere revisione umana quando il match è ambiguo.

SCADENZE: DALL'AGENDA ALL'OBLIGO GOVERNATO

Una scadenza ha valore soltanto se il sistema sa perché esiste, a chi si applica, chi deve agire, quale documento è richiesto e quale Evidence dimostra l'adempimento. Questo vale per sicurezza, lavoro, INPS/INAIL, fisco, privacy, cyber, assicurazioni, autorizzazioni, asset e obblighi settoriali.

Il vero salto è passare da 'ricordami questa data' a 'dimmi se questo requisito si applica alla mia azienda e cosa manca per dimostrarlo'.

COSA DEVE FARE SICURISSIMO OS

- costruire applicabilità e trigger;
- assegnare owner e deadline;
- collegare ente, fonte, documento ed Evidence;
- ricalcolare gli obblighi quando cambia la realtà aziendale.

CONOSCENZA: DAI FILE ALLA MEMORIA AZIENDALE

La conoscenza aziendale vive in cartelle, NAS, PC, email, PEC, foto, chat autorizzate e soprattutto nelle persone. Il problema non è archiviare di più, ma sapere che cosa significa ogni elemento e a quale cliente, commessa, asset, obbligo o decisione appartiene.

SICURISSIMO deve preservare le abitudini di archiviazione quando funzionano e costruire sopra una mappa logica interrogabile, con permessi, provenienza e storico.

COSA DEVE FARE SICURISSIMO OS

- mappare le sorgenti senza migrazione forzata;
- deduplicare e riconoscere versioni;
- collegare documenti e comunicazioni agli oggetti del Twin;
- trasformare know-how disperso in memoria verificabile.

SOFTWARE: CONNECT BEFORE REPLACE

Molte PMI rinunciano alla trasformazione perché temono mesi di migrazione. SICURISSIMO adotta il principio opposto: ciò che funziona resta al suo posto e diventa una sorgente o una capability.

Il valore nasce dal layer comune: identità, eventi, Evidence e contesto permettono a sistemi diversi di contribuire alla stessa rappresentazione aziendale.

COSA DEVE FARE SICURISSIMO OS

- usare connector read-only dove possibile;
- evitare doppio inserimento;
- sincronizzare per eventi e capability;
- sostituire un software solo quando il vantaggio è dimostrato.

TEMPO: MISURARE LA MICRO-GESTIONE

Il tempo perso non è un numero da promettere: è un costo da misurare. Ricerca documenti, telefonate di verifica, solleciti, approvazioni, riunioni di stato e doppio inserimento possono essere classificati per una settimana e trasformati in una baseline.

Da quella baseline si scelgono i workflow ad alta frequenza e basso rischio da automatizzare per primi.

COSA DEVE FARE SICURISSIMO OS

- misurare prima e dopo; • assegnare owner e stato alle richieste; • automatizzare solleciti e rollup ripetitivi; • mantenere human gate sulle decisioni sensibili.

DIREZIONE: DALLA DASHBOARD ALLA DECISIONE

Una Control Tower non deve impressionare con cento grafici. Deve ridurre il carico cognitivo della Direzione. Il sistema deve distinguere normale, anomalo, urgente, importante e incerto.

Ogni KPI utile dovrebbe poter portare a una domanda, a un drill-down e, quando serve, a un'azione con owner e scadenza.

COSA DEVE FARE SICURISSIMO OS

- mostrare eccezioni e priorità; • separare fatti verificati da dati mancanti; • produrre briefing giornalieri e periodici; • collegare decisione, azione ed esito.

MARGINE & CASH: SAPERE SE STAI GUADAGNANDO DA

Fatturato, utile e cassa sono tre viste diverse. Una commessa può fatturare molto, avere margine scarso e assorbire liquidità. Per capirlo servono costi diretti, indiretti, ore, materiali, mezzi, fornitori, crediti, debiti e movimenti bancari nello stesso contesto.

Il cash forecast deve guardare avanti: non soltanto quanto denaro c'è oggi, ma quali incassi e pagamenti sono attesi e con quale affidabilità.

COSA DEVE FARE SICURISSIMO OS

- ricostruire costo e margine per commessa/cliente; • monitorare aging crediti e debiti; • riconciliare movimenti bancari; • produrre forecast 7/30/60/90 giorni.

LE 12 FAMIGLIE DI PROBLEMI: LA MAPPA COMPLETA

I 7 Black Holes sono il linguaggio con cui l'imprenditore riconosce il dolore. Sotto di essi SICURISSIMO organizza dodici famiglie operative: caos informativo, software isolati, compliance 360, operations, procurement, finanza, marginalità, persone, asset, direzione, AI affidabile e decision-to-action.

Questa struttura rende il modello universale: cambiano ATECO, processi e obblighi, ma restano identità, persone, lavoro, asset, relazioni, documenti, denaro, tempo, regole, rischi e decisioni.

COSA DEVE FARE SICURISSIMO OS

- usare MATRIX81+ per configurare il DNA aziendale; • attivare soltanto le capability necessarie; • misurare Company Health per dominio; • trasformare ogni problema in Evidence, owner, workflow e risultato.

SICURISSIMO OS

LA TUA AZIENDA. SEMPRE SOTTO CONTROLLO.

**UN'AZIENDA PIÙ CONSAPEVOLE OGGI,
È UN FUTURO PIÙ FORTE DOMANI.**

SICURISSIMO OS unisce sicurezza, compliance, gestione aziendale, documenti, scadenze, fornitori, processi e dati in un unico ecosistema intelligente.

Un nuovo modo di lavorare, più semplice, più veloce, più sicuro. Per aziende, professionisti e tutti i settori ATECO.



PERSONE



PROCESSI



DOCUMENTI



SCADENZE



DATI



RISULTATI

**“ Il controllo oggi
è *libertà domani*. ”**

SICURISSIMO OS



SCOPRI SICURISSIMO OS

Visita il sito e inizia il tuo percorso verso un'azienda più forte e libera.

sicurissimo.online

STESSI PROBLEMI.
NUOVE SOLUZIONI.
PIÙ CONTROLLO.
PIÙ TEMPO.
PIÙ MARGINE.
PIÙ LIBERTÀ.

ISBN 979-12-997872-0-1



9 791299 787201