Blueprint di Digitalizzazione Sicura

Dal caos all'operatività: il modello "minimo sostenibile" per PMI che vogliono crescere senza esporsi

Un metodo pratico per costruire continuità, fiducia e resilienza digitale

---

Mini eBook a cura di:
Dennis Sepede

Co-Founder & CTO, Securitix Solutions
Cybersecurity Advisor

Securitix

Liberiamo le aziende dalla complessità digitale, rendendole più sicure e resilienti.

Prefazione

Perché ho scritto questo eBook

Negli ultimi anni ho osservato da vicino come molte imprese, soprattutto le PMI, affrontino la digitalizzazione con entusiasmo ma senza una direzione chiara.
Si trovano sommerse da strumenti, consulenze e soluzioni che promettono molto ma raramente portano valore reale e misurabile.
Il risultato è spesso lo stesso: complessità crescente, costi esuberanti e risultati poco trasparenti.

Molte aziende si sentono obbligate a *"essere digitali"*, ma finiscono per costruire infrastrutture fragili, scollegate, o non in linea con gli standard che garantiscono interoperabilità e competitività nel mercato.
Manca una visione strutturata che unisca organizzazione, tecnologia e sicurezza in un percorso coerente e sostenibile.

Ed è proprio da questa consapevolezza che nasce questo eBook.

Il mio obiettivo è offrire una guida concreta, un Blueprint di Digitalizzazione Sicura che aiuti a passare dal caos operativo a un modello stabile, scalabile e misurabile.
Un metodo basato sul concetto di "*minimo sostenibile*": fare di più con meno, ma in modo consapevole, seguendo standard riconosciuti e best practices internazionali.
Non servono soluzioni monumentali, ma scelte mirate, coerenti e replicate nel tempo.

Questo non è un manuale tecnico né un documento di conformità.
È una bussola pratica, pensata per imprenditori, IT manager e professionisti che vogliono capire come costruire continuità, fiducia e resilienza digitale senza sprecare risorse o rincorrere mode tecnologiche.

Spero che ogni sezione ti offra spunti da applicare subito, anche solo uno, per rendere la tua impresa un po' più solida, consapevole e competitiva in un mondo dove la sicurezza è ormai parte della produttività.

Dennis Sepede

Co-Founder & CTO, Securitix Solutions
Cybersecurity Advisor

Indice

1. Introduzione – La Sicurezza come Fondamento della Digitalizzazione 4
2. Digitalizzazione Sostenibile: Cosa Significa Davvero 6
3. Il Problema Tipico delle PMI: Frammentazione e Reattività 9
4. Il Blueprint: La Minima Architettura che Scala 13
5. Il Principio del "Minimo Sostenibile" 18
6. Roadmap Operativa 30·60·90 giorni 21
7. KPI e Metriche di Maturità 24
8. Cultura e Competenze: L'anello Debole che Diventa Vantaggio 28
9. Conclusione – Dal Caos alla Governance 31
10. Appendice – Strumenti & Template Pratici 33
11. Chi Sono e Perché mi occupo di Digitalizzazione Sicura 36

Introduzione

La Sicurezza come Fondamento della Digitalizzazione

Negli ultimi anni, la parola *digitalizzazione* è diventata una costante in ogni strategia aziendale.

Tuttavia, in molte realtà il termine viene ancora associato soltanto a nuove piattaforme, cloud, o processi automatizzati.

La verità è che **digitalizzare non significa solo usare tecnologia**, ma **governarla**, rendendola affidabile, controllabile e resiliente nel tempo.

Ogni impresa oggi, anche la più piccola, è a tutti gli effetti un'**azienda tecnologica**.

In pratica, **ogni giorno**:

- Gestisce dati,
- Accede a sistemi in cloud,
- Comunica in rete,
- Si affida a software per la propria produttività quotidiana.

Questo la espone, volente o nolente, agli stessi rischi informatici delle grandi organizzazioni, ma **con risorse molto più limitate**.

Una Trasformazione senza Basi Solide è un Rischio Sistemico

Le statistiche lo confermano: secondo i rapporti **ENISA** e **Clusit**, oltre l'80% degli incidenti di sicurezza che colpiscono le PMI europee sono dovuti a **errori evitabili**:

- Mancanza di aggiornamenti,
- Accessi non gestiti,
- Backup non verificati, o
- Assenza di policy interne.

Non si tratta di mancanza di volontà, ma di **assenza di metodo**.

La maggior parte delle aziende inizia a *"mettere in sicurezza"* quando qualcosa è già successo.

Ma a quel punto, la sicurezza non è più una protezione, **diventa una reazione costosa.**

Eppure, con una struttura minima e una visione coerente, la sicurezza può diventare **il vero motore della continuità operativa**, non un ostacolo.

Introduzione

La Sicurezza come Base, non come Aggiunta

La sicurezza dovrebbe essere integrata **dal primo giorno** in ogni percorso di *trasformazione digitale*.

Non come un layer aggiuntivo o un audit finale, ma come **principio architetturale**, il "***pavimento stabile*"** su cui costruire tutto il resto.

Integrare la sicurezza significa:

- **Progettare processi e tecnologie** pensando già alla resilienza;
- **Definire ruoli e responsabilità** prima che sorgano problemi;
- **Automatizzare** ciò che riduce errore umano e tempi di reazione;
- **Misurare e migliorare continuamente** la postura di sicurezza.

In questa prospettiva, la sicurezza non è più solo un costo o un vincolo:

Diventa una forma di efficienza.

Ogni misura che riduce la vulnerabilità riduce anche sprechi, downtime e interruzioni, **migliorando la produttività complessiva.**

La Digitalizzazione come Percorso di Fiducia

La fiducia è oggi una ***valuta digitale*.**

Clienti, partner e fornitori scelgono chi dimostra di saper **proteggere dati, processi e operatività.**

Una catena del valore sicura è anche una catena **più stabile, più competitiva** e **più capace di attrarre opportunità**.

La sicurezza, quindi, non è il punto d'arrivo della digitalizzazione, è **la condizione necessaria per farla funzionare**.

E questo è *il* ***filo conduttore*** che guiderà tutto il Blueprint:

Un **percorso concreto**, basato su **standard internazionali**, che mostra come costruire un'**infrastruttura digitale solida,** partendo dal *minimo sostenibile* per arrivare a una governance **matura** e **continua**.

Digitalizzazione Sostenibile

Cosa Significa Davvero

Il termine *digitalizzazione* è spesso associato a modernità, cloud, intelligenza artificiale e automazione.

Ma nella pratica quotidiana, per molte aziende digitalizzare significa anche introdurre **nuovi rischi e complessità**.

Ogni nuovo software, dispositivo o connessione è una **potenziale superficie d'attacco**.

Ogni processo automatizzato genera dipendenza da sistemi che, se non gestiti, **possono bloccare l'intera operatività**.

La vera domanda non è più *"Quanto siamo digitali?"*

Ma *"Quanto siamo in grado di governare la nostra digitalizzazione?"*

Il Concetto di Sostenibilità Digitale

Quando parlo di ***digitalizzazione sostenibile***, non mi riferisco alla sostenibilità ambientale, ma a qualcosa di altrettanto vitale:

La capacità di mantenere nel tempo ciò che costruiamo.

Una *digitalizzazione sostenibile* è:

- **Misurabile**, perché sappiamo cosa abbiamo e come funziona;
- **Controllata**, perché conosciamo chi accede, chi modifica e chi decide;
- **Resiliente**, perché può continuare a operare anche di fronte a guasti, errori o attacchi.

Non si tratta di fare tutto, ma di **fare bene le cose essenziali,** con continuità e metodo.

I Tre Pilastri della Sostenibilità Digitale

La *digitalizzazione sostenibile* si fonda su **tre pilastri chiave** che derivano dai principali standard internazionali, in particolare dal **NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)** e dalla **ISO 27001:2022**.

1. **Visibilità**

   Non si può proteggere ciò che non si conosce.

   Avere visibilità significa sapere *quali asset esistono, chi li usa e come vengono gestiti.*

   L'inventario IT, la mappatura dei flussi di dati e la consapevolezza dei fornitori sono le basi per qualsiasi decisione strategica.

Digitalizzazione Sostenibile

I Tre Pilastri della Sostenibilità Digitale

2. Controllo

Una volta che conosciamo il perimetro, serve poterlo governare.

Controllo significa definire regole, ruoli e automatismi: gestione degli accessi, patch management, log centralizzati, processi di approvazione chiari.

L'inventario IT, la mappatura dei flussi di dati e la consapevolezza dei fornitori sono le basi per qualsiasi decisione strategica.

3. Resilienza

È la capacità di resistere, adattarsi e riprendere rapidamente dopo un incidente.

Backup testati, piani di continuità, simulazioni di emergenza e una cultura interna pronta a reagire fanno la differenza tra un disservizio temporaneo e un blocco totale.

Come ricorda **ENISA**, la resilienza non si costruisce in emergenza, si costruisce con:

- Abitudini regolari,
- Processi semplici,
- Miglioramento continuo.

La Proporzionalità come Chiave di Efficienza

Un principio fondamentale, spesso trascurato nella digitalizzazione, è quello della **proporzionalità**.

Definito chiaramente nella **ISO/IEC 27001:2022 (Annex A)**, indica che **ogni controllo deve essere commisurato al rischio reale, al contesto e alle risorse disponibili**.

In pratica, significa che **non tutte le aziende devono adottare lo stesso livello di complessità**:

Un controllo efficace in una multinazionale può essere eccessivo (o controproducente) per una PMI.

La vera maturità sta nel scegliere con criterio **cosa implementare** e perché, valutando il bilancio tra **protezione**, **impatto operativo** e **costi di mantenimento**.

Questo principio è il cuore della ***sicurezza sostenibile***:

La capacità di applicare solo ciò che serve davvero, nel modo **più semplice ed efficiente possibile**.

Agire con proporzionalità non è un compromesso, è **strategia di efficienza**.

È ciò che permette a un'organizzazione di crescere senza appesantirsi, **mantenendo il controllo** e garantendo la continuità operativa nel tempo.

Digitalizzazione Sostenibile

Fare di Più con Meno (In Modo Consapevole)

La *sostenibilità digitale* si basa sullo stesso principio della ***sicurezza sostenibile***:

Fare di più con meno, ma con consapevolezza e metodo.

Non servono piattaforme costose o strumenti complessi; servono **standard, priorità** e **disciplina**.

Questo è ciò che trasforma la tecnologia in **leva di competitività**, invece che in fonte di fragilità.

Una ***digitalizzazione sostenibile*** non rallenta l'innovazione, la abilita:

- Riduce il rumore,
- Crea fiducia interna,
- Permette di crescere con basi solide.

Dalla Teoria alla Pratica

Nei prossimi capitoli vedremo come questi principi si traducono in **architettura operativa.**

Il **Blueprint di Digitalizzazione Sicura** non nasce per aggiungere burocrazia, ma per fornire una **struttura minima, replicabile** e **scalabile**, in linea con le migliori pratiche **NIST, CIS** e **ISO**.

Perché solo ciò che è **sostenibile nel tempo** può davvero essere **digitale, sicuro** e **competitivo**.

Il Problema Tipico delle PMI

Frammentazione e Reattività

Ogni impresa che intraprende un *percorso di digitalizzazione* parte con buone intenzioni:

- Automatizzare,
- Migliorare l'efficienza,
- Ridurre i costi,
- *"Mettere tutto in cloud"*.

Ma quasi sempre, dopo qualche anno, la realtà appare molto diversa da come era stata immaginata.

- Sistemi che non dialogano tra loro.
- Credenziali duplicate o dimenticate.
- Backup impostati, ma mai testati.
- Policy scritte, ma sconosciute a chi le deve applicare.

E alla fine, la tecnologia, invece di semplificare, **aumenta la complessità**.

Il *"Diagramma del Caos"*

Prima di parlare di metodo, vale la pena **visualizzare il punto di partenza più comune nelle PMI**.

Molte realtà si trovano in uno stato di digitalizzazione spontanea, cresciuta nel tempo, stratificata su esigenze urgenti, ma **priva di una regia unitaria**.

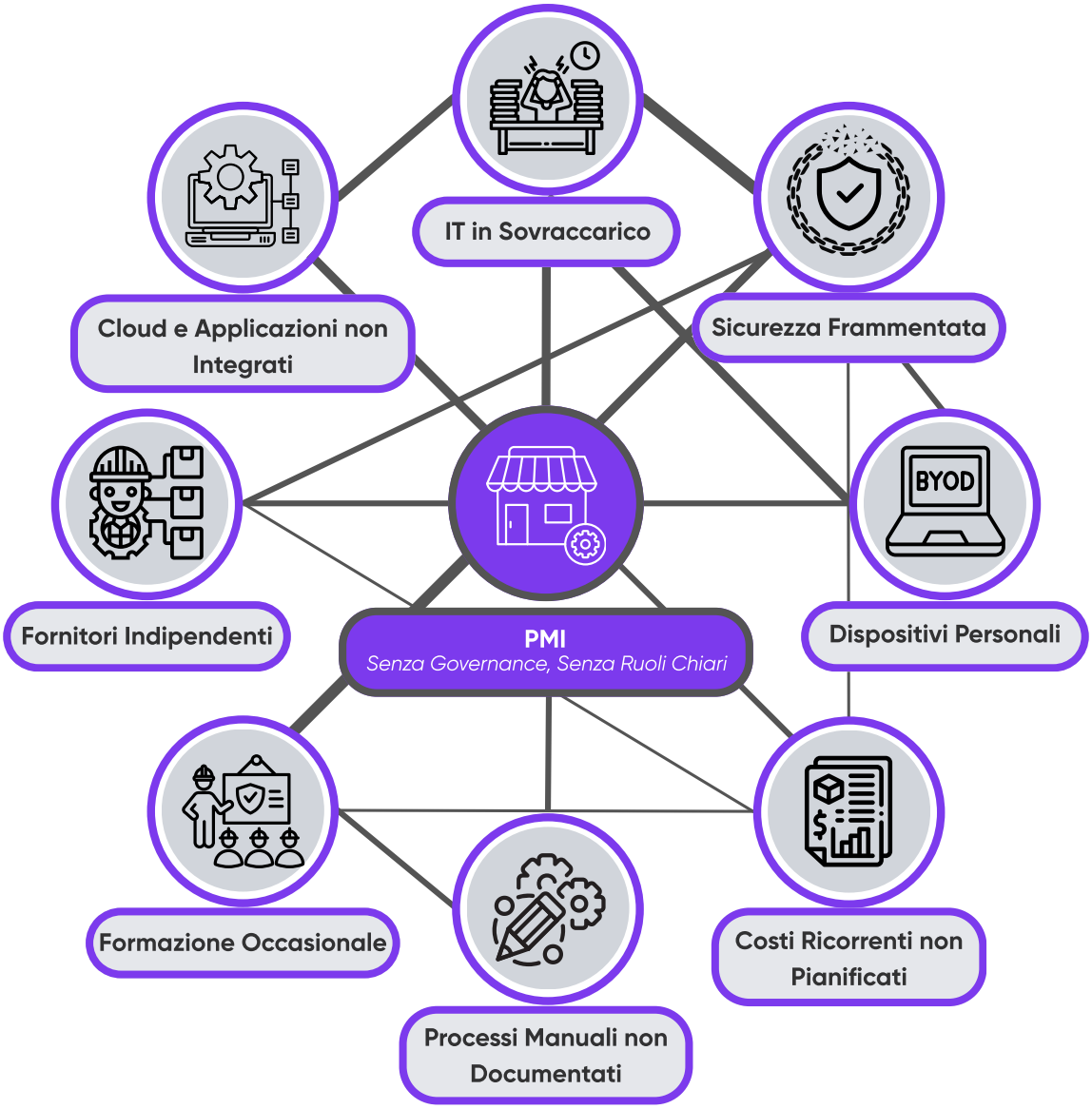
Nella pagina successiva, una rappresentazione schematica del ***"caos digitale tipico"***, dove strumenti, processi e persone convivono **senza una governance chiara**:

Un punto di partenza riconoscibile per molte PMI.

Il Problema Tipico delle PMI

Il Caos Digitale Tipico di una PMI

Quando ogni soluzione funziona da sola, ma nessuna lavora insieme.



Un ecosistema costruito per urgenze, **non per visione**.

Ogni nodo funziona da solo, ma **nessuno contribuisce a un sistema coerente**.

Questo è il punto di partenza più comune.

Non un errore, ma **la conseguenza naturale della crescita senza governance**.

Da qui nasce la necessità di un metodo, un ***Blueprint***, capace di trasformare il caos in continuità.

Il Problema Tipico delle PMI

Un Mosaico di Soluzioni, Senza una Regia

Il problema non è la mancanza di strumenti, ma **la mancanza di integrazione e visione**.

Le PMI spesso crescono per stratificazione:

Ogni esigenza urgente porta un nuovo software, un nuovo fornitore, un nuovo contratto.

Nel tempo, questo crea un **mosaico frammentato** di *soluzioni eterogenee*, con processi che si reggono solo sulla buona volontà delle persone.

Ecco alcuni esempi concreti di **criticità ricorrenti**:

- **Assenza di inventario IT aggiornato**: non si sa esattamente quali dispositivi, applicazioni o dati siano in uso.
- **Responsabilità disperse**: la sicurezza è *"di tutti"*, quindi di nessuno.
- **Fornitori non coordinati**: ognuno gestisce un pezzo (sistemi, cloud, rete), ma nessuno vede il quadro complessivo.
- **Processi reattivi**: si interviene solo quando c'è un guasto o un incidente.
- **Assenza di standard condivisi**: ogni scelta è episodica, non strategica.

Quest' **assenza di governance** è il principale ostacolo alla *digitalizzazione sicura*.

Non serve avere più strumenti, **serve avere un metodo**.

Costi Alti, Risultati Incerti

Molte aziende sono frenate anche da un altro fattore:

La percezione che per essere *"sicuri"* servano investimenti esorbitanti.

Il mercato è pieno di soluzioni **costose** e **iper-specialistiche**, spesso progettate per realtà enterprise, **non per PMI**.

Il risultato è che molte imprese rinunciano a investire o si affidano a strumenti isolati che danno una **falsa sensazione di protezione**.

Il paradosso è evidente: si spende tanto, ma **non si guadagna chiarezza né continuità**.

Manca un **criterio di priorità**, una **visione sostenibile** che faccia convivere **sicurezza, efficienza** e **competitività.**

Il Problema Tipico delle PMI

Dal Caos alla Struttura: Serve un Blueprint

Per uscire da questa frammentazione non servono progetti monumentali, ma **architetture semplici e coerenti**, in grado di crescere nel tempo.

Serve un modello che permetta di:

- Capire **dove siamo oggi**,
- Stabilire **quali controlli minimi implementare**,
- Costruire **una base solida che possa scalare** in futuro.

È proprio qui che entra in gioco il concetto di ***Blueprint di Digitalizzazione Sicura***:

Una mappa di riferimento che combina **standard internazionali** (NIST, CIS, ISO) con **esperienza operativa** sul campo, per aiutare le PMI a **fare ordine**, **automatizzare** in modo intelligente e **governare** la propria ***evoluzione digitale***.

Nel capitolo successivo vedremo come questo *Blueprint* si traduce in un' **architettura minima** che scala, fatta di **sei livelli logici** e **interdipendenti:**

- **Identità,**
- **Dispositivi,**
- **Rete,**
- **Dati,**
- **Cloud & Applicazioni,**
- **Governance & Continuità.**

Il Blueprint

La Minima Architettura che Scala

Ogni azienda ha la propria complessità, ma tutte condividono una sfida comune: **Costruire ordine digitale in modo sostenibile**.

Il *Blueprint di Digitalizzazione Sicura* nasce per rispondere a questa esigenza: offrire **un modello universale, ma adattabile**, che consente a qualsiasi PMI di rafforzare sicurezza e continuità operativa **senza appesantire l'organizzazione**.

L'obiettivo non è *"fare tutto"*, ma creare **una base stabile che possa crescere nel tempo**, seguendo priorità chiare e standard riconosciuti.

Questo *Blueprint* si fonda su **sei livelli logici**, ispirati al **NIST Cybersecurity Framework**, ai **CIS Critical Security Controls v8** e all'**ISO/IEC 27001:2022**.

1. Identità

Chi Accede e con Quali Diritti
NIST: Protect (PR.AC), CIS Controls 5–6

La *gestione delle identità* è **il primo mattone di ogni architettura sicura**.

Ogni accesso non controllato è una **possibile breccia**, e ogni utente con troppi privilegi è una **minaccia potenziale**.

Azioni chiave:

- Implementare **autenticazione multifattore** (MFA) su tutti i servizi critici.
- Applicare il principio del ***least privilege***: ognuno vede solo ciò che **serve** al proprio ruolo.
- Automatizzare il **provisioning/deprovisioning** di account e ruoli.
- Monitorare accessi anomali o tentativi falliti con **alert automatici**.

Risultato:

Tracciabilità e controllo, base essenziale per qualsiasi compliance.

Caso reale PMI– PMI manifatturiera (Lombardia)

Un'azienda metalmeccanica con 80 dipendenti gestiva credenziali condivise tra produzione e uffici.

L'introduzione di un sistema di **Single Sign-On con MFA** e la dismissione automatica degli account inattivi ha eliminato oltre 40 utenze ridondanti.

Il risultato? **Accessi tracciabili**, **meno errori** e **conformità più semplice** da dimostrare.

Il Blueprint

2. Dispositivi

Sapere Cosa Possiedi e Mantenerlo Sano
NIST: Identify (ID.AM), Protect (PR.IP), CIS Controls 1–2–7

Non si può proteggere **ciò che non si conosce**.

Ogni laptop, server, router o dispositivo mobile deve essere **censito, aggiornato** e **monitorato**.

Azioni chiave:

- Creare un **inventario centralizzato** degli asset IT (hardware e software).
- Standardizzare il **baseline di hardening** dei dispositivi (policy di sicurezza minima).
- Automatizzare gli **aggiornamenti e patch di sicurezza.**
- Segmentare i dispositivi BYOD (personali) da quelli aziendali.

Risultato:

Riduzione drastica delle vulnerabilità e gestione predittiva del rischio tecnico.

Caso reale PMI– Studio professionale (Emilia-Romagna)

Uno studio di consulenza fiscale con 25 postazioni aveva computer gestiti individualmente e aggiornamenti non tracciati.

Con l'introduzione di un **sistema RMM** *(Remote Monitoring & Management)* e **policy di patch automatizzate**, ha ottenuto un inventario completo e ridotto del 60% i problemi legati a software obsoleti.

Il risultato? **Maggiore efficienza operativa** e **riduzione dei tempi di intervento tecnico**.

3. Rete

Separare, Controllare, Proteggere
NIST: Protect (PR.PT), Detect (DE.CM), CIS Controls 12–13

La rete è **il sistema circolatorio dell'azienda**, se non è protetta, ogni compromissione **può propagarsi ovunque**.

Azioni chiave:

- **Implementare firewall** e **segmentazione logica delle reti** (es. separare produzione, uffici, guest).
- **Utilizzare VPN sicure** e **autenticazione forte** per accessi remoti.
- **Monitorare costantemente** il traffico con log centralizzati.
- **Rivedere regolarmente le regole di rete** obsolete o inutili.

Risultato:

Visibilità sul traffico, contenimento delle minacce e risposta più rapida agli incidenti.

Il Blueprint

3. Rete

Separare, Controllare, Proteggere
NIST: Protect (PR.PT), Detect (DE.CM), CIS Controls 12–13

Caso reale PMI– Azienda logistica (Veneto)

Un operatore logistico con tre magazzini interconnessi aveva un'unica rete piatta condivisa da uffici e dispositivi IoT.

Implementando una **segmentazione VLAN** e **VPN** con accesso **MFA**, ha isolato i sistemi di magazzino, ridotto del 90% i rischi di propagazione malware e migliorato la velocità di diagnosi in caso di incidenti.

Il risultato? **Riduzione del 90% dei rischi di propagazione malware** e diagnosi più veloce degli incidenti.

4. Dati

Proteggere ciò che Conta Davvero
NIST: Protect (PR.DS), Recover (RC.RP), CIS Controls 3–11

I dati sono **il patrimonio più prezioso**. Senza una gestione strutturata, la *digitalizzazione* diventa **vulnerabilità**.

Azioni chiave:

- **Classificare i dati** in base alla criticità (pubblici, interni, riservati).
- Implementare **backup automatici e testati periodicamente**.
- Applicare **cifratura** dei dati sensibili (at rest e in transit).
- Stabilire **policy di retention** e cancellazione sicura.

Risultato:

I dati rimangono disponibili, integri e riservati anche in caso di incidente.

Caso reale PMI – Azienda sanitaria privata (Lazio)

Una clinica con 50 operatori gestiva cartelle cliniche e referti su server locali non cifrati.

Implementando **backup cifrati e replica cloud in data center europeo** con test mensili di restore, ha garantito integrità dei dati e conformità GDPR.

Il risultato? **Continuità operativa assicurata** e **riduzione del rischio** di perdita o violazione dei **dati sensibili**.

Il Blueprint

5. Cloud & Applicazioni

Gestire l'Agilità Senza Perdere Controllo

NIST: Protect (PR.AC / PR.DS), Detect (DE.CM), CIS Controls 4–8–16

Il cloud è un ***abilitatore***, ma anche un **moltiplicatore di rischi** se gestito senza **governance**.

L'obiettivo non è evitarlo, ma **governarlo con regole chiare**.

Azioni chiave:

- Utilizzare **autenticazione federata (SSO)** per gestire accessi multi-piattaforma.
- Monitorare l'uso di ***shadow IT*** (app o servizi cloud non autorizzati).
- Centralizzare i log di accesso e attività.
- Verificare regolarmente le **configurazioni di sicurezza** dei servizi cloud (IAM, storage, policy di accesso).

Risultato:

Agilità senza perdita di controllo e conformità più semplice da dimostrare.

Caso reale PMI – PMI del retail (Campania)

Un gruppo di negozi con gestione multi-sede usava cinque piattaforme cloud diverse per ordini, contabilità e CRM.

Attraverso l'implementazione di un **sistema SSO con controllo IAM unificato**, ha ridotto del 40% gli errori di accesso e semplificato gli audit di sicurezza periodici.

Il risultato? **Gestione centralizzata**, **maggiore efficienza** e **sicurezza applicativa**.

6. Governance & Continuità

Il motore silenzioso della resilienza

NIST: Identify (ID.GV), Respond (RS), Recover (RC), CIS Controls 14–17

Nessuna tecnologia funziona senza una governance che la guidi.

Questo livello riguarda **processi, ruoli, cultura** e **continuità operativa**.

Azioni chiave:

- Definire **ruoli e responsabilità** chiari (es. referenti IT, responsabili sicurezza, DPO).
- Creare procedure di **Incident Response** e testarle periodicamente.
- Redigere un **Business Continuity Plan** (BCP) e un **Disaster Recovery Plan** (DRP) adeguati.
- Promuovere **formazione continua** e **consapevolezza** sulla sicurezza.

Risultato:

Capacità di rispondere e ripartire rapidamente, con fiducia e metodo.

Il Blueprint

6. Governance & Continuità

Il motore silenzioso della resilienza

NIST: Identify (ID.GV), Respond (RS), Recover (RC), CIS Controls 14–17

Caso reale PMI – Impresa di servizi (Piemonte)

Una società di consulenza digitale non aveva piani formalizzati di risposta agli incidenti.

Dopo un'interruzione dovuta a blackout, ha sviluppato un **BCP semplificato** basato su priorità operative e procedure di comunicazione interna.

Il risultato? Nel disservizio successivo, il ripristino è avvenuto in **2 ore** invece che 12, **riducendo l'impatto operativo** e **reputazionale**.

Un Sistema che Cresce nel Tempo

Questi sei livelli non sono compartimenti stagni:

Si nutrono a vicenda.

Un buon controllo delle identità migliora la sicurezza dei dati; una governance chiara rende più efficaci le decisioni sugli strumenti; una rete segmentata riduce l'impatto di errori umani.

Il ***Blueprint di Digitalizzazione Sicura*** è pensato per essere scalabile:

Puoi partire da un livello, consolidarlo e poi estendere la maturità sugli altri, secondo le priorità e le risorse disponibili.

Nel prossimo capitolo vedremo come questo approccio si traduce nel principio del ***"minimo sostenibile"***:

Come ottenere **l'80% del valore con il 20% delle azioni giuste**, riducendo rischi e costi in modo misurabile.

Il Principio del *"Minimo Sostenibile"*

Una delle convinzioni più radicate nella cultura aziendale è che *"più sicurezza significa più complessità"*.

In realtà, è vero l'esatto contrario:

La sicurezza efficace è quella semplice da mantenere.

Il principio del ***"minimo sostenibile"*** nasce da un'osservazione diretta:

Nelle PMI, le soluzioni che funzionano davvero non sono quelle più sofisticate, ma quelle **che si riescono a mantenere nel tempo**.

Una policy perfetta ma non applicata è inutile quanto una tecnologia costosa non configurata.

Cosa Significa *"Minimo Sostenibile"*

Il *minimo sostenibile* non è *"fare poco"*:

È **fare l'essenziale con disciplina**, scegliendo azioni che producono il massimo impatto sul rischio con il minimo sforzo operativo.

In altre parole, **è l'80/20 della sicurezza**:

Concentrarsi su quel 20% di controlli che riduce l'80% delle vulnerabilità e garantisce continuità.

Questo concetto è coerente con i **framework internazionali**:

- il **NIST Cybersecurity Framework**, che promuove azioni *"commensurate al rischio"*;
- i **CIS Critical Security Controls**, che individuano un set di controlli di base per le PMI (Implementation Group 1);
- la **ISO/IEC 27001:2022**, che valorizza l'approccio *"risk-based"*, ossia misurato sul contesto reale dell'organizzazione.

Il Principio del *"Minimo Sostenibile"*

Le 5 Aree del *Minimo Sostenibile*

Applicare questo principio significa costruire un piano d'azione pratico, che copre 5 aree fondamentali del *Blueprint*:

1. **Identità e Accessi**
   - Attivare MFA su tutti gli account amministrativi e cloud.
   - Disabilitare gli account inutilizzati.
   - Implementare la regola del *"least privilege"*.
2. **Backup e Continuità**
   - Automatizzare il backup e **testarlo periodicamente** (non basta farlo).
   - Mantenere almeno una copia **offline o offsite**.
   - Verificare il ripristino almeno ogni trimestre.
3. **Aggiornamenti e Patching**
   - Automatizzare gli update di sistema e applicazioni.
   - Monitorare le versioni critiche con alert centralizzato.
   - Creare un ciclo standard di manutenzione.
4. **Formazione e Consapevolezza**
   - Formare periodicamente tutti i dipendenti sulle minacce più comuni (phishing, password, data handling).
   - Simulare incidenti o campagne di phishing per misurare l'efficacia.
5. **Incident Response Minima**
   - Definire una **procedura base di gestione incidenti** (chi segnala, chi decide, chi comunica).
   - Creare una checklist operativa: *"in caso di blocco, cosa facciamo nei primi 30 minuti"*.

Un Metodo per Priorità, non per Strumenti

Ogni azienda può mappare le proprie azioni secondo tre livelli di priorità:

Livello	Obbiettivo	Esempi
Essenziale	Bloccare le cause più comuni di incidenti	MFA, backup testato, patch automatiche
Intermedio	Ridurre il rischio operativo e di errore umano	Logging centralizzato, formazione periodica
Avanzato	Automatizzare e integrare processi	Monitoraggio continuo, piani di risposta formalizzati

L'obiettivo non è arrivare subito al livello avanzato, ma **costruire solidità in modo progressivo**, senza dispersione.

Il Principio del *"Minimo Sostenibile"*

Il *Minimo Sostenibile* come Ciclo di Miglioramento

Un sistema digitale sostenibile non è mai *"finito"*.

Il ***minimo sostenibile*** è un punto di partenza che si evolve nel tempo, seguendo tre fasi:

1. **Standardizza:**
   Definisci poche regole semplici, applicabili a tutti.
2. **Automatizza:**
   Usa la tecnologia per ridurre attività ripetitive e aumentare coerenza.
3. **Monitora:**
   Misura, correggi, migliora. Ogni mese, non ogni incidente

Questo approccio crea un **effetto domino positivo**:

Più controllo → Meno errori → Più fiducia → Più tempo per innovare.

La Mentalità Giusta

Il *minimo sostenibile* non è una scorciatoia, è una **filosofia operativa**.

Richiede di accettare che non tutto può essere perfetto, ma molto può essere **sufficiente** e **stabile**.

Significa scegliere la semplicità come strategia di resilienza.

Come dice il framework **NIST CSF 2.0**, la sicurezza moderna non è più solo "proteggere", ma ***"saper adattarsi"***.

E per adattarsi, serve struttura, non caos.

Nel prossimo capitolo vedremo come trasformare questi principi in azioni calendarizzate, attraverso una roadmap concreta *30·60·90 giorni*, il percorso per costruire basi solide senza fermare il business.

Roadmap Operativa 30·60·90 Giorni

Cosa Significa *"Minimo Sostenibile"*

Ogni trasformazione digitale efficace parte da azioni **piccole ma mirate.**

L'errore più comune è voler sistemare tutto subito, e finire per non cambiare nulla.

Per questo, la *Roadmap 30·60·90 giorni* è pensata per creare **risultati visibili** e **misurabili** in tempi brevi, **senza dover stravolgere l'organizzazione**.

Si basa su un **approccio incrementale**, ispirato al **NIST Cybersecurity Framework** e ai **CIS Critical Security Controls v8**, e allineato ai livelli di priorità dei **CIS Implementation Groups 1–2** (le misure essenziali per PMI e organizzazioni in crescita).

Le tre fasi seguono la logica delle funzioni **NIST PR/DE/RR – Protect, Detect, Respond/Recover**, e accompagnano l'azienda nel passaggio da reattiva a governata: **Stabilizzare, Rafforzare, Consolidare.**

Fase 1 – 30 giorni

Mettere Ordine e Visibilità
NIST – Protect (PR), CIS IG1

Obbiettivo:

Ottenere una visione chiara dell'attuale situazione digitale e chiudere le vulnerabilità più ovvie.

In questa fase si *"accende la luce"* sulla realtà operativa.

Azioni Chiave:

- Creare o aggiornare l'inventario degli asset IT (dispositivi, account, software).
- Attivare autenticazione multifattore (MFA) su email, cloud e sistemi critici.
- Verificare la presenza di un backup funzionante e testato.
- Definire policy base di accesso e password.
- Nominare un referente interno per la sicurezza (anche non tecnico).

KPI di Successo:

- 100% account critici protetti da MFA.
- Tutti i dispositivi censiti in un inventario centralizzato.
- Backup testato almeno una volta con successo.

Risultato Atteso:

Chiarezza, consapevolezza e prime misure concrete di protezione.

Corrispondenza Framework:

- NIST PR.AC / PR.IP – Controllo accessi e protezione infrastrutture.
- CIS IG1 – Priorità base: MFA, inventario, backup.

Roadmap Operativa 30·60·90 Giorni

Fase 2 – 60 giorni

Standardizzare e Formare
NIST – Protect (PR) e Detect (DE), CIS IG1–2

Obbiettivo:

Passare dal *"sapere cosa abbiamo"* al *"saperlo gestire bene"*.

Si definiscono **regole ripetibili** e si coinvolgono le persone, perché la sicurezza non è solo tecnica, è anche **comportamentale**.

Azioni Chiave:

- Applicare patch management automatizzato (aggiornamenti regolari).
- Segmentare la rete: separare uffici, guest, produzione.
- Implementare logging centralizzato per accessi e attività critiche.
- Attivare formazione base per tutti i dipendenti (phishing, password, dati sensibili).
- Stendere una procedura Incident Response minima: chi fa cosa, quando succede qualcosa.

KPI di Successo:

- 90% dei dispositivi aggiornati automaticamente.
- Log raccolti da almeno 3 sistemi chiave.
- 100% dipendenti formati sui comportamenti di base.

Risultato Atteso:

Processi più coerenti, cultura della sicurezza avviata, minore dipendenza dalle emergenze.

Corrispondenza Framework:

- NIST DE.CM / PR.AT – Monitoraggio continuo e formazione utenti.
- CIS IG1–2 – Maturazione dei controlli: patching, logging, training.

Fase 3 – 90 giorni

Automatizzare e Misurare
NIST – Protect (PR) e Detect (DE), CIS IG1–2

Obbiettivo:

Consolidare il sistema, **misurare i miglioramenti** e creare continuità.

A questo punto si passa dalla reattività alla governance proattiva.

Azioni Chiave:

- Introdurre monitoraggio continuo (alert automatici, report periodici).
- Formalizzare un Business Continuity Plan (BCP) e testare il ripristino.
- Definire KPI e dashboard di sicurezza (MFA attivo, patch rate, incidenti chiusi).
- Creare un registro dei rischi digitali con priorità e responsabili.
- Pianificare una verifica trimestrale di maturità e aggiornamento roadmap.

Roadmap Operativa 30·60·90 Giorni

Fase 3 – 90 giorni

Automatizzare e Misurare
NIST – Protect (PR) e Detect (DE), CIS IG1–2

KPI di Successo:

- Tempo medio di ripristino (RTO) sotto le 8 ore per servizi critici.
- Dashboard con almeno 5 metriche di sicurezza attive.
- Miglioramento documentato rispetto al mese 1.

Risultato Atteso:

Resilienza misurabile, governance stabile e visione chiara delle priorità future.

Corrispondenza Framework:

- NIST DE.DP / RS.MI / RC.IM – Rilevazione, risposta e miglioramento continuo.
- CIS IG2 – Controlli avanzati: automazione, reporting, analisi di maturità.

Un Modello Ciclico, non Lineare

Questa roadmap non si chiude al novantesimo giorno:

Diventa un **ciclo di miglioramento continuo.**

Ogni trimestre si può riesaminare la maturità, aggiungere controlli, automatizzare nuove aree o rafforzare la formazione.

Come insegna il **NIST CSF** (funzioni PR, DE, RR), la maturità digitale non è un traguardo, ma **una traiettoria di crescita costante**.
L'obiettivo finale non è *"essere conformi"*, ma **essere continui,** pronti a evolvere, correggere e ripartire in ogni scenario.

Questa *roadmap* sintetizza il percorso pratico per passare dal **caos alla governance**:

90 giorni per creare basi misurabili di sicurezza sostenibile, con un linguaggio condiviso tra management, IT e business.

È la traduzione operativa del principio *"fare di più con meno, in modo consapevole."*

Nel prossimo capitolo entreremo nel tema della **misurazione e della maturità**:

Come definire **KPI**, **indicatori** e **metriche** che permettano di capire, con dati reali, se la sicurezza e la digitalizzazione stanno evolvendo nella giusta direzione.

KPI e Metriche di Maturità

Misurare per Migliorare: la Sicurezza come Processo Continuo

Un principio fondamentale della gestione moderna, e della sicurezza efficace, è semplice:

"Non puoi migliorare ciò che non misuri."

Molte aziende *"credono"* di essere sicure finché non succede qualcosa, **ma non hanno alcun dato oggettivo per verificarlo**.

Il risultato è una sicurezza percepita, non reale.

Per questo motivo, ogni percorso di ***digitalizzazione sicura*** deve includere fin dall'inizio un **sistema di metriche e indicatori** che permetta di:

- Capire se le azioni intraprese stanno funzionando;
- Comunicare i risultati in modo chiaro al management;
- Decidere le priorità future basandosi su evidenze, non su impressioni.

Le Tre Categorie di KPI nella Sicurezza Digitale

Per una PMI, non servono decine di grafici o report complessi, bastano **pochi KPI ben scelti**, leggibili e aggiornati.

I più utili si possono suddividere in **tre categorie**:

KPI di Protezione (Preventivi)

Misurano il livello di implementazione delle difese e dei controlli.

Indicatore	Obbiettivo	Esempi di Soglia
Percentuale dispositivi aggiornati	Garantire patching regolare	≥ 95%
Utenti con MFA attivo	Proteggere accessi critici	100
Copertura backup testato	Garantire continuità	≥ 90%
Tempo medio di aggiornamento software critico	Ridurre esposizione	< 7 giorni

Riferimento Standard:
NIST CSF – Function Protect (PR), CIS Controls 1–7.

KPI e Metriche di Maturità

KPI di Rilevazione e Risposta (Operativi)

Servono a capire se l'azienda è in grado di **vedere e reagire** agli incidenti.

Indicatore	Obbiettivo	Esempi di Soglia
Numero di incidenti rilevati e gestiti	Dimostrare capacità di monitoraggio	+ Rispetto al trimestre precedente
Tempo medio di rilevazione (MTTD)	Reagire prima che il danno cresca	< 24h
Tempo medio di risposta (MTTR)	Limitare impatto operativo	< 8h
Percentuale di eventi con root cause identificata	Evitare recidiva	≥ 80%

Riferimento Standard:
NIST CSF – Detect (DE), Respond (RS), ISO 27035.

KPI di Resilienza e Miglioramento (Strategici)

Valutano la capacità dell'organizzazione di **riprendersi e progredire** nel tempo.

Indicatore	Obbiettivo	Esempi di Soglia
Tempo medio di ripristino servizi critici (RTO)	Misurare continuità	< 8 ore
Disponibilità media dei sistemi core	Garantire operatività	≥ 99%
Percentuale di procedure testate	Verificare preparazione	≥ 90%
Incremento della maturità rispetto al trimestre precedente	Dimostrare crescita	+1 livello su 5

Riferimento Standard:
NIST CSF – Recover (RC), ISO 22301 (Business Continuity).

KPI e Metriche di Maturità

La Cyber Maturity Matrix per PMI

Una delle modalità più efficaci per comunicare la crescita digitale è usare una **matrice di maturità**:
Uno strumento visivo che mostra il livello raggiunto nei diversi ambiti del Blueprint.

Livello	Descrizione	Esempi di Stato
Caotico	Nessuna regola o visibilità	Sistemi gestiti a reazione
Iniziato	Alcune misure essenziali attive	MFA e backup presenti, ma non verificati
Strutturato	Processi ripetibili e monitorati	Patching automatizzato, policy definite
Gestito	Governance chiara e metriche operative	KPI periodici, formazione attiva
Ottimizzato	Miglioramento continuo e automazione	Revisione trimestrale, analisi predittiva

Obiettivo per le PMI:
Raggiungere stabilmente il **livello 3 (Strutturato)** entro 12 mesi, e avanzare verso il 4 nel biennio successivo.

Misurare in Modo Pratico

Non servono software costosi per monitorare questi indicatori.

Molti KPI possono essere tracciati con strumenti già presenti in azienda:

- Fogli di calcolo condivisi per inventario e patching.
- Dashboard integrate nei sistemi cloud *(es. Microsoft 365 Secure Score)*.
- Log centralizzati o report mensili del fornitore IT.

L'importante è **aggiornare regolarmente le metriche**, anche in modo semplice, e rivederle insieme al team o alla direzione.
Questo trasforma la sicurezza da spesa invisibile a **valore tangibile e dimostrabile**.

KPI e Metriche di Maturità

Dalla Misurazione al Miglioramento Continuo

La misurazione non è un punto d'arrivo, ma **il punto di partenza del miglioramento**.

Ogni dato raccolto, che sia il tempo medio di rilevazione di un incidente o la percentuale di backup testati, deve servire per **correggere**, **ottimizzare** e **anticipare**.

Questo è il principio del ***continuous improvement***, alla base anche del **NIST IR 8286**, che collega la sicurezza informatica al più ampio concetto di *Enterprise Risk Management*:

"La maturità digitale cresce quando le informazioni sulla sicurezza guidano le decisioni di business."

In pratica, significa portare la sicurezza nel ciclo decisionale quotidiano:

- Usare i KPI non solo per *"fare report"*, ma per **prendere decisioni migliori**;
- Confrontare trend trimestrali e verificare se gli investimenti producono effetti reali;
- Trasformare ogni errore o incidente in un'occasione di apprendimento.

Quando questo approccio diventa abitudine, la sicurezza smette di essere un progetto da chiudere:

Diventa un **processo che evolve nel tempo,** proprio come l'azienda che la adotta.

Il Valore dei Dati

Misurare serve anche a comunicare.

Un imprenditore che vede grafici, trend e numeri capisce dove sta investendo e quanto sta migliorando.

La cultura dei dati è la base della **fiducia interna ed esterna,** con i numeri, la sicurezza diventa finalmente una leva di business, non un costo necessario.

Pro Tip:
"Non serve perfezione, serve coerenza: i KPI valgono solo se vengono aggiornati regolarmente."

Cultura e Competenze

L'Anello Debole che Diventa Vantaggio

La tecnologia può essere impeccabile, i processi solidi e le procedure perfette.

Eppure, la maggior parte degli incidenti informatici nasce sempre da lì: **l'errore umano.**

Secondo **ENISA** e **Clusit**, oltre il 70% degli attacchi informatici che colpiscono le PMI ha origine da **comportamenti involontari**:

- Click sbagliati,
- Password riutilizzate,
- Allegati aperti senza controllo,
- Procedure ignorate.

Ma il vero rischio **non è il click**, è **la mancanza di consapevolezza**.

Cultura e Formazione

La Prima Linea di Difesa
CIS Control 14

La ***cultura della sicurezza*** è il primo e più efficace firewall umano.

Non si costruisce con policy o tecnologie, ma con **abitudini condivise e comportamenti consapevoli.**

Significa trasformare la sicurezza da obbligo percepito a **valore riconosciuto**, parte integrante della quotidianità lavorativa.

Il **CIS Control 14** lo definisce chiaramente:

"All employees, contractors, and third-party users must receive appropriate awareness training to recognize and report potential security incidents."

Tradotto:

La formazione è una **misura tecnica**, non un'**attività accessoria**.

Ogni collaboratore deve saper riconoscere e segnalare un comportamento anomalo, comprendere le conseguenze di un gesto digitale e agire nel rispetto delle procedure di sicurezza.

Una cultura matura parte da tre convinzioni:

- La sicurezza **aiuta il lavoro**, non lo ostacola.
- Proteggere i dati significa **proteggere le persone e la reputazione aziendale**.
- La fiducia digitale è un **vantaggio competitivo**, non un costo.

Quando tutti comprendono il *"perché"*, rispettare il *"come"* diventa molto più semplice.

Cultura e Competenze

Dalla Formazione al Coinvolgimento Attivo

Per rendere la sicurezza parte della quotidianità, la formazione deve essere **continua, breve** e **concreta**, non un evento una tantum.

In linea con le best practices del **CIS Control 14**, i programmi più efficaci combinano:

1. **Micro-learning periodico**
   a. Brevi moduli di 5–10 minuti su temi pratici (phishing, uso password, gestione dati, AI).
   b. **Più brevi, più frequenti, più assimilabili**.
2. **Simulazioni di phishing**
   a. Esercitazioni pratiche che aiutano le persone a riconoscere comportamenti rischiosi in un ambiente controllato.
   b. Lo scopo **non è punire**, ma **allenare la percezione del rischio**.
3. **Playbook e checklist operative**
   a. Procedure semplici e visive (*"Cosa fare se..."*), facilmente consultabili e integrate nei flussi di lavoro.
   b. **La semplicità è la chiave della memoria.**

Ogni attività deve essere **misurata** come un qualsiasi controllo tecnico.

Una cultura della sicurezza che non si misura, come i KPI tecnici, **tende a disperdersi nel tempo**.

3 Pratiche di Consapevolezza da Introdurre Subito

Per rafforzare da subito il *comportamento digitale quotidiano*, ecco tre azioni ad alto impatto e a basso costo, applicabili in qualunque contesto aziendale:

1. **Stop & Check prima del click**
   a. Un principio di pausa consapevole: prima di aprire un allegato, cliccare un link o approvare una richiesta, fermati 5 secondi e verifica la fonte.
   b. Riduce **fino al 60% degli attacchi di phishing** basati su errore umano.
2. **Aggiornamenti con responsabilità personale**
   a. Ogni utente è responsabile dei propri dispositivi.
   b. Promuovere la *"cura digitale"* individuale (aggiornamenti, backup, password robuste) rafforza l'intero ecosistema aziendale.
3. **Canale di segnalazione immediata**
   a. Creare un indirizzo o canale dedicato (es. sicurezza@azienda.it o Teams) per segnalare email sospette o comportamenti anomali.
   b. La velocità di segnalazione è la miglior alleata della risposta.

Cultura e Competenze

L'Alleanza tra Umani e Automazione

L'evoluzione tecnologica, in particolare l'intelligenza artificiale, **non deve sostituire le persone, ma potenziarle.**

Il futuro della sicurezza è fatto di **umani assistiti dall'AI**, non rimpiazzati da essa.

- Sistemi che segnalano comportamenti anomali.
- Assistenti che aiutano a riconoscere email sospette.
- Automazioni che eliminano attività ripetitive, lasciando agli umani le decisioni critiche.

Quando persone e automazione collaborano, la sicurezza diventa **più intelligente, più rapida** e **più sostenibile**.

La Cultura come Parte del Miglioramento Continuo

La formazione e la cultura seguono la stessa logica del ***continuous improvement***:

- **Misurare,**
- **Adattare,**
- **Migliorare.**

Ogni ciclo formativo o simulazione deve chiudersi con una domanda semplice:

"Cosa abbiamo imparato che ci rende più resilienti oggi rispetto a ieri?"

Questo approccio trasforma la sicurezza da insieme di regole a **comportamento collettivo.**

Le persone non sono più il punto debole:

Diventano la prima risorsa di resilienza.

La Sicurezza come Collaborazione

In definitiva, la sicurezza non è un software, un reparto o un controllo tecnico:

È una **collaborazione continua** tra tecnologia, processi e persone.

Quando tutti questi elementi lavorano insieme, la *digitalizzazione* smette di essere un rischio e diventa una leva di **fiducia, reputazione** e **continuità**.

La cultura della sicurezza è ciò che tiene unito tutto il *Blueprint*:

Il filo invisibile che collega identità, dispositivi, dati e governance, trasformando la sicurezza da vincolo tecnico a **vantaggio competitivo sostenibile**.

Conclusione

Dal Caos alla Governance

Ogni azienda, grande o piccola, vive oggi dentro un ***ecosistema digitale complesso***.

Sistemi interconnessi, dati in movimento, strumenti sempre più potenti, ma anche più fragili.

In questo contesto, la **governance** non è un lusso da grandi imprese, è la condizione minima per garantire **continuità** e **fiducia**.

Digitalizzare senza struttura è come costruire un edificio senza fondamenta, all'inizio sembra solido, ma al primo urto si incrina.

Il *Blueprint di Digitalizzazione Sicura* nasce proprio per questo:

Offrire **una base stabile e sostenibile**, capace di crescere nel tempo e adattarsi a contesti diversi.

Dalla Complessità alla Chiarezza

Il percorso che hai letto non è un progetto teorico, ma **un metodo di semplificazione.**

Non serve *"fare di più"*, serve **fare meglio,** con regole, priorità e processi che tutti possano comprendere e applicare.

Il principio del *minimo sostenibile* è la sintesi perfetta:

- Ridurre la complessità,
- Aumentare la continuità,
- Migliorare la fiducia.

Ogni passo, dalla visibilità iniziale ai KPI di maturità, dalla formazione alla resilienza, costruisce una sicurezza che non rallenta, ma **abilita il business**.

Governance come Cultura

La governance non è solo controllo, è **consapevolezza organizzata**.

Significa sapere dove si trovano i dati, chi li usa, come si proteggono e come ripartire se qualcosa si interrompe.

È la capacità di **gestire l'imprevisto senza interrompere il valore**.

Questo è il cuore della *digitalizzazione sicura*:

Una combinazione di tecnologia, metodo e cultura che trasforma la sicurezza da ostacolo a **fattore di fiducia,** interna ed esterna.

Quando un'organizzazione riesce a integrare questi tre elementi, smette di inseguire il cambiamento:

Inizia a guidarlo.

Conclusione

I Tre Messaggi Chiave del Blueprint

Tutto il percorso può essere riassunto in tre parole che rappresentano la filosofia alla base di questo eBook:

1. **Visione**: Guardare oltre la tecnologia, comprendendo l'impatto organizzativo della sicurezza.
2. **Metodo:** Adottare standard, processi e metriche misurabili per dare struttura e coerenza.
3. **Continuità:** Mantenere ciò che funziona, migliorando passo dopo passo, in un ciclo costante di evoluzione.

Questi tre principi, visione, metodo e continuità, sono ciò che trasforma la sicurezza da progetto tecnico a **motore di resilienza e competitività**.

Il Manifesto Finale

"La digitalizzazione sicura non è un lusso, è ciò che ti permette di restare operativo quando gli altri si fermano."

In questa frase si riassume tutto:

La digitalizzazione non è una corsa alla tecnologia, ma una **disciplina di continuità**.

La differenza tra un'azienda vulnerabile e una solida non è il budget, ma **la capacità di prevedere, misurare** e **migliorare**.

Ogni impresa può costruire la propria resilienza digitale, a partire dal suo *minimo sostenibile*:

Un passo alla volta, con **metodo**, **visione** e **cultura**.

Il Prossimo Passo

Ogni *Blueprint* è una mappa, ma serve qualcuno che inizi a percorrerla.

Il primo passo è sempre lo stesso, **guardarsi dentro**.

- Sai quali asset digitali gestisci oggi?
- Hai procedure semplici per rispondere a un incidente?
- I tuoi dati più critici sarebbero accessibili domani, se oggi tutto si fermasse?

Se queste domande non hanno una risposta immediata, significa che **il percorso di governance può iniziare proprio da qui**.

Questo eBook non chiude un discorso, lo apre.

È un invito ad adottare un modo di pensare diverso, **più strutturato, più consapevole**, **più umano**.

Perché la vera sicurezza non è quella che blocca, ma quella che **permette di continuare**.

Appendice

Strumenti & Template Pratici

Il valore di un *Blueprint* si misura nella sua applicabilità.

Questa sezione raccoglie strumenti, riferimenti e schemi operativi per aiutarti a **tradurre i principi del modello in azioni concrete**.

Sono materiali essenziali, selezionati per PMI e organizzazioni che vogliono costruire resilienza digitale in modo sostenibile, partendo dal proprio *"minimo sostenibile"*.

Checklist dei 10 Controlli Essenziali

CIS v8 - Implementation Group 1

Il CIS Controls v8 definisce un set di controlli prioritari per le organizzazioni con risorse limitate ma esigenze operative reali.

Questi 10 controlli rappresentano la base minima per ridurre in modo significativo la superficie d'attacco di una PMI.

Controllo	Obbiettivo Principale
1. Inventory and Control of Enterprise Assets	Sapere cosa proteggere
2. Inventory and Control of Software Assets	Evitare software non autorizzato
3. Data Protection	Garantire integrità e riservatezza
4. Secure Configuration of Assets	Evitare vulnerabilità predefinite
5. Account Management	Ridurre account inutilizzati o privilegiati
6. Access Control Management	Applicare principio del least privilege
7. Continuous Vulnerability Management	Intervenire sulle falle note
8. Audit Log Management	Tracciare azioni e anomalie
9. Email and Web Browser Protections	Difendersi da phishing e exploit
10. Malware Defenses	Rilevare e bloccare minacce note

Suggerimento Operativo:

Implementa almeno i controlli 1–5 nei primi 60 giorni e 6–10 nei successivi 90.

Questa sequenza garantisce equilibrio tra visibilità, controllo e reattività.

Appendice

Schema di Governance per PMI (Ruoli, RACI, Escalation)

Una buona governance non richiede strutture complesse, ma **chiarezza nei ruoli e nei flussi decisionali.**

Lo schema seguente rappresenta una struttura base, adattabile a realtà di piccole e medie dimensioni.

Ruoli Chiave

Ruolo	Responsabilità Principale
Owner / Direzione	Definisce la strategia e approva le priorità di sicurezza
IT / System Admin	Implementa e mantiene controlli tecnici e infrastrutture
Security / Compliance Lead	Supervisiona rischi, policy e conformità (può coincidere con IT in PMI.
DPO / Privacy Officer	Garantisce la conformità al GDPR e la gestione dei dati personali
Tutti i dipendenti	Rispettano policy e segnalano comportamenti anomali

Mini RACI Matrix (Semplificata)

Attività	Owner	Security Lead	IT	DPO	Utenti
Gestione Account e Accessi	A	C	R	I	I
Backup e Ripristino	A	C	R	I	I
Gestione Incidenti	A	C	R	C	R
Aggiornamenti Software	I	C	R	I	-
Formazione e Awareness	A	R	C	I	R

Legenda:

R = Responsible A = Accountable C = Consulted I = Informed

Appendice

Flusso di Escalation

1. **Segnalazione immediata** da parte dell'utente o tecnico (entro 15 min).
2. **Verifica preliminare** da parte del Security Lead o IT.
3. **Decisione operativa** (mitigazione, isolamento, recovery).
4. **Comunicazione interna** e registrazione dell'incidente.
5. **Analisi post-evento** e aggiornamento procedure.

Questo schema assicura rapidità, responsabilità e apprendimento continuo dopo ogni evento.

Link Utili e Risorse di Riferimento

Un percorso di digitalizzazione sicura deve basarsi su standard riconosciuti e aggiornati.

Ecco alcune risorse autorevoli per approfondire i temi trattati nel *Blueprint*:

ENISA - SME Cybersecurity Guide, enisa.europa.eu

NIST Cybersecurity Framework 2.0, nist.gov

CIS Critical Security Controls v8, cisecurity.org

ISO/IEC 27001:2022, iso.org

NIST IR 8286 - Integrating Cybersecurity and ERM, csrc.nist.gov

Come Usare Questa Appendice

- **Personalizza**: adatta la checklist ai tuoi asset e processi.
- **Centralizza**: raccogli i dati in un unico documento o dashboard.
- **Ripeti**: aggiorna ogni trimestre i controlli e le responsabilità.

La sostenibilità digitale nasce dalla **costanza nei piccoli gesti**:

Questa appendice è il punto di partenza per costruire una sicurezza quotidiana, concreta e condivisa.

Chi Sono e Perché mi occupo di Digitalizzazione Sicura

Sono **Dennis Sepede, Co-Founder e CTO di Securitix Solutions**.
Lavoro nel campo della **cybersecurity**, della **governance digitale** e della **resilienza operativa**, supportando aziende e organizzazioni nel rendere la tecnologia una **leva di fiducia**, non di complessità.

Nel mio percorso ho collaborato con imprese di settori diversi, dal manifatturiero ai servizi digitali, aiutandole a costruire **infrastrutture sicure**, **processi efficienti** e una **cultura consapevole della sicurezza**.
Negli anni ho compreso che la vera differenza non la fanno le **soluzioni costose**, ma la **chiarezza del metodo** e la **continuità delle persone** che lo applicano.

Mission Personale

"Diffondere un approccio pragmatico alla cybersecurity nelle PMI."

Credo che ogni impresa, indipendentemente dalle dimensioni, possa implementare **sicurezza sostenibile e misurabile**, basata su standard internazionali e buone pratiche operative.
La mia missione è **semplificare la sicurezza**, **renderla accessibile** e **integrarla nei processi aziendali** come fattore di competitività e crescita.

Vision

"Credo in una sicurezza che libera, non che complica."

La sicurezza dovrebbe **liberare il potenziale digitale** delle persone e delle imprese, non ostacolarlo.
Per questo promuovo un **modello di digitalizzazione** che mette al centro la **fiducia**, la **trasparenza** e la **sostenibilità tecnologica**, tre pilastri per costruire continuità nel tempo.

Contatti

LinkedIn: linkedin.com/in/dennis-sepede-cybersecurity
Sito web: www.securitixsolutions.com

Securitix Solutions

Securitix Solutions aiuta imprese e organizzazioni a costruire **fiducia digitale** attraverso un approccio integrato di **formazione**, **governance** e **sicurezza informatica**.

Scopri di più su securitixsolutions.com

Blueprint di Digitalizzazione Sicura

Dal caos all'operatività: il modello "minimo sostenibile" per PMI che vogliono crescere senza esporsi

---

"La digitalizzazione sicura non è un lusso: è ciò che ti permette di restare operativo quando gli altri si fermano."

Una frase semplice, ma che racchiude l'essenza di tutto questo eBook: la sicurezza non è un ostacolo alla digitalizzazione, è la condizione che la rende possibile.
È ciò che separa chi reagisce da chi governa, chi subisce gli eventi da chi continua a creare valore.

Un metodo pratico, non teoria

Questo eBook nasce dall'esperienza diretta sul campo con decine di PMI italiane che hanno affrontato la trasformazione digitale senza perdere la bussola.
Propone un modello operativo basato su standard internazionali (NIST, ISO 27001, CIS) per passare dal caos alla governance con azioni concrete, sostenibili e misurabili.

Un percorso per costruire continuità, fiducia e resilienza digitale, anche con risorse limitate, ma con metodo e visione.

Dennis Sepede

Specialista in cybersecurity, governance e digitalizzazione per PMI.
Aiuta imprese e organizzazioni a trasformare la sicurezza da costo a vantaggio competitivo, con un approccio umano, metodico e sostenibile.

🔗 linkedin.com/in/dennis-sepede-cybersecurity
🌐 www.securitixsolutions.com

Vuoi approfondire?

Richiedi un Assessment iniziale con il team Securitix.
Segui Dennis su LinkedIn per insight settimanali su AI, cybersecurity e governance.

Securitix

Liberiamo le aziende dalla complessità digitale, rendendole più sicure e resilienti.

www.securitixsolutions.com