Deloitte.

Sicurezza e resilienza infrastrutturale

Supporti, presidi e leve per proteggere il valore

#4

01.

Da infrastrutture critiche a ecosistemi interdipendenti

Le infrastrutture critiche costituiscono la base per il funzionamento quotidiano dell'economia e della società, garantendo la continuità di servizi essenziali quali energia, trasporti, servizi finanziari, salute, infrastrutture digitali e Pubblica Amministrazione (PA). La crescente interconnessione tra sistemi fisici, digitali, organizzativi e catene di fornitura fa sì che un'interruzione, inizialmente circoscritta, possa propagarsi oltre il singolo asset, generando effetti a cascata con impatti su infrastrutture, settori e territori diversi. La criticità non dipende più esclusivamente dalla rilevanza del singolo asset, ma dalla funzione che esso abilita e dalle relazioni di dipendenza che ne condizionano la continuità.

La Direttiva dell'Unione Europea (UE) 2022/2557[1,2], il Critical Entities Resilience Directive (CER), sulla resilienza dei soggetti critici, riconosce esplicitamente questa evoluzione, sottolineando come la fornitura dei servizi sia sempre più transfrontaliera e come le interdipendenze tra infrastrutture e settori possano amplificare gli effetti di un incidente. La Direttiva introduce per questo un quadro generale per rafforzare la resilienza dei soggetti critici rispetto a rischi naturali e antropici, accidentali o intenzionali. Il passaggio dalla protezione della singola infrastruttura ad un approccio orientato alla resilienza dei soggetti critici riflette quindi la necessità di considerare non solo la sicurezza dell'asset ma anche la continuità del servizio.

In questo contesto, sicurezza e resilienza rappresentano due dimensioni complementari: la prima mira a proteggere persone, siti, infrastrutture e asset dalle minacce che possono comprometterne l'integrità, la seconda riguarda la capacità di prevenire, resistere, rispondere, assorbire e recuperare da eventi che interrompono o degradano le funzioni essenziali.

Ne deriva una prospettiva nella quale anche la resilienza deve essere valutata considerando le dipendenze che collegano un soggetto agli altri attori dell'ecosistema: la capacità di garantire un servizio essenziale dipende infatti sia dalla resilienza delle proprie infrastrutture, sia da quella dei servizi e delle risorse da cui il soggetto stesso dipende.

Il settore bancario rappresenta in questo senso uno snodo centrale dell'ecosistema delle infrastrutture critiche: attraverso i sistemi di pagamento, le piattaforme digitali e i servizi finanziari, garantisce la circolazione del valore tra imprese, istituzioni e cittadini e svolge un ruolo essenziale nel funzionamento dell'economia. La sua rilevanza sistemica rende quindi la resilienza del settore un elemento importante per la stabilità e la continuità del più ampio ecosistema economico e infrastrutturale.

Un'infrastruttura può dipendere contemporaneamente da energia, telecomunicazioni, sistemi digitali, persone, processi, fornitori e servizi esterni, e l'indisponibilità di uno di questi elementi può compromettere una funzione critica anche in assenza di un danno diretto all'asset.

La sicurezza infrastrutturale non riguarda più la protezione di singoli asset ma di ecosistemi interconnessi dove una disruption può propagarsi lungo infrastrutture, reti digitali, fornitori e catene di approvvigionamento, generando un effetto moltiplicatore con impatti rilevanti per il Sistema Paese.

La vulnerabilità di un elemento diventa rischio sistemico quando compromette funzioni da cui dipendono altri servizi essenziali. Le interdipendenze richiedono di mappare non solo cosa proteggere, ma anche quali conseguenze e da quali risorse dipende un'interruzione dell'intero ecosistema. Il quadro normativo europeo (CER, NIS2, DORA, CRMA) impone un approccio integrato: protezione, rilevazione, risposta e recupero convergono verso una capacità comune di assorbire e recuperare dalle disruption, con la sicurezza che rappresenta una leva di valore e resilienza per garantire continuità operativa anche in condizioni avverse

Note: [1]Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Unione Europea (2022) | [2]«Making critical entities more resilient», Summary of Directive 2022/2557 on the resilience critical entities, Unione Europea (2022)

Un'interruzione dell'energia può, ad esempio, compromettere il funzionamento di data center e reti di comunicazione, mentre un malfunzionamento dei sistemi di pagamento o l'indisponibilità di un fornitore critico possono produrre effetti sulla continuità di funzioni essenziali senza che l'organizzazione subisca alcun danno diretto. La vulnerabilità di un singolo elemento può quindi trasformarsi in un rischio sistemico quando coinvolge funzioni dalle quali dipendono altri servizi essenziali.

La European Preparedness Union Strategy[3,4], presentata dalla Commissione Europea (CE) nel marzo 2025 per rafforzare la capacità dell'Unione e degli Stati membri di anticipare, prevenire e rispondere alle minacce emergenti, evidenzia come i rischi contemporanei richiedano una approccio integrato alla preparazione e alla gestione delle crisi. La strategia si fonda, in particolare, su un approccio «all-hazards», volto a considerare congiuntamente le diverse tipologie di rischio, e su un approccio «whole-of-society», che prevede il coinvolgimento di tutti i settori, delle organizzazioni e della popolazione nel suo complesso. A questi si affianca un approccio «whole-of-government», basato sul coordinamento tra le diverse amministrazioni e livelli di governo.

La preparazione alla crisi viene quindi concepita non come responsabilità del singolo operatore, ma come una capacità collettiva da costruire attraverso cooperazione, coordinamento e condivisione delle informazioni tra soggetti pubblici e privati.

In questo quadro, risultano particolarmente rilevanti alcuni settori strategici, tra cui Energia, Trasporti, Servizi Finanziari, Infrastrutture dei Mercati Finanziari, Salute, Infrastrutture Digitali e PA. Questo perimetro, coerente con i principali settori individuati dalla Direttiva CER[5], è caratterizzato da elevata criticità e forti interdipendenze fisiche, digitali, finanziarie e organizzative.

In particolare, la loro centralità deriva da tre elementi fondamentali:

- Ruolo e funzione essenziale per cittadini, imprese e istituzioni
- Elevata interdipendenza, che rende la continuità dei servizi legata alla resilienza dei sistemi
- Esposizione a diverse tipologie di rischio, tra cui minacce fisiche, tecnologiche, organizzative e di supply chain

Queste caratteristiche fanno sì che i settori strategici siano reciprocamente abilitanti: la resilienza di ciascun ecosistema contribuisce alla resilienza dell'intero sistema.

La Direttiva CER[5] collega infatti l'identificazione dei soggetti critici anche alla possibilità che un incidente produca effetti significativi sulla fornitura di altri servizi essenziali dipendenti dal servizio interessato. Nel settore bancario, il Comitato di Basilea[6] richiede inoltre agli intermediari di identificare le operazioni critiche e di mappare le interconnessioni e interdipendenze interne ed esterne necessarie alla loro erogazione, includendo

«Diventa necessario comprendere quali siano le funzioni essenziali della società, da quali risorse dipendano e quali conseguenze un'eventuale interruzione possa produrre sugli altri soggetti e sulle funzioni collegate»

persone, tecnologia, processi, informazioni, strutture e terze parti. Questi principi trovano un ulteriore riscontro nel quadro presentato dal Digital Operational Resilience Act[7] (DORA), che rafforza l'attenzione alla resilienza operativa e alla gestione delle dipendenze necessarie alla continuità delle funzioni critiche. Tale approccio consente di individuare le vulnerabilità lungo la rete di dipendenze e di verificare la capacità di mantenere le operazioni critiche durante una disruption.

In questo contesto diventa necessario comprendere quali siano le funzioni essenziali della società, da quali risorse dipendano e quali conseguenze un'eventuale interruzione possa produrre sugli altri soggetti e sulle funzioni collegate. La prospettiva si sposta così da una logica prevalentemente asset-centric ad una logica ecosystem-centric: non si tratta soltanto di proteggere ciò che è critico, ma di assicurare che ciò che è critico continui a funzionare, anche quando una parte dell'ecosistema è sottoposta a stress.

Note: [3]EU Preparedness Union Strategy, CE (2025) | [4]Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, UE (2025) | [5]Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, UE (2022) | [6]Basel Consolidated Guidelines, Basel Committee on Banking Supervision | [7]Digital Operational Resilience Act, Unione Europea

02.

I rischi associati agli ecosistemi critici: natura, geopolitica, tecnologia, finanza

La crescente interdipendenza tra infrastrutture, imprese, mercati e catene di fornitura amplia il perimetro dei rischi che possono compromettere la continuità dei servizi essenziali. Eventi naturali, tensioni geopolitiche, minacce cyber e shock finanziari possono infatti agire simultaneamente e propagarsi attraverso soggetti e settori, rendendo necessario un approccio integrato alla prevenzione e alla resilienza.

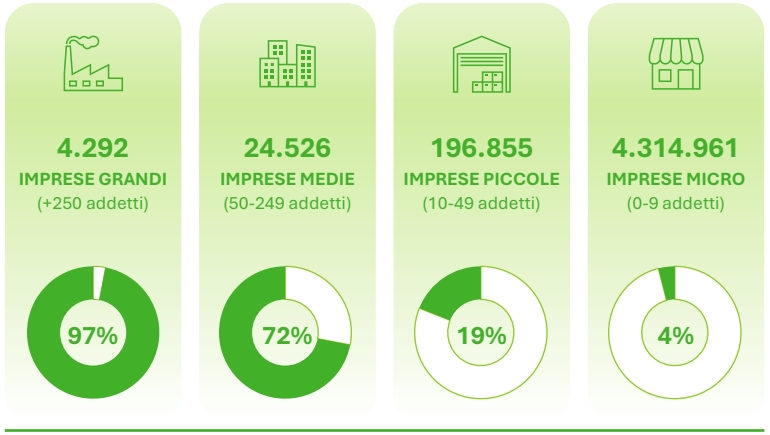
Rischi naturali e climatici

La crescente esposizione a eventi climatici rafforza questa necessità. La European Climate Risk Assessment (EUCRA) dell'European Environmental Agency (EEA) ha identificato 36 principali rischi climatici[8], raggruppati in cinque macro-cluster: (i) ecosistemi, (ii) cibo, (iii) salute, (iv) infrastrutture ed (v) economia e finanza, evidenziando come gli impatti del cambiamento climatico possano produrre effetti simultanei su più settori e funzioni critiche. In questo quadro, il rischio derivante da catastrofi naturali (Cat Nat) assume particolare rilievo: a livello UE, le perdite economiche da eventi meteorologici e climatici estremi hanno raggiunto €822 mld nel periodo 1980-2024[9], con Italia, Germania, Francia e Spagna tra i Paesi più colpiti. Ne deriva la crescente rilevanza di prevenzione, adattamento e trasferimento assicurativo del rischio per la resilienza di imprese e territori. *(Figura 1[10])*

Rischi geopolitici

Le tensioni geopolitiche, la frammentazione commerciale e le restrizioni agli scambi possono incidere sulla disponibilità di input critici, energia e componenti strategiche, trasformando uno shock esterno in una disruption operativa. La vulnerabilità delle catene di fornitura è significativa: secondo una survey della Banca Centrale Europea (BCE), il 55%[11,12] delle imprese intervistate approvvigiona input critici in modo rilevante da uno specifico Paese o gruppo di Paesi e, nel 52%[12] dei casi complessivi tale dipendenza è considerata esposta a un rischio elevato. La resilienza richiede quindi di considerare concentrazione geografica dei fornitori, dipendenze strategiche e capacità di sostituzione degli input critici.

Figura 1. Stima imprese assicurate in Italia per cluster dimensionale



Rischi cyber e di protezione

La progressiva dipendenza da infrastrutture e servizi digitali amplia la superficie di esposizione e rafforza le interdipendenze tra sistemi, organizzazioni e catene di fornitura. Secondo l'ENISA Threat Landscape 2025[13], il report dell'Agenzia dell'UE per la cybersicurezza, nel periodo luglio 2024 – giugno 2025 sono stati analizzati 4.875 incidenti cyber nell'UE. Tra gli incidenti per i quali il settore è stato identificato, la PA è risultata il settore maggiormente colpito, seguita da trasporti, infrastrutture e servizi digitali e finanza; il 53,7% degli incidenti complessivi ha coinvolto entità classificate come «essential entities» ai sensi della Direttiva NIS2[14]. Il dato conferma come le minacce digitali interessino in misura significativa gli ambiti che abilitano funzioni essenziali e come la compromissione di una dipendenza tecnologica possa amplificare l'impatto di un incidente oltre il perimetro dell'organizzazione colpita.

Rischio di credito e convergenza sistemica

Rischi fisici, geopolitici e cyber possono tradursi in rischio finanziario attraverso interruzioni operative, riduzione dei ricavi, perdita di valore degli asset e maggiore probabilità di default. La convergenza tra queste categorie rende il rischio non lineare: un singolo evento può attivare simultaneamente più canali di trasmissione e amplificare gli effetti lungo la rete di interdipendenze. La capacità di resilienza dipende pertanto non solo dall'esposizione al singolo rischio, ma dalla posizione del soggetto nell'ecosistema e dalla robustezza delle dipendenze critiche che ne sostengono le funzioni.

Note: [8]European Climate Risk Assessment, EEA (2024) | [9]Economic losses from weather- and climate-related extremes in Europe, EEA (2025) | [10]Allontaniamo i rischi rimaniamo protetti, ANIA (2024) | [11]ECB Occasional Paper Series No 365 (2024) | [12]Global production and supply chain risks: insights from a survey of leading companies, European Central Bank (2023) | [13]ENISA Threat Landscape (2025) | [14]Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), UE (2022)

03.

La resilienza delle infrastrutture passa attraverso le supply chain oltre i confini Paese

Se la continuità di una funzione critica dipende da una rete di infrastrutture e fornitori, una fonte ulteriore di vulnerabilità è costituita dalle dipendenze che si estendono oltre i confini Paese.

Se da un lato l'integrazione in supply chain e catene del valore globali consentono all'economia europea di accedere a materie prime, componenti, tecnologie e servizi essenziali, dall'altro aumentano l'esposizione a shock geopolitici, commerciali e logistici. La vulnerabilità cresce soprattutto quando la fornitura è concentrata in pochi Paesi e la sostituibilità delle risorse è limitata. In questi casi, un'interruzione localizzata della produzione o dei flussi commerciali può propagarsi lungo la filiera, trasformandosi in una criticità per la continuità operativa di infrastrutture e servizi essenziali.

La dimensione dell'esposizione emerge chiaramente nel caso delle materie prime critiche. L'European Critical Raw Materials Act[15] (CRM Act), pubblicato dalla CE nel Marzo 2023, evidenzia che il 63% del cobalto mondiale, utilizzato nelle batterie, è estratto nella Repubblica Democratica del Congo; il 97% della fornitura UE di magnesio proviene dalla Cina; il 98% della fornitura UE di borato, con impieghi che spaziano dall'industria chimica ai materiali da costruzione, proviene dalla Turchia.

I dati evidenziano che il rischio non riguarda solo la disponibilità fisica della risorsa, ma soprattutto la capacità di mantenere operative le funzioni che da essa dipendono, anche in presenza di shock prolungati o di interruzioni improvvise delle forniture.

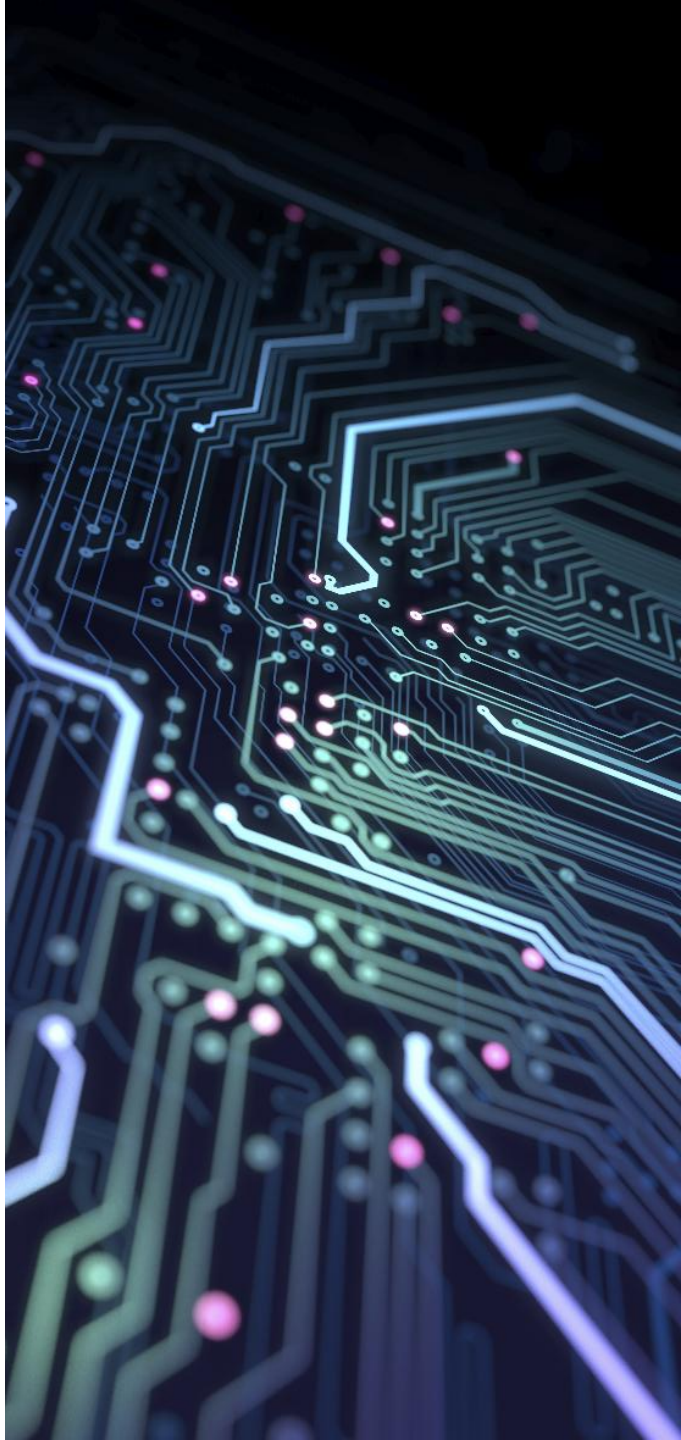
La dipendenza da un numero ristretto di fornitori o di Paesi può quindi costituire una vulnerabilità sistemica, soprattutto quando i tempi necessari per individuare fonti alternative, riconfigurare la produzione o sostituire un componente sono elevati.

Il CRM Act[15] fissa inoltre, entro il 2030, specifici obiettivi per rafforzare la capacità dell'UE lungo la filiera delle materie prime strategiche: la capacità di estrazione dovrebbe coprire almeno il 10% del consumo annuo dell'UE, quella di trasformazione almeno il 40% e quella di riciclo almeno il 25%. Inoltre, per diversificare le importazioni, nessun singolo Paese terzo dovrebbe fornire più del 65% del consumo annuo di ciascuna materia prima strategica[16].

Il CRM Act[15] mostra quindi come la resilienza non sia soltanto una questione di protezione dell'infrastruttura, ma anche di riduzione delle dipendenze critiche, diversificazione delle fonti di approvvigionamento e capacità di riconfigurare rapidamente le catene del valore in risposta a uno shock.

Questa logica è particolarmente rilevante per infrastrutture digitali ed energetiche, nelle quali la disponibilità di componenti, tecnologie e materie prime può rappresentare un prerequisito per la continuità del servizio, ma si riflette indirettamente anche sugli altri settori.

La sicurezza infrastrutturale assume quindi una dimensione di filiera: proteggere l'asset senza presidiare le dipendenze esterne che ne sostengono il funzionamento può lasciare irrisolta una parte rilevante della vulnerabilità complessiva.



Note: [15]European Critical Raw Materials Act, Commissione Europea (Marzo 2023) | [16]Regulation (EU) 2024/1252 of the European Parliament and of the Council, Unione Europea (Aprile 2024)

04.

Il quadro normativo europeo: dalla protezione dell'infrastruttura alla resilienza dell'ecosistema

L'evoluzione delle minacce e delle interdipendenze si riflette nella progressiva costruzione di un quadro normativo europeo che interviene su dimensioni diverse ma complementari. I principali riferimenti sono:

- **CER[17]:** mira a rafforzare la resilienza fisica delle entità critiche attraverso un approccio all-hazards, considerando rischi naturali, accidentali e intenzionali
- **CRMA[18]:** interviene sulla resilienza delle catene di approvvigionamento, promuovendo sicurezza e diversificazione delle materie prime strategiche
- **AI Act[19]:** fornisce i requisiti per l'adozione di sistemi di Artificial Intelligence ad alto rischio, inclusi quelli impiegati per le componenti di sicurezza delle infrastrutture critiche
- **DORA[20]:** introduce specifici requisiti di resilienza operativa digitale per il settore finanziario, con focus sul rischio Information and Communication Technology (ICT), sulla gestione del rischio delle terze parti ICT, sugli incidenti, sul testing e sulla continuità operativa
- **Cyber Resilience Act[21]:** estende il presidio alla sicurezza dei prodotti con elementi digitali lungo l'intero ciclo di vita
- **NIS2[22]:** ha l'obiettivo di rafforzare la resilienza cyber delle entità essenziali e importanti, intervenendo su gestione del rischio, incidenti, supply chain e responsabilità del management

Nel loro insieme, questi atti evidenziano il progressivo superamento del concetto di sicurezza focalizzato sul singolo asset a favore di un modello orientato alla resilienza operativa e alla continuità dei servizi essenziali, quale presupposto per la tutela della clientela e della stabilità del sistema Paese e finanziario. La convergenza dei sistemi richiede un modello integrato di gestione del rischio, capace di presidiare le interdipendenze tra banche, infrastrutture, fornitori e servizi critici, valutandone gli impatti lungo l'intera catena di erogazione dei servizi.

Il recepimento in Italia

In Italia[23] le Direttive CER[17] e NIS2[22] sono state recepite attraverso il D.Lgs. 4 settembre 2024 n. 134 e n. 138. Nell'ambito dell'adeguamento dell'ordinamento italiano al quadro DORA[20], è inoltre intervenuto il D.Lgs. 10 marzo 2025, n. 23[24]. Tali provvedimenti rafforzano il sistema nazionale di resilienza considerando, da un lato, la gestione dei rischi e la continuità dei servizi essenziali e, dall'altro, la sicurezza delle reti e dei sistemi informativi e la gestione del rischio cyber.

Note: [17]Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Unione Europea | [18]CRMA, Unione Europea | [19]AI Act, Unione Europea | [20]DORA, Unione Europea | [21]Cyber Resilience Act, Unione Europea | [22]Direttiva NIS 2, Unione Europea | [23]D.Lgs. 4 settembre 2024, n. 134 e n. 138 | [24]D.Lgs 10 marzo 2025, n. 23

05.

I presidi: dalla protezione del singolo asset ad un framework integrato di Operational Resilience

Con l'ampliamento del perimetro di rischio, anche i presidi devono evolvere, passando da un approccio basato su controlli distinti a framework integrati in grado di prevenire e rilevare le minacce, contenere gli impatti degli eventi avversi e assicurare il rapido ripristino delle funzioni e dei servizi prioritari.

Un framework integrato di sicurezza e resilienza operativa può essere ricondotto alle sei funzioni del NIST Cybersecurity Framework (CSF) 2.0[25]:

- **Govern:** definizione di strategie, policy, ruoli e responsabilità per governare i rischi cyber e di resilienza
- **Identify:** identificazione e valutazione di asset, dipendenze, vulnerabilità e rischi rilevanti
- **Protect:** protezione di persone, sedi e asset da minacce fisiche e tecnologiche
- **Detect:** rilevazione di anomalie e segnali di minaccia attraverso monitoring, sensoristica e analytics
- **Respond:** risposta immediata agli eventi per contenere l'impatto e garantire le funzioni prioritarie
- **Recover:** ripristino rapido di servizi e operatività attraverso business continuity e disaster recovery

A queste sei funzioni si affianca, come elemento trasversale, la gestione delle interdipendenze, necessaria per comprendere quali persone, tecnologie, processi, informazioni, strutture e soggetti terzi siano indispensabili alla continuità delle funzioni critiche e come un'interruzione in uno di questi elementi possa propagarsi all'interno dell'ecosistema.

Le guidelines elaborate nell'ambito del Comitato di Basilea[26,27] ribadiscono che la mappatura delle dipendenze rappresenta un prerequisito fondamentale per il settore bancario. DORA[28] rafforza questa impostazione introducendo per il settore finanziario un framework di resilienza operativa che collega la gestione dei rischi alla capacità di mantenere la continuità delle funzioni critiche, anche in presenza di eventi avversi. Tuttavia, la valutazione dei presidi deve andare oltre la semplice identificazione delle vulnerabilità, valutando la massima interruzione che l'organizzazione può tollerare per ciascuna funzione critica. I presidi devono quindi essere calibrati su questa tolleranza e verificati attraverso stress test che simulino scenari di disruption severa.

Il presidio efficace non consiste quindi nel massimizzare ogni singola misura di sicurezza ma nel garantire che l'insieme dei presidi sia coerente con la criticità della funzione e con la capacità dell'organizzazione di mantenerla operativa in condizioni avverse. La valutazione dei presidi deve pertanto partire dalle funzioni critiche e dalle relative tolleranze all'interruzione per identificare le misure di protezione, rilevazione, risposta e recupero necessarie a mantenerne la continuità.

06.

Tecnologia e AI: dalla rilevazione alla capacità di anticipazione

La crescente complessità delle minacce rende la tecnologia una componente rilevante della resilienza, consentendo di correlare dati provenienti dai sistemi informatici, dalle infrastrutture fisiche e dai processi operativi, e individuare anomalie prima che si traducano in una disruption.

L'evoluzione va dalla semplice rilevazione dell'evento alla correlazione dei segnali, fino all'anticipazione delle anomalie e alla prioritizzazione delle azioni di risposta. AI e advanced analytics possono supportare attività di anomaly detection, predictive maintenance e decision-making durante una crisi.

Per generare valore, queste tecnologie devono essere integrate nei processi operativi e di governance, contribuendo a prevenire o ridurre l'impatto delle disruption e ad accelerarne la gestione.

Questa evoluzione porta con sé anche nuove esigenze di governo: l'AI Act[29] considera ad alto rischio determinati sistemi di AI impiegati come safety components nelle infrastrutture critiche, richiedendo specifici presidi di sicurezza, affidabilità e gestione del rischio.

La tecnologia rappresenta quindi una doppia sfida: leva per anticipare e gestire le minacce, ma anche componente critica da preservare e governare, in un modello in cui dati, tecnologie e capacità umane concorrono alla resilienza.

Note: [25]NIST Cybersecurity Framework (CSF) 2.0 (2024) | [26]Basel Consolidated Guidelines, Basel Committee on Banking Supervision | [27]Principles for operational resilience, Basel Committee on Banking Supervision | [28]Digital Operational Resilience Act, Unione Europea | [29]Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), Unione Europea (2024)

07.

La sicurezza come centro di valore: dal modello di costo al paradigma strategico

L'evoluzione delle interdipendenze, delle minacce e del quadro normativo porta a rivedere il ruolo della sicurezza all'interno delle organizzazioni. In un sistema interconnesso, il valore della sicurezza risiede nella capacità di proteggere la continuità delle funzioni da cui dipendono servizi, ricavi, fiducia e operatività. Questo implica un'evoluzione anche nelle modalità di misurazione. Accanto a indicatori tradizionali, tra cui incidenti, vulnerabilità e investimenti, assumono rilevanza metriche legate agli outcome, come tempo di ripristino, disponibilità dei servizi critici, tolleranza alla disruption, capacità di sostituzione e impatto su Clienti e stakeholder.

Il principio è particolarmente evidente nel settore finanziario, dove il framework di operational resilience del Comitato di Basilea[29,30] non assume che ogni disruption possa essere prevenuta, ma pone l'accento sulla capacità di continuare a erogare le operazioni critiche. Questa evoluzione trova riscontro anche nell'approccio regolamentare europeo che con DORA[31] porta la resilienza operativa al centro del modello di gestione del rischio degli intermediari finanziari. La stessa logica si estende agli altri settori: la resilienza si misura sulla capacità di assorbire l'impatto e mantenere operative le funzioni essenziali.

La sicurezza infrastrutturale evolve così da centro di costo a leva strategica: l'investimento genera valore quando protegge la continuità dei servizi, riduce l'esposizione alle disruption, rafforza la fiducia di Clienti e stakeholder e aumenta la capacità dell'organizzazione di operare in condizioni di incertezza.

08.

Conclusioni

La crescente interconnessione tra infrastrutture critiche, sistemi digitali, persone, fornitori e catene di approvvigionamento rende sempre più difficile separare sicurezza, continuità operativa e resilienza.

Conoscere le dipendenze critiche diventa il primo presupposto della resilienza: non è più sufficiente identificare gli asset strategici, ma occorre comprendere le funzioni che abilitano, le risorse da cui dipendono e gli effetti che la loro indisponibilità può generare sull'ecosistema.

Rafforzare i presidi rappresenta il secondo passaggio: protezione fisica, cybersecurity, continuità operativa, crisis management e gestione delle terze parti devono convergere verso una capacità comune di prevenire, assorbire e recuperare dagli eventi disruptive. In questo, la tecnologia costituisce una leva per migliorare la capacità di anticipazione, purché AI, analytics e sensoristica siano integrati nei processi, nella governance e nel modello complessivo di resilienza.

La sfida non consiste quindi nell'eliminare ogni possibile disruption, ma nella capacità di continuare ad erogare le funzioni essenziali quando si verifica un evento critico. In questa prospettiva, la sicurezza infrastrutturale non rappresenta più solo un presidio a difesa del valore, ma una capacità strategica per proteggerlo e preservarlo nel tempo.

.

Note: [29]Basel Consolidated Guidelines, Basel Committee on Banking Supervision | [30]Principles for operational resilience, Basel Committee on Banking Supervision | [31]Digital Operational Resilience Act, Unione Europea

Deloitte.

Deloitte Creative Team - Italia | SG.139.26