COME GOVERNARE IL RISCHIO E APPLICARE LA DIRETTIVA CER

Roadmap Pratica per i Soggetti Critici

Di Giuseppe Alverone

Cyber & Cyber
Sicurezza • Dati • Geopolitica

Cyber & Cyber
Sicurezza • Dati • Geopolitica

INDICE

La **Direttiva CER** (*Direttiva UE 2022/2557*), nota anche come *Critical Entities Resilience*, è il quadro normativo europeo per la sicurezza e resilienza fisica delle infrastrutture critiche. La direttiva è stata recepita in Italia con il *Decreto Legislativo n.134/2024*, in vigore da **ottobre 2024**.

La nuova normativa poggia su precisi punti chiave che si esprimono attraverso quattro capisaldi:

- Garantire la continuità dei servizi essenziali per il funzionamento della società e dell'economia (es. energia, trasporti, sanità, banche) in caso di minacce fisiche, disastri naturali, sabotaggi o atti terroristici.
- Imporre agli Stati membri di censire le *"entità critiche"* attive in settori strategici.
- Lavorare in piena assonanza con la normativa sulla sicurezza logica/informatica (Direttiva NIS 2).
- Richiedere alle entità individuate di adottare valutazioni del rischio e misure tecniche, organizzative e di gestione delle crisi per mitigare l'impatto di interruzioni nei servizi.

Il recepimento nazionale e le linee guida attuative sono coordinati in Italia dalla Presidenza del Consiglio dei Ministri.

Per far comprendere al meglio tali tematiche **Cyber & Cyber** mette a disposizione sette contributi a firma del Gen. **Giuseppe Alverone**, riconosciuto esperto nazionale del settore della privacy e della sicurezza, che mettono a disposizione di manager pubblici e privati tutti gli strumenti necessari non solo per adempiere agli obblighi della nuova normativa, ma anche per aggiungere ulteriore livello di consapevolezza professionale al loro ruolo.

Raffaele Barberio
Direttore
Cyber & Cyber

Cyber & Cyber
Sicurezza • Dati • Geopolitica

GIUSEPPE ALVERONE

Consulente, formatore e divulgatore in *data protection, cybersecurity* e gestione del rischio.
Lavora con un obiettivo preciso: portare le organizzazioni a prendere decisioni corrette nei momenti in cui ogni scelta ha conseguenze reali.
Generale di Brigata in congedo dell'**Arma dei Carabinieri**, ha prestato servizio per oltre **40 anni**, operando in contesti complessi dove decidere bene non è una scelta ma una necessità.
Questa esperienza oggi è il cuore del suo metodo: non parte dalla norma ma dalla realtà.
Non si limita a spiegare **GDPR** e **NIS 2**. Traduce obblighi in scelte operative e aiuta le organizzazioni a chiarire chi decide, su cosa e con quali responsabilità perché la sicurezza non nasce dai documenti ma da decisioni assunte e sostenute.
È stato Data Protection Officer dell'**Arma dei Carabinieri** fino al **2024**.
Oggi è amministratore unico di **DATA FABER**, ricopre il ruolo di DPO a livello di gruppo in una primaria realtà industriale nazionale e affianca imprese e vertici aziendali che vogliono superare la compliance formale per costruire sistemi che funzionano davvero, integrando governance, processi e responsabilità.
È DPO certificato *UNI CEI EN 17740:2024*, docente presso IF Academy, presso **A-Sapiens Business School** e membro del Comitato Scientifico **A-SAPIENS**.
Autore di manuali e articoli specialistici, interviene in contesti di alto livello a diretto contatto con il top management.
Il suo metodo è diretto: leggere i segnali giusti, decidere con lucidità, tracciare ogni scelta.

Cyber & Cyber
Sicurezza • Dati • Geopolitica

DIRETTIVA CER: ECCO COME COMPRENDERLA, GOVERNARLA E APPLICARLA

La Direttiva CER: ecco come comprenderla, governarla e applicarla

Il *d.lgs. 134/2024* – che ha recepito la *Direttiva (UE) 2022/2557* (**c.d. Direttive CER: Critical Entities Resilience**) – nell'**art.1** racconta meglio di qualsiasi commento il cambio di paradigma che l'Europa ha imposto agli Stati membri: *«Il presente decreto stabilisce misure volte a garantire che i servizi essenziali [...] siano forniti senza impedimenti» «[...] e obblighi per i soggetti critici [...] volti a rafforzarne la resilienza»*

Non si parla più di *"infrastrutture critiche"* come oggetti da proteggere ma di servizi essenziali e di soggetti critici che devono continuare a funzionare anche quando accadono eventi destabilizzanti come alluvioni, blackout, sabotaggi fisici, crisi energetiche, interruzioni della *supply chain*, attacchi ibridi.

La **Direttiva CER (Critical Entities Resilience)** e il decreto legislativo che la recepisce in **Italia** sono una nuova costituzione della resilienza nazionale.

E questo articolo serve a spiegare, con chiarezza, cosa cambia, per chi, e perché.

Perché è stata emanata la Direttiva CER

Negli ultimi dieci anni l'Europa ha scoperto che la continuità dei servizi essenziali non è affatto garantita. Tre shock hanno accelerato la consapevolezza:

- la **pandemia**: ospedali sotto stress, supply chain globali interrotte, logistica in tilt;
- la **guerra in Ucraina**: energia, gasdotti, cavi sottomarini, porti, ferrovie diventano bersagli.
- **eventi climatici estremi:** alluvioni, incendi, siccità che colpiscono acqua, energia, trasporti.

La vecchia *Direttiva 2008/114/CE* del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, era una direttiva costruita in un contesto storico molto diverso da quello attuale. Dopo gli attentati terroristici degli anni 2000, l'attenzione era concentrata soprattutto sulla protezione fisica di alcune infrastrutture considerate essenziali per la sicurezza europea. La normativa riguardava pochi settori, con focus quasi esclusivo sul terrorismo e approccio statico.

La **Direttiva CER (UE 2022/2557)** cambia radicalmente lo scenario: non protegge più solo infrastrutture ma garantisce la continuità dei servizi essenziali attraverso la resilienza dei soggetti che li erogano.

È un passaggio culturale di grande rilevanza: non conta più solo il "muro" che protegge un impianto, ma la capacità complessiva dell'organizzazione di prevenire, assorbire, resistere e ripristinare.

Il cuore del decreto: servizi essenziali e soggetti critici

Il *d.lgs. 134/2024* recepisce la direttiva CER e introduce due concetti chiave: servizi essenziali e soggetti critici.

1. **Servizi essenziali**, sono i servizi senza i quali la società non funziona: energia, trasporti, acqua, salute, alimenti, spazio, infrastrutture digitali, finanza, pubblica amministrazione. Il decreto definisce il servizio essenziale come *«un servizio fondamentale per il mantenimento di funzioni vitali della società».*
2. **Soggetti critici**, sono gli operatori – pubblici o privati – che erogano i servizi essenziali e che sono individuati nell'ambito delle categorie di soggetti che operano nei settori e sottosettori riportati nell'allegato A del decreto CER.

Non tutti gli operatori di un settore diventano soggetti critici: solo quelli la cui interruzione può generare effetti negativi rilevanti.

Il cambio di paradigma: dalla protezione alla resilienza

Il decreto CER introduce una frattura culturale prima ancora che normativa. Infatti, non richiede semplicemente di *"proteggere"* un'infrastruttura ma di ripensare il modo stesso in cui immaginiamo la continuità del Paese. La resilienza è un movimento, un ciclo vitale che accompagna l'organizzazione prima, durante e dopo l'incidente.

La definizione del decreto è rivelatrice: la resilienza è *«la capacità di un soggetto critico di prevenire, attenuare, assorbire un incidente [...] di rispondervi, resistervi, adattarvisi e ripristinare le proprie capacità operative».*

È una definizione che contiene sei verbi che sono sei fasi di un'unica dinamica:

- **prevenire:** agire prima che la minaccia prenda forma, leggere i segnali deboli, anticipare;
- **attenuare:** ridurre l'impatto, limitare la superficie di danno, contenere l'onda d'urto;
- **assorbire:** reggere il colpo senza perdere la funzione essenziale, mantenere il servizio anche in condizioni degradate;
- **rispondere:** coordinare, comunicare, decidere. La risposta è un atto di governo, non solo tecnico;
- **resistere:** non cedere alla pressione, evitare l'effetto domino, impedire che un incidente diventi crisi sistemica;
- **adattarsi:** cambiare configurazione, riallocare risorse, modificare processi mentre l'incidente è ancora in corso;
- **ripristinare:** tornare operativi, ma non come prima: tornare meglio di prima, integrando ciò che si è imparato.

Questi verbi non sono un mero elenco di attività ma una sequenza dinamica, un ciclo che non si chiude mai.

Qui avviene il vero cambio di paradigma: la resilienza non è un piano di emergenza né un faldone da tirare fuori quando scatta l'allarme. È un processo continuo, un modo di progettare, gestire e governare un'infrastruttura critica sapendo che l'incidente non è un'eccezione ma una variabile strutturale del contesto.

La protezione appartiene al mondo in cui si pensava di poter evitare l'imprevisto.

La resilienza, invece, appartiene al mondo in cui sappiamo che l'imprevisto arriverà – e ci prepariamo a non farci travolgere.

L'ambito di applicazione: cosa copre e cosa esclude

Il decreto CER non è stato emanato per *"mappare tutto"* ma per identificare ciò che, se si ferma, blocca il *"sistema Paese"*. La logica è coerente con questa finalità: nel perimetro di applicazione rientrano i settori la cui interruzione comprometterebbe la continuità della vita civile, economica e istituzionale; fuori restano invece gli ambiti che già dispongono di regimi speciali di sicurezza, o che per natura non possono essere assoggettati a un quadro europeo uniforme.

Cosa copre: i settori che tengono in piedi il Paese

I settori inclusi nel perimetro **CER** rappresentano la spina dorsale funzionale dello Stato. Non sono scelti per categoria merceologica ma per funzione sistemica: ciò che alimenta, muove, connette, cura, governa e sostiene la società.
Ecco la logica che li accomuna:

ENERGIA: senza energia non esiste alcun altro servizio essenziale: è il prerequisito materiale di tutto

BANCARIO: assicura liquidità, pagamenti, accesso ai fondi: condizione minima di stabilità economica

ACQUA POTABILE: servizio primario di sopravvivenza e igiene pubblica

TRASPORTI: garantiscono la mobilità di persone, merci, medicinali, cibo: sono la circolazione del sistema-Paese

SALUTE: ospedali, reti sanitarie, emergenza: la continuità è vitale in senso letterale

ACQUE REFLUE: presidiano sicurezza igienico-sanitaria e tutela ambientale

INFRASTRUTTURE DIGITALI: data center, cloud, reti, IXPs: l'ossatura invisibile che sostiene tutti gli altri settori

PUBBLICA AMMINISTRAZIONE: lo Stato deve continuare a funzionare anche sotto stress: servizi amministrativi, fiscali, decisionali

SPAZIO: satelliti per navigazione, comunicazioni, osservazione: componente ormai strutturale dei servizi critici terrestri

PRODUZIONE E DISTRIBUZIONE ALIMENTARE: catene logistiche che non possono interrompersi senza generare tensioni sociali

ACQUE IRRIGUE: essenziali per la produzione agricola: un'interruzione colpisce direttamente la sicurezza alimentare

INFRASTRUTTURE MERCATI FINANZIARI: svolgono funzioni di regolazione, compensazione, regolamento: senza di esse il sistema finanziario si blocca

Cosa è escluso dal perimetro di applicazione: gli ambiti già protetti da regimi speciali

Le esclusioni non sono *"vuoti normativi"* ma scelte intenzionali.
Il decreto CER non si applica a quei settori che già operano sotto regimi di sicurezza dedicati, spesso più stringenti, o che per natura non possono essere ricondotti a un quadro europeo uniforme.
Sono esclusi: **Difesa – Sicurezza nazionale – Intelligence – Forze di polizia – Attività di contrasto e indagine – ACN (perimetro cyber) – Parlamento- Banca d'Italia – UIF – Organi giudiziari**.
Qui la logica è opposta rispetto ai settori inclusi: non si tratta di servizi *"non essenziali"*, ma di servizi talmente sensibili da richiedere un quadro autonomo, spesso classificato, con regole di sicurezza non armonizzabili a livello europeo.

Quindi, in sintesi, il perimetro di applicazione della normativa CER è una mappa funzionale del Paese. Dentro ci sono i settori che devono continuare a funzionare perché tutto il resto possa funzionare. Fuori ci sono gli ambiti che già vivono in un ecosistema di sicurezza separato, spesso più rigido, più riservato, più nazionale.
Il risultato è un quadro che non pretende di essere totale ma coerente perchè protegge ciò che serve a mantenere in piedi la vita civile, senza sovrapporsi ai regimi speciali che tutelano la sicurezza dello Stato.

Il baricentro operativo del sistema CER: la valutazione del rischio

La **Direttiva** e il **Decreto CER** costruiscono l'intero sistema su un principio semplice: la resilienza non si improvvisa, si progetta e la progettazione parte sempre da una valutazione del rischio solida, strutturata, multilivello.
Per questo motivo la normativa introduce un doppio livello di risk assessment, che si alimenta in entrambe le direzioni.

La valutazione del rischio dello Stato (approccio top-down)

Lo Stato elabora una propria valutazione nazionale dei rischi che possono colpire i settori essenziali: minacce, vulnerabilità, interdipendenze, scenari di impatto. È una visione *"dall'alto"*, sistemica, che serve a:

- individuare i rischi strategici per il Paese;
- comprendere gli effetti domino tra settori;
- orientare le priorità di prevenzione e risposta;
- fornire un quadro comune a tutte le autorità settoriali.È il riferimento che guida l'intero sistema.

La valutazione del rischio dei soggetti critici (approccio bottom-up)

Parallelamente, ogni soggetto critico deve valutare i rischi che riguardano la propria infrastruttura, i propri processi, le proprie dipendenze. È un'analisi *"dal basso"*, operativa, che:

- fotografa le vulnerabilità reali dell'operatore;
- integra la prospettiva nazionale con la conoscenza del campo;
- permette di costruire misure di resilienza proporzionate e concrete;

alimenta il flusso informativo verso le autorità competenti.In altre parole: lo Stato vede il sistema, il soggetto critico vede la macchina e solo mettendo insieme le due prospettive si ottiene una resilienza autentica.

CER non è NIS2 (e non è DORA)

L'articolo 1, comma 3 del decreto **CER** stabilisce che: quando gli obblighi di resilienza di un soggetto critico sono già disciplinati da uno specifico atto giuridico dell'Unione europea, e gli effetti di tali obblighi sono almeno equivalenti a quelli previsti dal decreto CER, si applica l'atto europeo e non il CER.
In altre parole: niente duplicazioni.
Se un settore è già regolato da una disciplina europea specialistica – come **NIS2** per la sicurezza delle reti e dei sistemi informativi, o **DORA** per la resilienza operativa digitale nel settore finanziario – il CER *"si ritira"* e lascia spazio alla normativa settoriale.

È un principio di coerenza regolatoria: evitare sovrapposizioni, evitare oneri inutili per gli operatori ed evitare che la resilienza diventi un labirinto burocratico.

Questo tema sarà approfondito nel quinto articolo dell'eptalogia, dove analizzeremo nel dettaglio il rapporto tra CER, NIS2 e DORA e i casi concreti in cui opera il principio di equivalenza.

Incidenti fisici: nasce un nuovo obbligo di notifica

Il **CER** introduce un obbligo che in Italia non esisteva: la notifica degli incidenti fisici. Non solo cyber, non solo digitali: qualsiasi evento fisico che comprometta la continuità di un servizio essenziale deve essere comunicato al **Punto di Contatto Unico (PCU)** e all'**Autorità Settoriale Competente (ASC).**
È un cambio di paradigma importante perché si riconosce che gli incidenti fisici (sabotaggi, incendi, guasti, alluvioni, blackout, attacchi ibridi) possono avere impatti sistemici quanto quelli informatici.
Così, si crea un flusso informativo nazionale che prima non esisteva e si integra la dimensione fisica e quella cyber in un'unica logica di resilienza.
Questo nuovo obbligo sarà approfondito nel quarto articolo dell'eptalogia, dedicato alla gestione degli incidenti e ai flussi di notifica.

La dimensione europea

La normativa CER non è solo un esercizio nazionale ma è anche parte di un ecosistema europeo di resilienza. Alcuni operatori, per dimensione, ruolo o interdipendenze, saranno classificati *"di particolare rilevanza europea"*. Per questi soggetti, la Commissione europea può inviare missioni di consulenza.
È un livello di supervisione che supera i confini nazionali e riconosce che alcune infrastrutture non servono solo un Paese ma l'intero mercato interno.

La roadmap istituzionale

Il decreto **CER** non si limita a fissare obblighi ma disegna un percorso, una sequenza logica che porta il Paese dalla strategia alla piena operatività.
La roadmap è già tracciata e si articola in quattro passaggi:

- **Strategia nazionale** – la visione complessiva dello Stato sulla resilienza;
- **Valutazione del rischio** – la mappa delle minacce e delle vulnerabilità;
- **Individuazione dei soggetti critici** – chi è dentro il perimetro e perché;
- **Avvio degli obblighi** – piani, misure, notifiche, vigilanza.

ECCO CHI GOVERNA LA RESILIENZA NELLA MACCHINA CER ITALIANA

La resilienza diventa materia di governo: un cambio politico prima che tecnico

Il *d.lgs. 134/2024* non è solo un testo normativo, è anche un atto politico.
Per la prima volta, la resilienza dei servizi essenziali viene collocata al centro dell'azione di governo e non come tema settoriale ma come funzione strategica dello Stato.
Il decreto lo afferma in modo chiaro: *«Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva l'alta direzione e la responsabilità generale delle politiche per la resilienza dei soggetti critici»*
È un passaggio molto rilevante: la resilienza è diventata una politica pubblica di livello primario, al pari della sicurezza nazionale, della difesa e della protezione civile.

Chi governa la resilienza in Italia?

PRESIDENTE DEL CONSIGLIO

- definisce la strategia nazionale per la resilienza;
- impartisce direttive alle amministrazioni;
- coordina le politiche interministeriali;
- può delegare l'attuazione, ma non la responsabilità;
- è il punto di riferimento politico per l'UE.

CABINA DI REGIA INTERMINISTERIALE (CIR)

- I compiti principali: Il decreto affida al Comitato la definizione degli indirizzi generali per le politiche di resilienza e l'alta sorveglianza sull'attuazione della strategia nazionale, delineando una visione unitaria dello Stato;
- Riunisce i ministri che gestiscono le leve fondamentali del Paese (Affari esteri, Interno, Giustizia, Difesa, Economia, Imprese e Made in Italy, Agricoltura, Ambiente ed Energia, Infrastrutture e Trasporti, Salute, Protezione civile), insieme alle Autorità delegate per la sicurezza nazionale e per lo spazio.

AUTORITA'SETTORIALI COMPETENTI (ASC)

- applicano le disposizioni nei rispettivi ambiti;
- vigilano sui soggetti critici;
- conducono ispezioni;
- verificano le misure di resilienza;
- ricevono le notifiche degli incidenti;
- mantengono il raccordo costante con il Punto di Contatto Unico e con le istituzioni europee.

Le ASC servono a prendere la strategia nazionale e a trasformarla in azioni settoriali concrete, calibrate, proporzionate, aderenti alla realtà operativa di ciascun ambito.
Sono il punto in cui la visione del Paese incontra la complessità dei sistemi che lo fanno funzionare.

PUNTO DI CONTATTO UNICO (PCU)

- dialoga con la Commissione europea;
- coordina le attività con gli altri Stati membri;
- riceve le notifiche degli incidenti fisici;
- supporta le Autorità Settoriali Competenti nell'attuazione degli obblighi.

Il suo lavoro è continuo e multilivello. Da un lato mantiene il raccordo con Bruxelles, elabora il rapporto biennale sullo stato della resilienza nazionale e partecipa ai flussi informativi europei; dall'altro coordina con ACN, Protezione Civile, Interno, Difesa e intelligence, perché un incidente fisico o ibrido non è mai confinato a un solo settore.

GLI ATTORI "OMBRA"

- L'Agenzia per la Cybersicurezza Nazionale è il presidio sulle minacce ibride: si coordina con PCU e ASC quando un incidente cyber ha effetti fisici, quando un'infrastruttura digitale diventa il punto di vulnerabilità di un'intera filiera e quando le interdipendenze tecnologiche amplificano un evento locale.
- Il Dipartimento della Protezione Civile entra in campo quando la minaccia è naturale: alluvioni, terremoti, incendi, emergenze climatiche.
- Il Ministero dell'Interno e il Ministero della Difesa presidiano l'ordine pubblico, la sicurezza fisica, le minacce ostili, i sabotaggi.

Una governance pensata per le crisi del XXI secolo

La nuova architettura CER nasce da un'esigenza precisa: governare crisi che sono molto diverse da quelle del passato. Le minacce sono più veloci, più interconnesse, più difficili da contenere.

Per questo motivo, il sistema è costruito su tre pilastri.

Il primo è la **velocità**: le crisi moderne non aspettano, e la governance deve essere in grado di prendere decisioni rapide, coordinate, informate.

Il secondo è il **coordinamento**: nessun settore è isolato e la resilienza richiede una regia unica che tenga insieme energia, trasporti, digitale, finanza, salute, ambiente.

Il terzo è la **visione strategica**: la resilienza non è una politica pubblica che riguarda la sicurezza nazionale, la continuità economica, la stabilità sociale.

Il decreto CER costruisce, così, un sistema che non si limita a reagire ma anticipa, prevede e integra. È una governance pensata per le crisi del XXI secolo non per quelle del passato.

Cosa cambia per gli operatori

Per gli operatori – sia pubblici che privati – la normativa CER rappresenta un cambio di paradigma. Non basta più garantire la continuità del proprio servizio ma occorre inserirsi in un sistema istituzionale più ampio, comprendere i flussi informativi, dialogare con gli attori della governance.

Ogni operatore dovrà interfacciarsi con la propria **ASC** per gli obblighi settoriali, con il **PCU** per le notifiche e i flussi europei e, indirettamente, con il **CIR** che definisce gli indirizzi strategici.

Per la componente digitale entrerà in gioco l'**ACN**; per la gestione delle emergenze fisiche, la **Protezione Civile**.

La resilienza è un processo condiviso, multilivello, che richiede consapevolezza istituzionale.

In altre parole, non è più sufficiente *"fare bene il proprio mestiere"*: bisogna capire come funziona la macchina dello Stato e come il proprio ruolo si inserisce nella sicurezza complessiva del Paese.

COME LO STATO VALUTA IL RISCHIO E DECIDE CHI ENTRA NEL PERIMETRO CER

La domanda che tutti si pongono: "Diventeremo soggetti critici?"

Da quando il *d.lgs. 134/2024* è entrato in vigore, questa è la domanda che attraversa aziende, enti pubblici, *utility*, gestori di infrastrutture, ospedali, operatori digitali, banche e trasporti.
È una domanda semplice nella forma ma complessa nella sostanza.
La risposta, infatti, non dipende da autocandidature, autocertificazioni o valutazioni soggettive ma dipende esclusivamente dalla valutazione del rischio che lo Stato sta conducendo.
La **Direttiva CER** è inequivocabile: non esiste discrezionalità da parte degli operatori e non esiste un *"bollino"* da richiedere nè percorso volontario.
È lo Stato che designa, sulla base di criteri oggettivi e dell'impatto sistemico dei servizi erogati.
In altre parole: non si diventa soggetti critici perché lo si vuole ma perché lo si è per funzione, per ruolo e per rilevanza strategica nel funzionamento del Paese.

Il punto di partenza: i servizi essenziali

Prima ancora di individuare chi siano i soggetti critici, lo Stato deve rispondere a una domanda preliminare e decisiva: quali sono i servizi essenziali da cui dipende la vita del Paese? Il decreto li definisce come *«servizi fondamentali per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente»*. Una definizione ampia ma tutt'altro che generica: è una lente che obbliga lo Stato a interrogarsi su quali attività, se interrotte anche solo per poche ore, produrrebbero un danno grave e immediato alla collettività.
Questo postula la necessità di chiedersi quali settori sostengono la vita quotidiana del Paese, quali infrastrutture non possono fermarsi senza mettere a rischio sicurezza, economia, salute, ambiente, e quali interdipendenze rendono vulnerabile l'intero sistema.
Questa analisi converge nell'Allegato A del decreto CER, che individua dodici settori che rappresentano i pilastri della società moderna: **energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, salute, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio, produzione e distribuzione alimentare, acque irrigue.**
Sono i domini senza i quali il Paese semplicemente non funziona: la spina dorsale invisibile che sostiene ogni attività civile, economica e istituzionale.

La valutazione del rischio dello Stato: il "cervello" del sistema CER

Al centro dell'architettura **CER** c'è un meccanismo fondamentale: la valutazione nazionale del rischio. L'articolo 7 affida allo Stato un compito complesso, quasi chirurgico, che richiede di:

- **analizzare minacce naturali, accidentali e intenzionali;**
- **individuare vulnerabilità fisiche, organizzative e territoriali;**
- **comprendere le interdipendenze tra settori;**
- **stimare gli impatti potenziali di un'interruzione.**

È un processo che costruisce una mappa dinamica di ciò che può mettere in crisi la continuità dei servizi essenziali. Il decreto lo definisce come *«l'intero processo per la determinazione della natura e della portata di un rischio»*, un lavoro che permette allo Stato di capire non solo cosa può accadere ma cosa significherebbe per il Paese.
In questo modo la resilienza diventa la capacità concreta di continuare a funzionare anche quando qualcosa non funziona come dovrebbe.
Per individuare chi è davvero critico, lo Stato deve prima capire dove si annidano le fragilità del sistema.

Il criterio chiave: gli "effetti negativi rilevanti"

La **Direttiva CER** introduce un principio che cambia la prospettiva: un soggetto è critico non *"per ciò che è"*, ma per *"ciò che accadrebbe se si fermasse"*. La soglia è quella degli *"effetti negativi rilevanti"*, un concetto che abbraccia impatti sulla vita e sulla salute delle persone, sull'economia, sulla sicurezza pubblica, sull'ambiente, sulle relazioni transfrontaliere e sulle interdipendenze tra settori.
È una logica di sistema. Così, ad esempio:

- **un TSO (Transmission System Operator) elettrico** – un gestore che trasporta l'energia dai produttori ai distributori locali – che si interrompe, può generare un blackout nazionale;
- **un grande ospedale che si ferma, mette a rischio vite umane;**
- **un porto strategico bloccato paralizza la logistica;**
- **un data center nazionale compromesso interrompe la continuità istituzionale;**
- **un acquedotto metropolitano fuori uso crea un'emergenza sanitaria.**

Quindi, non conta la dimensione dell'operatore ma l'impatto della sua interruzione.
Questo è il super-criterio CER.

Cosa devono aspettarsi gli operatori nei prossimi mesi

La macchina amministrativa è già in movimento.
Gli operatori devono attendersi richieste di informazioni dalle **Autorità Settoriali Competenti**, (ASC), richieste di dati tecnici e organizzativi, questionari sulla continuità operativa, incontri conoscitivi, analisi delle interdipendenze e valutazioni territoriali.
I primi settori a essere designati saranno probabilmente quelli più interdipendenti e più esposti: energia, acqua, trasporti, infrastrutture digitali, sanità, alimentare e finanza.
Sono i settori che, se colpiti, generano effetti a cascata.

Cosa devono fare gli operatori prima della designazione

Anche se non sono ancora soggetti critici, gli operatori lungimiranti si stanno già muovendo.
Stanno:

- **mappando i propri servizi essenziali;**
- **analizzando rischi fisici e organizzativi;**
- **valutando la solidità della supply chain;**
- **aggiornando i piani di continuità, integrando i requisiti CER con quelli di NIS2 e DORA;**
- **predisponendo una governance interna adeguata.**

Fanno questo perchè quando arriverà la designazione, il tempo per adeguarsi sarà limitato.
Chi si prepara ora avrà un vantaggio competitivo e istituzionale.

Perché questo processo è rivoluzionario

La normativa CER rappresenta una svolta per tre motivi fondamentali.
Primo motivo: lo Stato torna a fare strategia: non si limita a controllare ma decide, pianifica e coordina.
Secondo motivo: la resilienza diventa un bene pubblico; non più un costo privato ma un dovere verso la collettività.
Terzo motivo: la criticità non è un'etichetta, è una responsabilità. Essere soggetto critico significa essere essenziale, vulnerabile e responsabile della continuità di un servizio che sostiene la vita del Paese.

COME I SOGGETTI CRITICI DEVONO GESTIRE IL RISCHIO

Il momento della verità: cosa accade quando si diventa "soggetto critico"

La designazione come soggetto critico non è un riconoscimento né un'etichetta da esibire ma è l'inizio di un percorso impegnativo che richiede governance, processi, investimenti, cultura organizzativa e capacità di coordinamento con lo Stato.
Il decreto è inequivocabile: una volta designati, i soggetti critici devono raggiungere un livello elevato di resilienza. Non un livello *"adeguato"* né un livello *"ragionevole"* ma elevato.
È il momento in cui l'organizzazione deve dimostrare di essere all'altezza del ruolo che ricopre nel funzionamento del Paese.

Il primo obbligo: la valutazione del rischio (art. 13)

La valutazione del rischio rappresenta il fulcro dell'intero impianto CER perchè è il primo obbligo che scatta dopo la designazione ed è il fondamento su cui poggeranno tutte le misure di resilienza successive.
Il decreto è chiarissimo: entro nove mesi dalla notifica di designazione – e poi almeno ogni quattro anni – il soggetto critico deve condurre una valutazione completa di tutti i rischi che potrebbero perturbare la fornitura dei suoi servizi essenziali.
Non si tratta di un esercizio formale né di un documento da produrre per adempiere a un obbligo ma è un processo strutturato, continuo e strategico che deve guidare le decisioni operative e di governance.
La valutazione deve partire dall'identificazione delle infrastrutture critiche dell'organizzazione, così come definite dall'art. 2, e deve basarsi sulla valutazione nazionale del rischio elaborata dallo Stato, integrandola con tutte le altre informazioni rilevanti disponibili.
Da qui discende l'obbligo di analizzare l'intero spettro dei rischi: quelli naturali e quelli di origine umana, includendo esplicitamente rischi intersettoriali e transfrontalieri, incidenti, catastrofi naturali, emergenze di sanità pubblica, minacce ibride e altre minacce antagoniste, fino ai reati con finalità di terrorismo, anche internazionale.
La valutazione deve inoltre considerare le interdipendenze: da un lato, quanto altri settori dipendano dal servizio essenziale fornito dal soggetto critico; dall'altro, quanto il soggetto critico dipenda a sua volta da servizi essenziali erogati da terzi, anche in altri Stati membri o Paesi terzi vicini.
È un'analisi che richiede una visione sistemica, capace di cogliere vulnerabilità dirette e indirette.
Il decreto consente ai soggetti critici di utilizzare, ove pertinenti, documenti già predisposti per altri regimi normativi (come **NIS2, DORA**, *safety, business continuity*), a condizione che tali documenti includano tutti i rischi e le dipendenze richieste dall'art. 13.

Saranno poi le **ASC**, nell'esercizio della vigilanza, a verificare se tali documenti soddisfano in tutto o in parte gli obblighi previsti.
L'errore da evitare è uno solo: considerare la valutazione del rischio come un adempimento.
L'art. 13 del **decreto CER** richiede un sistema e una capacità. Questo è il passaggio che distingue la compliance dalla resilienza.

Il secondo obbligo: le misure di resilienza (art. 14)

L'articolo 14 del **Decreto CER** è il punto in cui la resilienza diventa un dovere operativo.
Una volta valutato il rischio ai sensi dell'art. 13, i soggetti critici devono adottare e applicare misure tecniche, organizzative e di sicurezza adeguate e proporzionate, costruite sulla base della valutazione nazionale del rischio fornita dal **PCU** e dei risultati della propria valutazione interna.
È certamente un obbligo ampio, che postula la necessità di:

- **prevenire gli incidenti;**
- **proteggere fisicamente i siti;**
- **resistere e mitigare gli impatti;**
- **ripristinare rapidamente la continuità del servizio;**
- **garantire la sicurezza del personale.**

Le misure richieste dal decreto si articolano in aree precise e complementari.
La sicurezza fisica impone la protezione dei siti e delle infrastrutture critiche attraverso recinzioni, barriere, controlli perimetrali, sistemi di rilevamento, controllo degli accessi e ogni altra misura necessaria a prevenire intrusioni e atti ostili.
La sicurezza del personale richiede l'individuazione delle categorie che svolgono funzioni critiche, la gestione delle autorizzazioni di accesso, le procedure per i controlli dei precedenti personali previsti dall'art. 15 e l'adozione di requisiti di formazione e qualificazione adeguati.
La sicurezza organizzativa riguarda la costruzione di una governance interna della resilienza, con ruoli, responsabilità, procedure e meccanismi di coordinamento chiari, inclusa la designazione del referente **CER** da comunicare a **PCU** e **ASC**.
La continuità operativa impone misure per garantire il ripristino delle capacità operative in caso di incidente: piani di continuità, misure di *disaster recovery*, individuazione di catene di approvvigionamento alternative, protocolli di gestione delle crisi.
La gestione della *supply chain* richiede di valutare i fornitori critici, assicurare la continuità dei servizi essenziali esternalizzati e prevedere soluzioni alternative in caso di interruzione.
La comunicazione in emergenza impone la capacità di informare tempestivamente il personale sui rischi e sulle misure adottate, attraverso formazione, materiale informativo, esercitazioni e canali di comunicazione ridondanti.
Infine, la protezione delle infrastrutture digitali fisiche riguarda la sicurezza materiale di data center, sale server, reti fisiche, cavi e infrastrutture di telecomunicazione. Attenzione, non si tratta della sicurezza cyber (disciplinata da **NIS2**) ma della loro protezione fisica.
Tutte queste misure devono confluire in un Piano di Resilienza, da aggiornare quando necessario e comunque almeno ogni tre anni.

Le ASC, nell'esercizio della vigilanza, dovranno valutare se le misure adottate e i documenti prodotti soddisfano gli obblighi dell'articolo 14.
Il decreto consente inoltre di riutilizzare misure e documenti già predisposti per altri regimi normativi, purché pienamente coerenti con i requisiti CER.

Il terzo obbligo: i controlli sui precedenti personali (art. 15)

L'articolo 15 introduce uno dei meccanismi più sensibili dell'intero impianto CER: il controllo dei precedenti personali per il personale che ricopre ruoli critici.
Non si tratta di un controllo generalizzato né di un potere discrezionale del datore di lavoro ma di uno strumento mirato, proporzionato e strettamente regolato, pensato per prevenire minacce interne che potrebbero compromettere la fornitura dei servizi essenziali.
Il decreto stabilisce che il soggetto critico possa richiedere il certificato del casellario giudiziale europeo per le seguenti tre categorie di persone:

- **chi svolge ruoli sensibili, in particolare quelli con responsabilità o competenze in materia di resilienza;**
- **chi è autorizzato ad accedere, in presenza o da remoto, ai siti, ai sistemi informatici o ai sistemi di controllo dell'organizzazione;**
- **i candidati destinati a ricoprire tali ruoli.**

L'attivazione del controllo non è automatica: il soggetto critico deve presentare all'**Autorità Settoriale Competente** una richiesta motivata, indicando il ruolo, le ragioni del controllo e i reati ritenuti rilevanti. L'**ASC** verifica che il controllo sia necessario, proporzionato e limitato allo stretto indispensabile e che sia effettuato esclusivamente per valutare un potenziale rischio per la sicurezza del soggetto critico. Se l'**ASC** non risponde entro dieci giorni, l'autorizzazione si intende negata.
Una volta autorizzata, la richiesta viene trasmessa all'Ufficio Centrale del Casellario, che deve rispondere entro dieci giorni lavorativi, nel pieno rispetto della normativa nazionale ed europea sulla protezione dei dati personali.
Le modalità e i tempi di conservazione dei certificati dovranno essere definiti con decreto del **Presidente del Consiglio dei Ministri**, sentito il **Garante Privacy**.
L'articolo 15 non introduce una forma di sorveglianza ma una misura di protezione: serve a garantire che chi opera in ruoli critici lo faccia con un livello di affidabilità coerente con la responsabilità che il servizio essenziale richiede.

Il quarto obbligo: la notifica degli incidenti fisici (art. 16)

L'articolo 16 del decreto **CER** introduce un obbligo nuovo e strategico: i soggetti critici devono notificare senza indebito ritardo all'**Autorità Settoriale Competente (ASC)** e al **PCU** ogni incidente che perturbi, o possa perturbare in modo significativo, la fornitura dei servizi essenziali.
La notifica deve avvenire, salvo impossibilità operativa, entro 24 ore dal momento in cui l'organizzazione viene a conoscenza dell'evento, con una relazione dettagliata da trasmettere entro i successivi trenta giorni quando opportuno.
Rientrano in questo obbligo tutti gli incidenti fisici che possono compromettere la continuità del servizio: alluvioni, incendi, guasti gravi, interruzioni della *supply chain*, atti intenzionali e qualsiasi evento che abbia un impatto rilevante sulla capacità operativa.
Non rientrano invece nell'obbligo gli incidenti cyber, disciplinati dalla **NIS 2**, né gli eventi privi di effetti sulla fornitura del servizio.
La rilevanza dell'incidente viene valutata sulla base di tre parametri:

- **il numero e la percentuale di utenti coinvolti;**
- **la durata della perturbazione;**
- **l'area geografica interessata, tenendo conto anche di eventuali condizioni di isolamento territoriale.**

Le soglie quantitative per ciascun settore saranno definite con decreto del Presidente del Consiglio dei Ministri.

Come integrare CER con NIS 2, DORA e gli altri regimi

Per molti soggetti critici, la CER non sarà un'isola normativa: si sovrapporrà a **NIS 2, DORA**, al **Perimetro di sicurezza nazionale cibernetica (PSNC)** e ai regimi di vigilanza settoriale **(Banca d'Italia, Consob, IVASS, MIT, MASE)**.
È un mosaico evidentemente complesso che però è governabile se viene affrontato con la logica giusta.
La regola d'oro è semplice e imprescindibile: un solo sistema di gestione del rischio, più compliance.
Non serve – e sarebbe controproducente – costruire un risk assessment per **CER**, uno per **NIS 2**, uno per **DORA** e così via.
La resilienza non si frammenta ma si orchestra. Pertanto, serve un'unica architettura che integri tutto:

- **un'unica governance**, con ruoli e responsabilità chiari;
- **un'unica mappa dei rischi**, che includa minacce fisiche, cyber, operative, finanziarie e di supply chain;
- **un'unica analisi delle interdipendenze**, perché i servizi essenziali non si fermano mai per un solo motivo;
- **un'unica strategia di continuità**, capace di rispondere a incidenti fisici, digitali, organizzativi e di terze parti.

La normativa CER non richiede di duplicare ciò che già esiste, richiede di armonizzare.
Ovviamente, chi saprà farlo, non solo sarà conforme ma avrà costruito un vero vantaggio competitivo: una resilienza unica, coerente e misurabile, capace di soddisfare contemporaneamente tutte le autorità di vigilanza.

Le priorità operative per i soggetti critici

Una volta designati, i soggetti critici devono muoversi con rapidità e metodo.
La resilienza non deriva da un adempimento ma da una sequenza di scelte strategiche.
Le organizzazioni che vogliono essere davvero pronte dovrebbero concentrarsi su cinque priorità essenziali:

- **la prima è costruire una governance interna della resilienza**, definendo ruoli, responsabilità, un comitato dedicato e un referente CER capace di dialogare con ASC e PCU. Senza una regia chiara, nessuna misura sarà efficace;
- **la seconda è mappare i servizi essenziali e gli asset che li sostengono**: capire cosa è davvero critico, quali processi lo abilitano e quali infrastrutture lo rendono possibile;
- **la terza è condurre una valutazione del rischio completa e realistica**, che includa minacce naturali, accidentali, intenzionali, interdipendenze e impatti sistemici;
- **la quarta è definire e implementare le misure di resilienza** previste dall'art. 14, trasformando l'analisi in azione concreta: protezione fisica, continuità operativa, sicurezza del personale, gestione della supply chain;
- **la quinta è preparare la capacità di notificare gli incidenti, con procedure, ruoli, canali e modelli già pronti**: quando accade un evento rilevante, non c'è tempo per improvvisare.

Queste cinque priorità non sono un elenco: sono la spina dorsale del sistema CER.

Gli errori da evitare

Accanto alle priorità, ci sono errori che possono compromettere l'intero impianto.
Il più grave è trattare il CER come un adempimento, riducendolo a un fascicolo da compilare.
Un altro possibile errore consiste nel delegare tutto alla funzione *"sicurezza fisica"*, dimenticando che la resilienza è un ecosistema che coinvolge governance, personale, processi, *supply chain* e comunicazione.
Alcuni operatori sottovalutano la dipendenza dai fornitori, ignorando che una supply chain fragile può interrompere un servizio essenziale più rapidamente di un attacco diretto.
Grave è anche non integrare **CER** con **NIS2, DORA** e gli altri regimi, creando silos che si contraddicono invece di rafforzarsi.
Infine, due errori che rivelano immaturità organizzativa sono: non coinvolgere il vertice organizzativo e non fare esercitazioni. Senza leadership e senza prove, la resilienza resta mera teoria.
Un ultimo rilevante errore è non documentare i processi. Gli antichi padri dicevano quod non est in actis non est in mundo: ciò che non è documentato non esiste.

CER, NIS 2, DORA, BANCARIO E DIGITALE: COME ORIENTARSI NEL LABIRINTO DELLE REGOLE SULLA RESILIENZA

Il problema di fondo: la normativa CER non arriva in un deserto normativo

Quando la **Direttiva CER** è stata approvata, alcuni operatori hanno reagito con un misto di stupore e stanchezza: *"Un'altra normativa? Non bastavano NIS 2, DORA, GDPR, il perimetro cyber, le regole bancarie, quelle finanziarie, quelle sulle telecomunicazioni?"*. Il legislatore conosce perfettamente questa stratificazione.
Per questo motivo il *d.lgs. 134/2024* contiene una clausola decisiva: se un settore è già regolato da un atto europeo che impone obblighi equivalenti, **CER** *"si ritira"*. Non si somma, non si sovrappone e non crea duplicazioni.
È un principio di igiene regolatoria, pensato per evitare che gli operatori debbano costruire sistemi paralleli, incoerenti e costosi.
La normativa CER entra solo dove serve, e si fa da parte dove altri regimi coprono già gli stessi effetti.

CER e NIS 2: due normative sorelle ma non gemelle

Alcuni hanno pensato che la **CER** fosse semplicemente la *"NIS2 per il mondo fisico"*.
È un errore concettuale perché le due normative sono sorelle ma non gemelle: condividono la logica della resilienza ma guardano a dimensioni diverse.
NIS2 si occupa di sicurezza delle reti e dei sistemi informativi, incidenti cyber, gestione del rischio ICT, misure tecniche e organizzative digitali.
CER, invece, guarda alla resilienza fisica, alla continuità dei servizi essenziali, ai rischi naturali, accidentali, intenzionali e ibridi, alla *supply chain* materiale, alle infrastrutture fisiche.
I due mondi si incontrano nella protezione fisica delle infrastrutture digitali – data center, cavi, sale server – e nella gestione delle interdipendenze.
Si incrociano anche nella logica della notifica degli incidenti, che distingue tra eventi fisici e cyber. Ma si separano nettamente nelle autorità: **NIS 2** si relaziona con l'**ACN**, **CER** con **ASC** e **PCU**.
Per gli operatori soggetti a entrambe, la soluzione non è duplicare ma costruire un solo sistema di gestione del rischio, con due flussi di compliance.

CER e DORA: il caso più delicato

Nel settore finanziario il decreto è inequivocabile: banche e infrastrutture dei mercati finanziari possono essere individuate come soggetti critici ma non sono soggette agli obblighi operativi del CER.
L'*articolo 8, comma 5*, stabilisce infatti che per questi soggetti non si applicano l'articolo 12 e i Capi III e IV, cioè l'intero blocco degli obblighi su valutazione del rischio, misure di resilienza, controlli sui precedenti e notifica degli incidenti.
La loro resilienza regolatoria resta integralmente disciplinata da **DORA** e dalla vigilanza di **Banca d'Italia**, **Consob** e delle autorità europee.
Il CER mantiene solo funzioni di designazione, coordinamento istituzionale e integrazione nella strategia nazionale, senza imporre obblighi operativi aggiuntivi.
È l'applicazione più chiara del principio di non duplicazione: nel settore finanziario non esiste un doppio binario **CER/DORA**. Esiste un'unica architettura regolatoria, in cui CER riconosce la piena copertura offerta da DORA e si ritira dagli obblighi operativi.

CER e Perimetro di Sicurezza Nazionale Cibernetica

Il perimetro cyber italiano è un regime di sicurezza nazionale e non di resilienza dei servizi essenziali. Si applica a operatori strategici e infrastrutture critiche, con obblighi tecnici e controlli stringenti. **CER** e Perimetro vivono su piani diversi: il primo guarda alla continuità dei servizi essenziali, il secondo alla sicurezza nazionale.
Si incontrano nella protezione fisica delle infrastrutture digitali, nella gestione delle minacce ibride e nella cooperazione tra **ACN** e **PCU**.
Ma si separano nella finalità: il Perimetro protegge lo Stato, **CER** protegge la continuità dei servizi.

CER e regolazione delle telecomunicazioni

Gli operatori di telecomunicazioni si muovono già in un quadro fitto di regole: Codice delle comunicazioni elettroniche, obblighi di sicurezza delle reti, continuità del servizio, vigilanza **AGCOM** e **MIMIT**, oltre agli obblighi di cibersicurezza derivanti dalla **NIS 2**.
In questo contesto, il *d.lgs. 134/2024* non replica la disciplina cyber né quella sulla sicurezza delle reti: introduce, anche per il settore delle infrastrutture digitali di cui all'allegato A, gli obblighi generali CER in materia di resilienza dei soggetti critici.
Questo significa, in concreto, misure di resilienza fisica delle infrastrutture (ai sensi dell'art. 14), valutazione del rischio (art. 13) e obbligo di notifica degli incidenti fisici che perturbano in modo significativo la fornitura dei servizi essenziali (art. 16), con il relativo coinvolgimento di ASC e PCU (art. 5 e art. 16).
CER, quindi, non sostituisce né duplica la disciplina di settore: la completa sul versante della resilienza fisica e organizzativa dei servizi essenziali di comunicazione elettronica.

CER e regolazione dell'energia

Il settore energia è già tra i più regolati: disciplina di mercato e regolazione ARERA, normativa europea su gas, elettricità e idrogeno, perimetro di sicurezza nazionale cibernetica, obblighi NIS 2 per la componente digitale.

Su questo terreno, il decreto CER innesta un set di obblighi trasversali che valgono anche per i soggetti critici dell'energia:

- **valutazione del rischio rispetto a minacce naturali, accidentali, intenzionali e ibride (art. 13);**
- **adozione di misure tecniche, di sicurezza e organizzative adeguate e proporzionate per garantire la resilienza delle infrastrutture critiche (art. 14);**
- **predisposizione di un piano di resilienza (art. 14, comma 4);**
- **notifica degli incidenti fisici rilevanti ad ASC e PCU (art. 16).**

Non introduce nuovi obblighi di mercato né ridefinisce la disciplina cyber o di sicurezza nazionale ma si colloca accanto a queste, focalizzandosi sulla capacità del sistema energetico di prevenire, assorbire e superare incidenti fisici che possano compromettere la continuità dei servizi essenziali.

CER e sanità: un caso complesso

Anche la sanità vive già in un ecosistema normativo stratificato: **NIS 2** per gli ospedali e talune strutture sanitarie, **GDPR**, normative regionali, regolazione AIFA, obblighi di continuità operativa e di qualità dell'assistenza.

In questo quadro, il *d.lgs. 134/2024* aggiunge, per i soggetti critici del settore salute di cui all'allegato A, gli obblighi CER in materia di resilienza:

- **valutazione del rischio che tenga conto di eventi naturali, accidentali, intenzionali e ibridi e delle interdipendenze con energia, acqua, digitale e trasporti (art. 13);**
- **misure di resilienza fisica e organizzativa delle strutture e delle infrastrutture critiche sanitarie (art. 14);**
- **piano di resilienza aggiornato, gestione della sicurezza del personale e informazione sui rischi (art. 14, commi 2 – 4);**
- **notifica degli incidenti fisici che perturbano la continuità dei servizi essenziali sanitari ad ASC e PCU (art. 16).**

Anche qui, la normativa CER non riscrive la disciplina sanitaria né quella privacy o cyber: la attraversa, imponendo che pronto soccorso, terapia intensiva, diagnostica e gli altri servizi essenziali possano continuare a funzionare anche quando l'evento critico è fisico, sistemico, intersettoriale.

DIRETTIVA CER E RESILIENZA EUROPEA: GUIDA PER I SOGGETTI CRITICI TRANSFRONTALIERI

La resilienza non è più nazionale: è europea

La **Direttiva CER** nasce da una constatazione che non può essere ignorata: i servizi essenziali non si fermano ai confini degli Stati. Infatti:

- l'energia viaggia lungo reti interconnesse che attraversano l'Europa;
- i trasporti si muovono su corridoi che uniscono porti, aeroporti e ferrovie di più Paesi;
- le telecomunicazioni scorrono dentro cavi sottomarini e dorsali continentali;
- la finanza opera come un unico sistema;
- la supply chain alimentare è globale.

In un mondo così intrecciato, la resilienza non può essere costruita Stato per Stato.
Deve essere coordinata, condivisa, armonizzata.
Per questo motivo, la **Direttiva CER** introduce una categoria nuova e decisiva: i soggetti critici di particolare rilevanza europea, operatori la cui interruzione può generare impatti immediati in più Stati membri. È la presa d'atto che la resilienza è ormai un bene comune europeo.

Chi sono i soggetti critici di particolare rilevanza europea (SCRE)

L'articolo 17 del decreto non lascia spazio a interpretazioni: un **soggetto critico diventa di particolare rilevanza europea (SCRE)** solo quando è individuato dalla Commissione europea, secondo la procedura prevista dall'articolo 17 della **Direttiva CER**, e ha ricevuto la relativa notifica formale. Non è lo Stato italiano a decidere chi rientra in questa categoria: è un atto dell'Unione, basato su una valutazione europea degli impatti transfrontalieri.
Il decreto stabilisce inoltre un obbligo preliminare: entro un mese dalla propria designazione nazionale, i soggetti critici che forniscono servizi essenziali ad almeno sei Stati membri devono comunicare al **PCU** e all'**Autorità Settoriale Competente** quali servizi forniscono e in quali Paesi.
Su questa base il **PCU** trasmette alla Commissione l'identità dei soggetti potenzialmente rilevanti a livello europeo e partecipa, insieme alle **ASC** e agli operatori interessati, alle consultazioni previste dalla procedura europea.
Solo al termine di questo processo – e solo dopo la notifica della **Commissione** – un soggetto critico assume lo status di SCRE, con l'applicazione del Capo IV del decreto CER a partire dalla data di ricezione della notifica.

Essere classificati come SCRE significa, in sostanza, entrare in una dimensione regolatoria sovranazionale: non si risponde più soltanto allo Stato italiano ma si diventa parte di un ecosistema europeo di resilienza, con obblighi di cooperazione, consultazione e trasparenza che riflettono la natura transfrontaliera dei servizi essenziali forniti.

Le missioni di consulenza della Commissione: uno strumento europeo di verifica e cooperazione

L'articolo 18 introduce uno degli strumenti più significativi dell'intero impianto **CER**: le missioni di consulenza della Commissione europea. Non si tratta di ispezioni punitive né di audit sanzionatori ma di un meccanismo formale attraverso cui l'Unione può valutare, in modo diretto, le misure adottate da un soggetto critico che sia stato designato a livello nazionale e che sia stato individuato come **SCRE**.
Il decreto stabilisce che il **PCU**, d'intesa con l'**Autorità Settoriale Competente (ASC)**, possa chiedere alla Commissione di organizzare una missione, oppure accogliere una richiesta proveniente dalla Commissione stessa.
Quando la missione viene attivata, gli esperti europei possono accedere – nei limiti necessari – alle informazioni, ai sistemi e agli impianti del soggetto critico, per esaminare la valutazione del rischio, le misure di resilienza adottate, gli eventuali provvedimenti correttivi e ogni elemento utile a verificare l'adempimento degli obblighi previsti dal Capo III della Direttiva CER.
Durante la procedura, il **PCU** e le **ASC** collaborano con la Commissione, fornendo le informazioni richieste e partecipando alle consultazioni. Al termine della missione, la Commissione trasmette una relazione al PCU, che la inoltra senza ritardo all'Autorità Settoriale Competente. Se la relazione riguarda uno SCRE che opera in un altro Stato membro ma fornisce servizi essenziali all'Italia, il PCU può formulare osservazioni alla Commissione, segnalando eventuali criticità o la necessità di misure aggiuntive.
La Commissione può inoltre emettere un parere formale sull'adempimento degli obblighi da parte dello **SCRE**: il **PCU** lo riceve, lo trasmette all'**ASC** e, se riguarda un soggetto critico italiano, quest'ultimo è tenuto ad adeguarsi, sotto verifica dell'Autorità Settoriale Competente.
Infine, il PCU informa la Commissione e gli altri Stati membri interessati sulle misure adottate a seguito del parere, e propone gli esperti nazionali che parteciperanno alle missioni europee.
Le missioni di consulenza sono quindi uno strumento di cooperazione strutturata, che consente all'Unione di verificare la resilienza dei soggetti critici di rilevanza europea e agli Stati membri di condividere informazioni, esperienze e raccomandazioni.
Un meccanismo che riflette la natura transfrontaliera dei servizi essenziali e la necessità di una vigilanza coordinata a livello europeo.

Il gruppo per la resilienza dei soggetti critici (CERG)

La dimensione europea della resilienza prende forma nell'articolo 19 della **Direttiva CER**, che istituisce il **CERG**, il gruppo europeo incaricato di coordinare la resilienza dei soggetti critici nell'Unione.
Il decreto italiano non ne disciplina la composizione – perché è un organismo europeo – ma ne integra pienamente il funzionamento attraverso le competenze attribuite al **PCU** (art. 5, comma 6, lett. d) e gli obblighi di informazione e cooperazione previsti dagli articoli 17 e 18.
Il **CERG** riunisce rappresentanti degli **Stati membri**, la **Commissione europea** e le **agenzie competenti**, con il compito di analizzare rischi e minacce a livello europeo, favorire la convergenza delle valutazioni nazionali del rischio, promuovere buone pratiche e sostenere gli Stati nei processi di individuazione dei soggetti critici e degli **SCRE**.
È anche il destinatario delle informazioni che il **PCU** italiano deve trasmettere: dalle sintesi biennali sugli incidenti notificati (art. 5, comma 7) ai risultati delle missioni di consulenza (art. 18, comma 14).
La sua funzione è strategica, in quanto volta a creare un quadro comune di resilienza, evitare frammentazioni tra Stati e garantire che la protezione dei servizi essenziali sia coerente in tutta l'Unione.

La cooperazione tra Stati membri: come funziona

La cooperazione tra Stati membri non è un principio astratto: è un obbligo operativo che attraversa tutto il decreto CER.
L'articolo 5 assegna al **PCU** il ruolo:

- di nodo italiano della rete europea, responsabile del collegamento con i punti di contatto degli altri Stati membri (comma 6, lett. b);
- della cooperazione sulle valutazioni del rischio e sugli incidenti (comma 10);
- della trasmissione delle informazioni rilevanti agli organismi di sicurezza (comma 11).

Questa cooperazione si manifesta in più momenti; in particolare:

- nella procedura di individuazione degli **SCRE**, dove **PCU**, **ASC** e operatori partecipano alle consultazioni avviate dalla Commissione (art. 17, comma 4);
- nelle missioni di consulenza, che possono essere richieste dalla **Commissione** o da altri **Stati membri** e che prevedono scambi di informazioni tecniche, valutazioni e misure correttive (art. 18, commi 1 – 3);
- nella gestione degli incidenti fisici con potenziale impatto transfrontaliero, che devono essere notificati e condivisi secondo le procedure dell'art. 16 e sintetizzati nel rapporto biennale inviato alla **Commissione** e al **CERG** (art. 5, comma 7).

Il **PCU** è quindi il punto di raccordo che collega l'Italia alla governance europea della resilienza: coordina le notifiche, partecipa alle consultazioni, gestisce i flussi informativi e assicura che il sistema nazionale dialoghi in modo coerente con quello europeo.

Cosa cambia per gli operatori transfrontalieri

Per gli operatori che forniscono servizi essenziali in più Stati membri, la **CER** introduce un livello di complessità aggiuntivo: non basta essere conformi alla normativa nazionale ma occorre:

- garantire coerenza delle misure di resilienza tra Paesi;
- rispondere a più autorità competenti;
- partecipare alle consultazioni europee previste dall'art. 17;
- prepararsi alle missioni di consulenza disciplinate dall'art. 18;
- assicurare che i piani di continuità e le analisi delle interdipendenze siano armonizzati su scala europea.

La ratio è chiara: costruire un solo sistema di resilienza, valido in tutta l'Unione, capace di soddisfare contemporaneamente gli obblighi nazionali e le aspettative europee.
Non serve replicare modelli diversi per ogni Paese: serve un'architettura unica, scalabile, che permetta di dialogare con ASC, PCU e Commissione senza duplicazioni.

Perché la dimensione europea è la vera forza della Direttiva CER

La **Direttiva CER** nasce dalla consapevolezza che la resilienza non può più essere confinata entro i confini nazionali.
Le minacce che colpiscono i servizi essenziali – eventi climatici estremi, sabotaggi, attacchi ibridi, crisi energetiche, interruzioni della supply chain – sono per loro natura transfrontaliere.
Allo stesso modo, i servizi essenziali sono interconnessi: l'energia scorre su reti europee, i trasporti attraversano corridoi **TEN-T** (*Trans-European Transport Network*), [la Rete Transeuropea dei Trasporti: sono assi strategici continentali che collegano capitali, porti, hub logistici e aree industriali di diversi Stati membri, garantendo che persone e merci possano muoversi attraverso l'Europa come in un'unica infrastruttura continua], il digitale vive su infrastrutture fisiche distribuite, la finanza opera su piattaforme comuni.
Per questo la resilienza diventa un bene comune europeo, che richiede strumenti condivisi, responsabilità distribuite e un coordinamento costante tra Stati membri, Commissione, PCU e ASC. Il CERG, le missioni di consulenza e gli obblighi di cooperazione previsti dagli articoli 5, 17 e 18 sono l'ossatura di questa architettura.

Gli errori da evitare per gli operatori europei

Gli operatori transfrontalieri devono evitare alcuni errori che il decreto, indirettamente, rende evidenti:

- considerare la **CER** come una normativa solo nazionale;
- ignorare il ruolo delle missioni di consulenza;
- non coordinare le misure tra Paesi;
- non integrare **CER** con **NIS2, DORA** e gli altri regimi europei;
- non costruire una governance della resilienza che tenga conto delle interdipendenze continentali.

La resilienza non può essere frammentata: deve essere un sistema unico, coerente, europeo.

ROADMAP CER PER PA E OPERATORI: COSA FARE, TEMPI E PRIORITÀ

La domanda che tutti si fanno: "Da dove cominciamo?"

La **Direttiva CER** è ampia, intersettoriale, ambiziosa. Il decreto italiano che la recepisce è tecnico, articolato, denso. Molti operatori – pubblici e privati – hanno compreso che la resilienza diventerà un asse strategico della governance ma non hanno ancora chiaro quale sia il primo passo.
Questa roadmap è stata predisposta per rispondere a questa incertezza, in linea con la sequenza temporale reale che il decreto impone allo Stato e agli operatori.
La data che interessa agli operatori è il **17 luglio 2026**.
Entro quel giorno, il Governo deve adottare il DPCM che contiene l'elenco ufficiale dei soggetti critici. È la linea di demarcazione tra il *"prima"* e il *"dopo"*.

La roadmap CER: tre fasi, una scansione temporale precisa

La roadmap si sviluppa come un continuum che segue fedelmente il calendario del decreto

FASE 1 : PREPARAZIONE

La preparazione riguarda tutti, anche chi non è ancora stato designato.
Il decreto **CER** non lascia dubbi: la resilienza è una responsabilità di governo (*art. 1, comma 1, lett. b*) e non può essere improvvisata.
Il primo passo è costruire una governance interna solida.
Serve un referente CER con responsabilità chiare, un gruppo di lavoro che riunisca le funzioni chiave – *risk management*, sicurezza fisica, *ICT, operations*, *compliance*, HR, comunicazione – e un canale stabile con le **Autorità Settoriali Competenti (ASC)** e con il **Punto di Contatto Unico (PCU)** istituito dall'articolo 5.
Senza questa architettura, la resilienza rischia di diventare un insieme di iniziative sparse.
Il secondo passo è comprendere la propria criticità. Prima ancora di sapere se si è soggetti critici, occorre mappare i servizi essenziali, come definiti dall'*articolo 2, comma 1, lettera e*), e le interdipendenze che li sostengono: energia, acqua, digitale, trasporti, fornitori strategici.
La designazione CER si basa sugli *"effetti negativi rilevanti"* (art. 8) e questi effetti dipendono dalla natura dei servizi e dalla loro vulnerabilità.

Il terzo passo è avviare una pre-valutazione del rischio. L'articolo 13 richiede una valutazione multirischio complessa, che considera minacce naturali, accidentali, intenzionali e ibride, vulnerabilità fisiche e organizzative, interdipendenze e impatti potenziali.
Gli operatori più maturi iniziano prima della designazione, integrando già da subito CER con NIS 2, DORA e gli altri regimi settoriali.
Chi arriva al 17 luglio 2026 senza aver iniziato questo lavoro rischia di non riuscire a rispettare i tempi successivi.

FASE 2: ADEGUAMENTO

Entro il **17 luglio 2026** il Governo deve adottare il DPCM con l'elenco dei soggetti critici (art. 8, comma 5). Da quel momento si apre una finestra di 30 giorni entro la quale il PCU deve notificare individualmente ad ogni soggetto critico che è compreso nell'elenco dei soggetti critici (art. 8, comma 6).
La notifica è lo spartiacque operativo: da quel giorno gli obblighi CER diventano immediatamente attivi.
Il primo obbligo è la **valutazione del rischio CER** (art. 13): un'analisi completa, proporzionata e documentata.
Il secondo obbligo è l'**attuazione delle misure di resilienza** (art. 14): sicurezza fisica, personale, governance, continuità operativa, supply chain, comunicazione in emergenza, protezione fisica delle infrastrutture digitali.
Il terzo obbligo è la **capacità di notificare gli incidenti fisici** (art. 16): *"senza indebito ritardo"*, con procedure, ruoli e canali verso ASC e PCU.
Per alcuni operatori, gli obblighi europei scattano ancora prima: i soggetti che forniscono servizi essenziali ad almeno sei Stati membri devono comunicare entro un mese dalla notifica quali servizi forniscono e a quali Paesi (art. 17, comma 2). È l'avvio della procedura europea per individuare I *"soggetti critici di rilevanza europea"* (SCRE).

FASE 3: MATURITA'

La maturità è la fase in cui la resilienza diventa un modo di lavorare.
Il primo elemento è l'integrazione: l'articolo 1, comma 3, stabilisce il principio di non duplicazione. Quindi il sistema **CER** deve convivere con **NIS2, DORA** e gli altri regimi in un unico sistema di gestione.
Il secondo elemento è la verifica: esercitazioni, test, simulazioni, prove di continuità e comunicazione. La resilienza si misura nella performance, non nella carta.
Il terzo elemento è la cultura: formazione, consapevolezza, leadership, coinvolgimento del personale. Nessuna misura tecnica funziona senza cultura.
Questa fase culmina in una data precisa: **17 luglio 2028**. Entro quel giorno il PCU deve inviare alla **Commissione europea** la prima relazione biennale sulle notifiche di incidenti ricevute (art. 5, comma 7). Questo è il primo vero banco di prova del sistema italiano.
Da quel momento, la relazione diventa biennale, mentre il documento sullo stato della resilienza diventa annuale (art. 5, comma 8).

La roadmap istituzionale: cosa farà lo Stato

Mentre gli operatori si preparano, anche lo Stato segue la propria roadmap:

- **30 ottobre 2024:** accordo Stato – Regioni per definire le modalità di collaborazione tra le ASC, le regioni e le province autonome interessate (art. 5, c. 2);
- **17 gennaio 2026:** DPCM per la designazione delle ASC per il settore degli enti della pubblica amministrazione (art. 5, c. 1, lett. i);
- **17 luglio 2026:** DPCM con l'elenco dei soggetti critici (art. 8, c. 5);
- **entro 30 giorni:** notifiche individuali ai soggetti critici da parte del PCU (art. 8, c. 6)
- **entro 3 mesi** dall'istituzione di PCU e ASC: notifica alla Commissione europea (art. 5, c. 12)
- **17 luglio 2028:** prima relazione biennale (art. 5, c. 7)

Gli operatori devono essere pronti a dialogare con ASC, PCU, Dipartimento della Protezione Civile, ACN e le altre autorità competenti. La resilienza è un ecosistema: nessuno può agire da solo.

La domanda finale: "Quanto tempo abbiamo?"

La risposta è: meno di quanto pensiamo, perché:

- la designazione dei soggetti critici arriverà entro **17 luglio 2026**;
- gli obblighi scatteranno **entro 30 giorni** dalla notifica;
- le notifiche degli incidenti saranno operative da subito;
- la prima grande verifica europea arriverà il **17 luglio 2028**.

Chi aspetta rischia di arrivare tardi e nella resilienza, arrivare tardi significa essere vulnerabili.

Cyber & Cyber

Sicurezza • Dati • Geopolitica

Cyber & Cyber tratta le principali tematiche che alimentano il settore: sicurezza, tecnologie, dati, policy, malware, hacking, difesa nazionale, guerra ibrida e geopolitica. Non insegue la notizia del giorno, ma guarda con particolare attenzione alla ricostruzione di scenari, alla valutazione dei contesti nazionali, all'analisi dei casi di studio, alla descrizione delle tecnologie, agli equilibri internazionali, il tutto nei principali domini fisici: terra, acqua, aria e spazio.
È anche e soprattutto un circuito autorevole di competenze (e un tessuto connettivo di aziende, università, centri di ricerca e singoli professionisti), che promuove occasioni di incontro e confronto come conferenze, workshop e appuntamenti conviviali, tra i membri della community.

CONTATTI

https://cyberandcyber.com

Cyber &Cyber

Cyber &Cyber

cyberandcyber