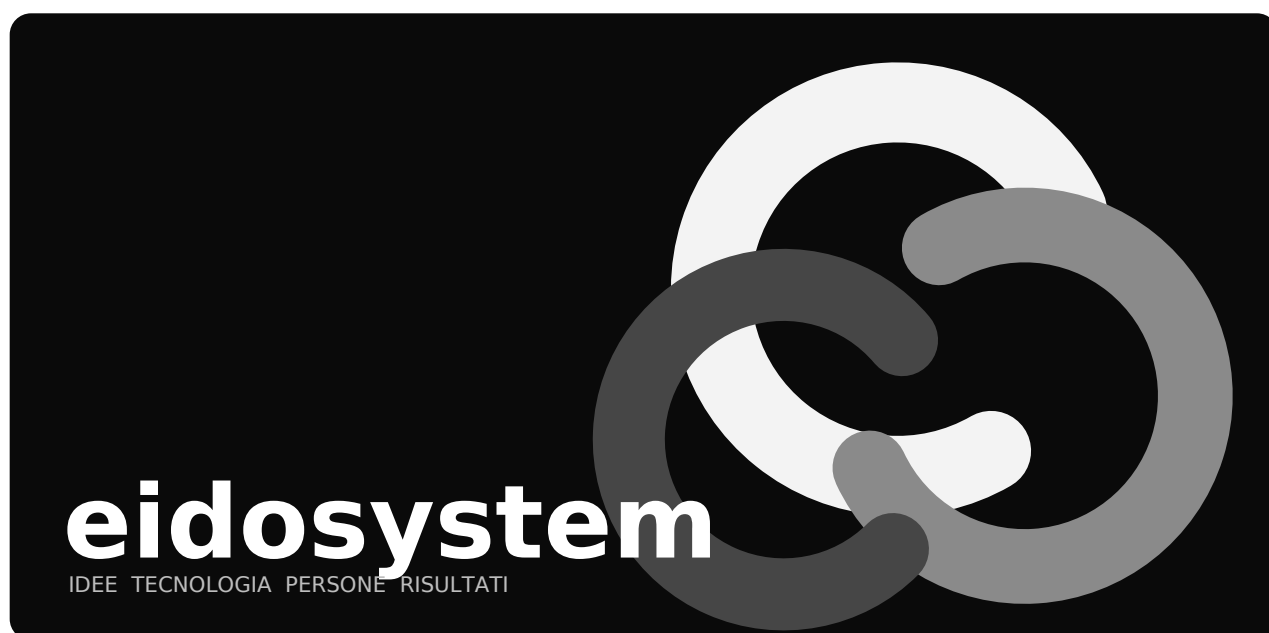


Autovalutazione della resilienza informatica aziendale

Continuità operativa risposta agli incidenti ripristino e polizza cyber

Questo strumento valuta la capacità dell'azienda di continuare a operare, prendere decisioni e ripristinare servizi e dati dopo un incidente informatico o fisico. L'obiettivo non è eliminare ogni rischio, ma rendere espliciti servizi critici, dipendenze, tempi attesi e responsabilità.



Istruzioni per la compilazione

Rispondi considerando la situazione effettivamente dimostrabile oggi. Quando assegni 2 o 3, indica una prova disponibile: documento, configurazione, verbale, contratto, log o risultato di test. Usa N A solo quando la non applicabilità è motivata.

AZIENDA

SETTORE

NUMERO ADDETTI

DATA

COMPILATO DA FACOLTATIVO

Scala di valutazione

0	Assente o sconosciuto	Il presidio non esiste oppure nessuno sa indicare come funziona.
1	Informale o parziale	Esiste in alcuni casi, dipende dalle persone o non è documentato.
2	Definito e applicato	E documentato e applicato nella maggior parte dei casi rilevanti.
3	Verificato e migliorato	E applicato, testato, misurato e riesaminato periodicamente.
N A	Non applicabile	Escludere dal calcolo soltanto indicando il motivo.

Calcolo

Somma i punti delle domande applicabili. Il massimo è pari a 3 moltiplicato per il numero di domande applicabili. Percentuale uguale punti ottenuti diviso massimo moltiplicato per 100. Valuta ogni area separatamente: una media generale può nascondere una lacuna critica.

Servizi critici e impatto

Definisce cosa deve essere protetto e con quale priorit .

01 Sono identificati i servizi e i processi senza i quali l'azienda non puo operare?

Evidenza utile Elenco servizi critici, proprietari, priorit  e impatto del fermo.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

02 Per ogni servizio sono note le dipendenze da persone, rete, energia, software, cloud e fornitori?

Evidenza utile Mappa delle dipendenze interne ed esterne e punti singoli di guasto.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

03 Sono valutati scenari realistici come ransomware, guasto, indisponibilit  cloud, incendio o assenza di connettivit ?

Evidenza utile Analisi dei rischi aggiornata, impatti economici e operativi.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Backup e ripristino

Verifica se tempi e risultati di recupero sono noti e provati.

04 Per ogni servizio critico sono definiti il tempo massimo di ripristino RTO e la perdita dati accettabile RPO?

Evidenza utile Valori approvati dal business e collegati ai sistemi effettivi.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

05 I dati critici hanno copie separate o isolate dall'infrastruttura principale e protette da accessi non autorizzati?

Evidenza utile Copie offsite, cloud o offline, separazione account e retention.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

06 E stato eseguito un ripristino completo e sono stati registrati durata, problemi e azioni correttive?

Evidenza utile Data ultimo test, risultato, tempo reale e responsabile della verifica.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Rilevazione risposta e filiera

Valuta rapidità decisionale, preparazione delle persone e dipendenze esterne.

07 Esistono monitoraggio, registri e avvisi per rilevare tempestivamente anomalie e incidenti?

Evidenza utile Fonti di log, alert, reperibilità e tempi medi di presa in carico.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

08 Il piano di risposta indica responsabili, sostituti e contatti tecnici, legali, assicurativi e istituzionali?

Evidenza utile Piano, lista contatti offline, ruoli decisionali e criteri di escalation.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

09 Piano e fornitori sono stati provati con un esercitazione e sono stati misurati i tempi reali?

Evidenza utile Verbale dell'esercitazione, lezioni apprese, SLA e azioni correttive.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Trasferimento del rischio

Verifica che la copertura assicurativa sia comprensibile e coerente con i rischi residui.

10 Esiste una polizza cyber specifica e aggiornata, distinta da eventuali coperture generiche o implicite?

Evidenza utile Polizza, appendici, data di rinnovo, broker e referente sinistri.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

11 Coperture, massimali e servizi includono gli scenari rilevanti per l'azienda?

Evidenza utile Interruzione, recupero dati, forense, legale, comunicazione, responsabilit  e fornitori.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

12 Esclusioni, franchigie, periodi di carenza, obblighi di sicurezza e tempi di denuncia sono compresi e verificati?

Evidenza utile Matrice coperture esclusioni, fornitori imposti e procedura di attivazione.

PUNTEGGIO ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ N A

NOTA

Lettura del risultato

Calcola ogni area separatamente. I livelli descrivono la preparazione osservata e non attestano conformità o sicurezza assoluta.

AREA	PUNTI	MASSIMO	PERCENTUALE
Servizi critici e impatto			
Backup e ripristino			
Risposta e filiera			
Polizza cyber			

Livelli di preparazione

0-24 Non presidato 25-49 Gestione reattiva 50-74 Gestione strutturata 75-100 Gestione misurata e migliorata

Segnali prioritari

Se una delle condizioni seguenti è vera, trattala come prioritaria anche in presenza di un punteggio complessivo elevato.

- ☐ Non sono identificati i servizi critici e le loro dipendenze.
- ☐ Non è mai stato completato un test di ripristino dei dati critici.
- ☐ Manca un piano di risposta con ruoli e contatti utilizzabile durante il fermo.
- ☐ La polizza non è stata confrontata con rischi, tempi di fermo ed esclusioni reali.

Dai punteggi alle decisioni

Scegli poche azioni verificabili. Ogni intervento dovrebbe avere un responsabile, una scadenza, un risultato atteso e una prova di completamento.

ENTRO 30 GIORNI

ENTRO 90 GIORNI

ENTRO 180 GIORNI

Quando chiedere un approfondimento

Richiedi una verifica guidata quando una risposta non è nota, quando un controllo esiste solo informalmente, quando manca una prova recente o quando una lacuna coinvolge un servizio critico, dati personali, obblighi di notifica o coperture assicurative.

Parla con un esperto www.eidosystem.com

Riferimenti ufficiali

Il questionario sintetizza principi e aree di controllo ricavati dalle fonti seguenti. Le fonti prevalgono sempre su questa autovalutazione e devono essere consultate nella versione vigente.

ENISA Cybersecurity guide for SMEs

Misure pratiche per la sicurezza e la resilienza delle piccole e medie imprese.

<https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>

NIST Cybersecurity Framework 2.0

Gestione del rischio attraverso governo, identificazione, protezione, rilevazione, risposta e recupero.

<https://www.nist.gov/cyberframework>

NIST SP 800 34 Contingency Planning Guide

Analisi di impatto, priorità, continuità operativa e prove di ripristino.

<https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>

Unione europea Direttiva NIS2 2022 2555

Gestione del rischio, continuità, filiera e segnalazione degli incidenti.

<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

EIOPA Chiarezza delle esclusioni e coperture cyber

Chiarezza delle condizioni, delle esclusioni e della coerenza con il mercato destinatario.

https://www.eiopa.europa.eu/eiopa-publishes-supervisory-statements-exclusions-related-systemic-events-and-management-non-2022-09-22_en

Limiti dello strumento

Il risultato non costituisce audit di sicurezza né consulenza assicurativa. La polizza trasferisce parte del rischio residuo e non sostituisce prevenzione, backup e continuità operativa.

Documento predisposto da Eidosystem Versione 1.0 17 settembre 2026