REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

DIREZIONE GENERALE DELL'INNOVAZIONE E SICUREZZA IT

SERVIZIO SICUREZZA IT

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE
DIREZIONE GENERALE DELL'INNOVAZIONE E SICUREZZA IT
SERVIZIO SICUREZZA IT

Linee guida per il coordinamento operativo delle attività comunali finalizzate alla predisposizione del Documento comunale di sicurezza cibernetica

Indice

1 PREMESSA

La trasformazione digitale della Pubblica Amministrazione, la crescente interconnessione dei sistemi informativi e l'ampliamento dei servizi erogati in modalità digitale rendono la sicurezza cibernetica un presupposto essenziale per assicurare la continuità amministrativa, la tutela dei dati e l'affidabilità dell'azione pubblica.

In tale contesto, dando attuazione alla Legge regionale 8 maggio 2025, n. 12, art. 6, co. 16 e in coerenza con le previsioni del D.Lgs. n. 138/2024 di recepimento della Direttiva (UE) 2022/2555 (cd. "Direttiva NIS2") e con il quadro normativo di riferimento, l'Amministrazione regionale ha attivato un nuovo intervento, rivolto agli Enti del territorio, finalizzato all'**analisi e valutazione dei propri sistemi informatici e alla realizzazione di primi interventi di sicurezza cibernetica**, allo scopo di rafforzare i livelli di sicurezza cibernetica degli Enti locali, prevenire potenziali rischi e vulnerabilità in grado di compromettere la continuità dei servizi pubblici e garantire una risposta efficace alle minacce informatiche.

L'intervento prevede la concessione di contributi agli Enti locali finalizzati alla **redazione di un Documento comunale di sicurezza cibernetica**, di seguito DCSC, volto a rappresentare il **livello di sicurezza dei sistemi informativi dell'Ente e a individuare le principali azioni di miglioramento**. In particolare, il DCSC deve contenere almeno l'analisi e la valutazione dei sistemi informatici dell'Ente, l'individuazione delle vulnerabilità e l'identificazione dei primi interventi per il miglioramento dei livelli di sicurezza cibernetica.

In tale quadro, le presenti Linee guida intendono fornire agli Enti aderenti all'iniziativa regionale **indicazioni operative comuni per la predisposizione del DCSC del singolo Ente** al fine di assicurare omogeneità metodologica, proporzionalità rispetto alla dimensione e alla complessità organizzativa dell'Ente, nonché confrontabilità degli esiti a livello regionale.

2 SCOPO DEL DOCUMENTO

Le presenti Linee guida hanno lo scopo di **supportare i Comuni e le Unioni di Comuni aderenti all'iniziativa regionale nella redazione del Documento comunale di sicurezza cibernetica**, fornendo indicazioni operative per rappresentare in modo ordinato e omogeneo il livello di sicurezza dei sistemi informativi dell'Ente.

Il documento definisce un **percorso metodologico per l'individuazione dell'ambito di analisi, la ricognizione degli asset, dei servizi e dei dati rilevanti, l'identificazione delle principali vulnerabilità** e dei gap di sicurezza, nonché la definizione dei primi interventi di miglioramento dei livelli di sicurezza cibernetica. Le Linee guida costituiscono, dunque, un riferimento di indirizzo e coordinamento operativo e non intendono sostituire le valutazioni tecniche, organizzative e gestionali proprie di ciascun Ente.

La loro applicazione deve avvenire secondo criteri di proporzionalità, tenendo conto della dimensione dell'Ente, della complessità del relativo contesto organizzativo, del livello di digitalizzazione dei servizi erogati e delle risorse disponibili.

La standardizzazione del percorso metodologico e degli output prodotti dagli Enti è altresì funzionale a consentire all'**Amministrazione regionale**, successivamente alla trasmissione dei DCSC, lo **svolgimento di attività di analisi, monitoraggio e lettura omogenea degli esiti a livello regionale**. Tali attività potranno comprendere l'elaborazione, da parte della Regione, di una **classificazione del livello di compliance e maturità rilevato**, secondo criteri uniformi definiti dall'Amministrazione regionale, con finalità di governance, indirizzo, prioritizzazione e accompagnamento.

Restano, in ogni caso, ferme, per quanto applicabili, sia con riferimento alla predisposizione del DCSC da parte degli Enti, sia con riferimento alle successive attività di analisi svolte dall'Amministrazione regionale, le indicazioni contenute nelle Linee guida dell'Agenzia per la Cybersicurezza Nazionale per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90, nonché gli ulteriori obblighi e adempimenti previsti dalla normativa vigente in materia di cybersicurezza.

3 SOGGETTI DESTINATARI

Le presenti Linee guida sono rivolte ai **Comuni e alle Unioni di Comuni** aderenti all'iniziativa regionale per la redazione del Documento comunale di sicurezza cibernetica.

All'interno degli Enti destinatari, il documento si rivolge, in particolare, a:

- organi di direzione e governo dell'Ente;
- responsabili amministrativi e organizzativi coinvolti nella gestione dei servizi digitali;
- Responsabile per la transizione digitale, ove individuato;
- referenti ICT e sicurezza informatica;
- uffici e alle strutture dell'Ente che, a vario titolo, partecipano alla raccolta delle informazioni, alla compilazione della matrice di assessment e alla definizione degli interventi di miglioramento.

4 TERMINI E DEFINIZIONI

Termine	Definizione
Asset	Risorsa, componente o elemento rilevante per l'erogazione dei servizi dell'Ente e per il funzionamento dei relativi sistemi informativi. Possono costituire asset, a titolo esemplificativo, hardware, software, dati, servizi digitali, infrastrutture, apparati di rete, postazioni di lavoro e sistemi di sicurezza.
Asset critico	Asset la cui compromissione, indisponibilità o alterazione può incidere in modo significativo sulla continuità amministrativa, sull'erogazione dei servizi pubblici, sulla tutela dei dati o sul funzionamento dell'Ente.

Termine	Definizione
Assessment	Attività di analisi e valutazione strutturata finalizzata a rilevare lo stato corrente dell'Ente rispetto a determinati ambiti di sicurezza cibernetica, anche attraverso la raccolta di informazioni, la compilazione di check-list o matrici e l'individuazione di eventuali carenze o aree di miglioramento.
Matrice di assessment	Strumento operativo di supporto alla raccolta e sistematizzazione delle informazioni relative al livello di sicurezza cibernetica dell'Ente, utile alla predisposizione del DCSC e all'individuazione dei principali gap e ambiti di miglioramento.
Function	Macro-ambito logico utilizzato nella Matrice di assessment per organizzare le attività e le misure di sicurezza.
Category	Ambito di dettaglio riconducibile a una Function, utilizzato per classificare specifici obiettivi, attività o misure di sicurezza.
DCSC	Documento comunale di sicurezza cibernetica predisposto dall'Ente nell'ambito dell'iniziativa regionale, volto a rappresentare il livello di sicurezza dei sistemi informativi dell'Ente, individuare le principali vulnerabilità e identificare i primi interventi di miglioramento dei livelli di sicurezza cibernetica.
Ente	Il Comune o l'Unione di Comuni aderente all'iniziativa regionale e destinatario delle presenti Linee guida.

5 RIFERIMENTI NORMATIVI

Le presenti Linee guida sono predisposte tenendo conto del seguente quadro di riferimento normativo, programmatico e tecnico-metodologico:

- 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, cosiddetta direttiva NIS2;
- Decreto legislativo 4 settembre 2024, n. 138, recante il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione;
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i., recante il "Codice in materia di protezione dei dati personali";
- Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici;
- Decreto-legge 21 settembre 2019, n. 105 recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica"
- Direttiva del Presidente del Consiglio dei Ministri 29 dicembre 2023 recante "Resilienza cibernetica del Paese - Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici"

- Decreto Direttoriale ACN n. 21007/24 del 27 giugno 2024 recante "Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221"
- Linee guida dell'Agenzia per la Cybersicurezza Nazionale per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90, pubblicate nel mese di novembre 2024;
- Legge regionale 8 maggio 2025, n. 12, con particolare riferimento all'articolo 6, comma 16, che prevede interventi finalizzati al rafforzamento della sicurezza cibernetica degli Enti locali;
- Legge regionale 6 febbraio 2026, n. 1, recante la Legge di stabilità regionale 2026, e legge regionale 6 febbraio 2026, n. 2, recante il Bilancio di previsione 2026-2028, per quanto attiene alla programmazione delle risorse destinate agli interventi in materia di sicurezza cibernetica degli Enti locali;
- Deliberazione della Giunta regionale n. 11/37 dell'11 marzo 2026, avente a oggetto "Contributi per la sicurezza cibernetica degli Enti locali. Legge regionale n. 1/2026 e n. 2/2026, Tabella A. Legge regionale n. 12/2025, art. 6, comma 16", e relativo allegato;
- Deliberazione della Giunta regionale n. 15/15 del 19 marzo 2025, concernente "Agenda digitale del PIAO 2025-2027. Misure per il rafforzamento della sicurezza cibernetica dei Comuni e delle Unioni di Comuni della Sardegna. Intervento Cyber2COM".

6 IL DOCUMENTO COMUNALE DI SICUREZZA CIBERNETICA: SCOPO, PERIMETRO E STRUTTURA MINIMA

Il Documento comunale di sicurezza cibernetica (DCSC) rappresenta lo strumento attraverso il quale l'Ente descrive in modo organico il proprio livello di esposizione ai rischi cibernetici, individua le principali vulnerabilità e definisce i primi interventi da attuare per il rafforzamento dei presidi di sicurezza.

Il DCSC deve essere inteso quale strumento di governance, analisi e programmazione, e non come mero adempimento di natura tecnica. Esso consente all'Ente di acquisire una rappresentazione strutturata del proprio perimetro digitale, individuare i sistemi e i servizi maggiormente rilevanti per la continuità amministrativa, rilevare le principali vulnerabilità tecniche e i principali gap o debolezze di controllo di natura organizzativa, procedurale e documentale, valutare i rischi prioritari e definire interventi di miglioramento realistici, sostenibili e proporzionati rispetto alla dimensione e alla complessità dell'Ente.

Il perimetro di analisi del DCSC deve includere almeno gli elementi richiamati dalla Deliberazione della Giunta regionale n. 11/37 dell'11 marzo 2026, ossia utenti, hardware, software, dati e data center. In chiave operativa, l'Ente dovrà considerare anche le sedi, le reti, le postazioni di lavoro, i server, i servizi cloud, le applicazioni gestionali, i sistemi di posta elettronica e PEC, i servizi digitali essenziali, i sistemi di backup, gli accessi remoti, le utenze privilegiate e i fornitori ICT.

Al fine di assicurare omogeneità metodologica e confrontabilità degli esiti a livello regionale, il DCSC deve essere redatto secondo una struttura minima comune. La seguente tabella individua le sezioni che ciascun Ente è tenuto a considerare nella predisposizione del documento.

#	Sezione del DCSC	Contenuto minimo atteso
1	**Anagrafica dell'Ente e riferimenti del documento**	Denominazione dell'Ente, referenti coinvolti, eventuali fornitori incaricati, data, versione e ambito di validità del documento.
2	**Obiettivi e ambito del DCSC**	Finalità del documento, collegamento con l'iniziativa regionale e descrizione sintetica degli obiettivi di sicurezza perseguiti.
3	**Perimetro digitale, asset e servizi critici**	Utenti, sedi, hardware, software, dati, data center/cloud, reti, applicazioni, servizi digitali essenziali, fornitori ICT e accessi remoti, con indicazione degli elementi ricompresi nel perimetro di analisi e specifica evidenza degli asset e dei servizi ritenuti critici per la continuità amministrativa dell'Ente.
4	**Modalità di svolgimento dell'assessment**	Descrizione delle attività svolte, soggetti coinvolti, strumenti utilizzati, fonti informative, evidenze raccolte, periodo di esecuzione e eventuali limiti dell'analisi.
5	**Esito dell'assessment e livello di maturità rilevato**	Sintesi degli esiti emersi dalla matrice di assessment, articolata per "Function", con evidenza del livello di maturità rilevato, delle principali aree presidiate e delle principali aree di debolezza.
6	**Vulnerabilità, gap e rischi prioritari**	Principali vulnerabilità tecniche, gap organizzativi, procedurali e documentali; minacce associate; misure già attive; probabilità, impatto e livello di rischio corrente, valutati tenendo conto dei presidi esistenti e con riferimento alle Function e alle Category pertinenti.
7	**Misure esistenti e interventi prioritari**	Presidi già attivi e relativo stato di effettiva operatività; contromisure esistenti; azioni di trattamento o mitigazione proposte; beneficio atteso in termini di riduzione del rischio; priorità; tempi indicativi; responsabilità di attuazione.
8	**Monitoraggio, aggiornamento e reporting**	Modalità di aggiornamento del DCSC, monitoraggio degli interventi, revisione periodica e reporting.

Il DCSC potrà contenere informazioni sensibili relative ad architetture, configurazioni, vulnerabilità, asset critici, fornitori e misure di sicurezza. Per tale ragione, il documento dovrà essere conservato con modalità idonee a garantirne riservatezza, integrità e accesso limitato ai soli soggetti autorizzati.

7 METODO OPERATIVO PER LA REDAZIONE DEL DCSC

Ai fini della stesura del DCSC, le presenti Linee guida propongono un metodo operativo volto a supportare gli Enti nella raccolta, organizzazione e valutazione delle informazioni necessarie alla predisposizione del documento.

Il metodo ha natura orientativa e costituisce uno strumento di supporto flessibile, adattabile in funzione della tipologia di Ente, della dimensione organizzativa, del livello di

digitalizzazione, della complessità del perimetro informatico e della disponibilità di risorse e competenze. L'Ente potrà pertanto modulare le attività, il livello di dettaglio dell'analisi e le modalità operative di svolgimento, purché il DCSC finale mantenga la struttura minima comune indicata nelle presenti Linee guida e contenga gli elementi essenziali richiesti dall'iniziativa regionale.

Si riporta di seguito il metodo operativo proposto, articolato in fasi logiche e output attesi, da utilizzare quale strumento di supporto flessibile alla redazione del DCSC.

Fase	Attività principale	Output atteso nel DCSC
1. Avvio	Individuazione del referente comunale, dei soggetti coinvolti, degli eventuali fornitori incaricati; raccolta dei documenti disponibili e pianificazione delle attività	Anagrafica dell'Ente e riferimenti del documento; Obiettivi e ambito del DCSC; prima descrizione del percorso seguito e dei soggetti coinvolti
2. Definizione del perimetro	Identificazione di sedi, servizi, asset, dati, utenti, fornitori, infrastrutture locali e cloud; individuazione degli asset e dei servizi critici per la continuità amministrativa	Perimetro digitale, asset e servizi critici, con indicazione degli ambiti inclusi ed eventualmente esclusi dall'analisi
3. Assessment	Compilazione della matrice di assessment, raccolta delle informazioni a supporto, analisi documentale, eventuali interviste ai referenti e ricognizione delle evidenze disponibili	Modalità di svolgimento dell'assessment; Esito dell'assessment e livello di maturità rilevato
4. Analisi di vulnerabilità e rischi	Ricognizione preliminare delle misure già presenti e del relativo stato di attuazione; individuazione delle principali vulnerabilità tecniche, dei gap organizzativi, procedurali e documentali e delle debolezze di controllo; identificazione delle minacce rilevanti; valutazione di probabilità, impatto e livello di rischio corrente tenendo conto dei presidi esistenti.	Vulnerabilità, gap e rischi prioritari
5. Individuazione degli interventi	Definizione delle opzioni di trattamento del rischio e delle azioni di mitigazione o miglioramento, attribuzione delle priorità, beneficio atteso in termini di riduzione del rischio, individuazione di tempi, responsabilità di attuazione, prerequisiti e dipendenze operative.	Misure esistenti e interventi prioritari
6. Validazione e aggiornamento	Verifica interna dei contenuti, approvazione o presa d'atto del documento, definizione delle modalità di conservazione, monitoraggio degli interventi e revisione periodica	Monitoraggio, aggiornamento e reporting; versione finale del DCSC validata dall'Ente

7.1 UTILIZZO DELLA MATRICE DI ASSESSMENT: FUNCTION, CATEGORY E AMBITI MINIMI

La matrice di assessment costituisce lo strumento operativo di supporto alla raccolta delle informazioni necessarie alla predisposizione del DCSC. Essa consente all'Ente di effettuare una prima autovalutazione del livello di maturità in materia di sicurezza cibernetica, evidenziando punti di forza, carenze e aree prioritarie di miglioramento.

La matrice è organizzata in sei macro-funzioni, articolate in Category, che consentono di analizzare i principali ambiti di sicurezza rilevanti per un Ente locale.

Function	Category	Finalità operativa
Govern	Contesto organizzativo; strategia di gestione del rischio; ruoli e responsabilità; politiche; supervisione; gestione del rischio della catena di approvvigionamento	Governo della sicurezza, ruoli, responsabilità, politiche, supervisione e gestione del rischio anche verso i fornitori
Identify	Gestione degli asset; risk assessment; miglioramento; data management	Conoscenza di asset, dati, servizi, vulnerabilità/gap e rischi
Protect	Identità, autenticazione e controllo degli accessi; consapevolezza e formazione; sicurezza dei dati; sicurezza delle piattaforme; resilienza dell'infrastruttura tecnologica	Misure preventive su identità, accessi, dati, formazione, sistemi, backup e infrastruttura
Detect	Monitoraggio continuo; analisi degli eventi avversi	Monitoraggio, logging e rilevazione di eventi anomali
Respond	Gestione degli incidenti; analisi degli incidenti; comunicazione della risposta; mitigazione degli incidenti	Gestione, analisi, comunicazione e mitigazione degli incidenti
Recover	Esecuzione del piano di ripristino; comunicazione sul ripristino	Ripristino dei servizi e comunicazione post-incidente

Per ciascuna Category la matrice prevede una o più domande, rispetto alle quali l'Ente è chiamato a esprimere un'autovalutazione, anche sulla base delle indicazioni contenute nella colonna "Guida alla valutazione". La compilazione deve essere fondata su informazioni verificabili e, ove possibile, supportata da evidenze documentali o tecniche, quali inventari, procedure, contratti, report, configurazioni, registri, esiti di test, screenshot o dichiarazioni motivate del referente tecnico.

Le informazioni raccolte sono quindi valutate dall'Ente ai fini dell'aggiornamento del DCSC. Le singole domande della matrice non costituiscono sezioni autonome del documento e non devono essere riprodotte integralmente; esse servono ad alimentare il quadro conoscitivo, l'individuazione delle vulnerabilità e dei gap, la valutazione dei rischi e la definizione degli interventi prioritari.

Gli elementi risultanti dalla compilazione della matrice di assessment, unitamente ai contenuti rappresentati nel DCSC, potranno inoltre essere utilizzati dall'Amministrazione regionale, successivamente alla trasmissione del documento, per lo svolgimento di analisi omogenee e comparative degli esiti. Tali analisi potranno concorrere all'attribuzione, da parte della Regione, di una classe sintetica rappresentativa del livello di compliance e maturità dell'Ente.

7.2 ANALISI DELLE VULNERABILITÀ, DEI GAP E VALUTAZIONE DEL RISCHIO

A seguito della compilazione della matrice di assessment, l'Ente individua, per le Function e le Category pertinenti, le principali vulnerabilità tecniche, i gap e le debolezze di controllo emersi, valutandone la rilevanza rispetto agli asset, ai servizi e ai dati interessati, con specifica evidenza del collegamento con gli elementi critici per la continuità amministrativa, ove presenti.

A titolo esemplificativo e non esaustivo, si riportano di seguito alcuni esempi di vulnerabilità e gap che possono emergere dalla compilazione della matrice di assessment, articolati per Function e Category.

Function	Category	Esempio di vulnerabilità o gap
Govern	Ruoli, responsabilità e correlati poteri	Ruoli cyber non formalizzati o responsabilità non comunicate alle strutture interessate.
Identify	Gestione degli asset	Asset non censiti o non classificati in base alla criticità per la continuità amministrativa.
Protect	Gestione delle identità, autenticazione e controllo degli accessi	Utenze privilegiate non censite o non soggette a revisione periodica; assenza di MFA su sistemi rilevanti.
Protect	Sicurezza dei dati	Backup non verificati mediante test di ripristino o non adeguatamente protetti.
Detect	Monitoraggio continuo	Log non centralizzati o non analizzati periodicamente, con ridotta capacità di rilevazione degli eventi.

La vulnerabilità o il gap identificato deve essere analizzato in relazione all'asset o al servizio interessato, alla minaccia che potrebbe sfruttarla e agli effetti attesi sulla continuità amministrativa, sulla riservatezza, integrità e disponibilità dei dati e sulla capacità dell'Ente di erogare servizi ai cittadini.

La valutazione del rischio deve essere semplice, comprensibile e ripetibile. Per ciascun rischio rilevante, l'Ente riporta almeno gli elementi indicati nella tabella seguente.

Elemento	Contenuto da riportare nel DCSC
Asset o servizio interessato	Asset, servizio o processo impattato, ad esempio protocollo, servizi demografici, posta elettronica, server, backup, rete comunale o gestionale cloud.
Minaccia	Evento o scenario di minaccia, ad esempio ransomware, accesso non autorizzato, perdita di dati, indisponibilità del servizio o compromissione di credenziali.
Vulnerabilità o gap	Debolezza tecnica, organizzativa, procedurale o documentale che rende più probabile la minaccia o ne aumenta l'impatto.

Elemento	Contenuto da riportare nel DCSC
Probabilità	Valore da 1 a 5, corredato della relativa motivazione qualitativa sintetica, definito tenendo conto di esposizione, facilità di sfruttamento, storico degli eventi, livello di esposizione verso l'esterno, dipendenza da fornitori e misure esistenti effettivamente attive.
Impatto	Valore da 1 a 5, corredato della relativa motivazione qualitativa sintetica, definito in base a servizi coinvolti, dati trattati, numero di utenti interessati, durata stimata del disservizio, conseguenze operative, obblighi di comunicazione o notifica, impatti reputazionali e capacità dell'Ente di garantire la continuità amministrativa.
Livello di rischio	Livello di rischio corrente, classificato come basso, medio, alto o critico, determinato combinando probabilità e impatto secondo la scala comune 1-5 e le soglie definite nelle presenti Linee guida, con indicazione degli elementi che ne giustificano la criticità.
Misure esistenti	Presidi già attivi, anche se parziali, quali procedure, configurazioni, strumenti tecnici, controlli organizzativi o misure contrattuali.
Intervento proposto	Azione di mitigazione o miglioramento collegata al rischio individuato.
Priorità	Alta, media o bassa, assegnata in funzione del livello di rischio e della criticità del servizio interessato.
Tempistica	Breve, medio o lungo periodo, con indicazione di eventuali vincoli, prerequisiti o dipendenze operative.

Ai fini di omogeneità metodologica e confrontabilità degli esiti a livello regionale, il DCSC utilizza una scala numerica unica da 1 a 5 per la probabilità e per l'impatto.

In particolare, la probabilità è valutata secondo i seguenti criteri indicativi:

Valore	Probabilità	Criterio indicativo
1	Remota	Evento non noto o molto difficilmente verificabile nel contesto dell'Ente.
2	Improbabile	Evento possibile ma senza indicatori significativi di esposizione o precedenti rilevanti.
3	Possibile	Evento plausibile in presenza di esposizione, dipendenze esterne o precedenti nel settore.
4	Probabile	Evento favorito da debolezze significative, esposizione rilevante o misure solo parziali.
5	Molto probabile	Evento altamente plausibile per esposizione elevata, vulnerabilità facilmente sfruttabile, eventi ricorrenti o assenza di presidi essenziali.

L'impatto è, invece, valutato secondo i seguenti criteri:

Valore	Impatto	Criterio indicativo
1	Trascurabile	Nessun impatto significativo su servizi, dati o continuità amministrativa.
2	Limitato	Disservizio circoscritto, pochi utenti coinvolti, dati non critici, ripristino rapido.
3	Significativo	Interruzione di un servizio rilevante, impatto su uffici o procedimenti, trattamento di dati personali o ripristino non immediato.
4	Grave	Interruzione di servizi essenziali, perdita o alterazione di dati, possibili obblighi di comunicazione o notifica, impatto rilevante su cittadini o uffici.
5	Molto grave	Indisponibilità prolungata di servizi essenziali, ampia compromissione di dati, grave impatto sulla continuità amministrativa, sulla fiducia dei cittadini o sull'operatività dell'Ente.

La valutazione del rischio deve tenere conto delle misure già attive e della loro effettiva applicazione. Le misure esistenti non devono essere riportate solo come informazione descrittiva, ma devono essere considerate nella stima della probabilità e, ove incidano sugli effetti dell'evento, dell'impatto. Le misure solo pianificate, non attuate o non verificabili non devono ridurre il livello di rischio corrente.

Il livello di rischio è determinato secondo la formula: Rischio = Probabilità × Impatto. Il valore risultante è classificato secondo le seguenti soglie:

Valore P x I	Livello di rischio
1 – 4	Basso
5 – 9	Medio
10 – 16	Alto
17 - 25	Critico

Il valore risultante dalla combinazione tra probabilità e impatto non esaurisce la valutazione del rischio. Per ciascun rischio rilevante, l'Ente deve riportare una **motivazione qualitativa della classificazione attribuita**, esplicitando gli elementi che determinano la criticità del rischio, quali la rilevanza dell'asset o del servizio interessato, la tipologia e il volume dei dati trattati, il numero di utenti coinvolti, il livello di esposizione, la dipendenza da fornitori, le misure esistenti effettivamente attive e le conseguenze operative sulla continuità amministrativa.

L'Ente può motivatamente elevare il livello di rischio qualora la criticità del servizio o dei dati trattati lo richieda; eventuali riduzioni rispetto al valore risultante dalla combinazione probabilità × impatto devono essere motivate.

7.3 INDIVIDUAZIONE DEGLI INTERVENTI

Le vulnerabilità, i gap e i rischi individuati costituiscono la base per la definizione degli interventi di miglioramento. Ciascun intervento deve essere collegato a uno specifico rischio, vulnerabilità o gap, indicare il beneficio atteso in termini di riduzione del rischio e riportare la relativa priorità. Ove possibile, devono essere inoltre indicati la tempistica di attuazione, il soggetto responsabile e le eventuali dipendenze operative.

Gli interventi possono avere natura governance/procedurale, tecnologica o formativa, di cui si riportano di seguito alcuni esempi.

Tipo di intervento	Esempi
Organizzativo o procedurale	Formalizzazione di ruoli e responsabilità cyber; definizione o aggiornamento delle procedure di gestione degli incidenti; revisione del processo di gestione delle utenze; inserimento di requisiti di sicurezza nei contratti ICT.
Tecnologico	Attivazione dell'autenticazione multifattore; aggiornamento dei sistemi; rafforzamento delle soluzioni di backup e dei test di ripristino; centralizzazione dei log; configurazione o potenziamento di firewall, antivirus/EDR e strumenti di monitoraggio.
Formativo	Sessioni di awareness per gli utenti; formazione mirata per amministratori di sistema e utenti privilegiati; esercitazioni su phishing e gestione degli incidenti; aggiornamento periodico dei referenti comunali.

Per ciascun intervento deve essere indicata una priorità, come di seguito riportato.

Priorità	Criterio indicativo
Alta	Intervento necessario per ridurre rischi critici o elevati su servizi essenziali, dati sensibili, accessi privilegiati o vulnerabilità facilmente sfruttabili.
Media	Intervento utile a rafforzare presidi esistenti o a ridurre rischi significativi, ma non immediatamente critici.
Bassa	Intervento migliorativo, documentale o evolutivo, da programmare in una fase successiva.

Infine, il DCSC deve indicare, per ciascun intervento prioritario, il beneficio atteso in termini di riduzione del rischio, specificando quale criticità l'intervento intende mitigare.

8 OUTPUT ATTESI E AGGIORNAMENTO

Al termine del percorso, l'Ente dispone di un DCSC completo, coerente con la struttura minima indicata nelle presenti Linee guida e supportato da informazioni verificabili. Gli output minimi attesi sono:

Output minimo	Descrizione
DCSC	Documento principale redatto secondo la struttura minima indicata nelle presenti Linee guida
Matrice di assessment compilata	Strumento di raccolta dati e autovalutazione utilizzato per alimentare il DCSC
Evidenze a supporto	Documentazione o riferimenti interni che supportano le informazioni riportate*

**Nei casi in cui le evidenze contengano dati tecnici sensibili, credenziali, dettagli architetturali, vulnerabilità o informazioni sui fornitori, esse devono essere conservate con accesso controllato.*

A seguito della trasmissione del DCSC, della matrice di assessment compilata e delle eventuali evidenze a supporto, **l'Amministrazione regionale procederà all'analisi degli esiti restituiti dagli Enti**, al fine di disporre di un quadro conoscitivo omogeneo sul livello di sicurezza cibernetica e di compliance e maturità rilevato a livello regionale.

In esito a tale attività, **l'Amministrazione regionale potrà attribuire a ciascun Ente una classe sintetica rappresentativa del livello di compliance e maturità rilevato**, determinata secondo **criteri uniformi e proporzionati**. A tal fine, potranno essere considerati, a titolo esemplificativo, gli esiti della matrice di assessment, il livello di presidio delle diverse Function e Category, la presenza di carenze in ambiti essenziali di sicurezza, la criticità degli asset, dei servizi e dei dati interessati, il livello dei rischi prioritari indicati nel DCSC, lo stato di effettiva attuazione delle misure esistenti, la disponibilità di evidenze a supporto e la coerenza degli interventi proposti rispetto ai gap, alle vulnerabilità e ai rischi rilevati.

In particolare, all'Ente potrà essere attribuita una delle seguenti **classi sintetiche**:

- **verde**: livello di compliance e maturità complessivamente adeguato o presidiato, con presenza di misure, processi o evidenze idonei a rappresentare un assetto di sicurezza sostanzialmente coerente con gli ambiti oggetto di assessment;
- **giallo**: livello di compliance e maturità intermedio o parziale, con presenza di misure o presidi non pienamente strutturati e con aree di miglioramento da rafforzare o completare;
- **rosso**: livello di compliance e maturità carente o non adeguatamente presidiato, con presenza di criticità significative o diffuse tali da richiedere attenzione prioritaria nell'ambito delle successive attività di monitoraggio, indirizzo e accompagnamento.

Si precisa che il DCSC deve rappresentare la situazione corrente dell'Ente e deve essere aggiornato in caso di variazioni significative del perimetro digitale (es. introduzione di nuovi servizi digitali rilevanti), dell'organizzazione (es. modifica organizzativa che incide su ruoli e responsabilità), dell'esposizione alle minacce (es. emersione di nuove campagne di

phishing) o delle misure di sicurezza adottate (es. attivazione o modifica di sistemi di backup).