SISTEMA DI GESTIONE PER LA CYBERSECURITY - NIS 2

Policy A
Gestione del rischio

Controllo del documento	
Rev.	1.0
Data di emissione	15.05.2026
Autore	Sibille Tschenett - Pietro Lanzetta
Firma Autore	
Firma per approvazione	
Stato del documento	In uso ☑ Ritirato ☐

1. Scopo

Lo scopo della Policy di gestione del rischio adottata dall'organizzazione è quello di assicurare che le esigenze e le aspettative degli stakeholder, inerenti alla cybersicurezza e alla data protection siano compiutamente soddisfatte.

Per tale proposito l'organizzazione, nell'ambito più ampio del sistema di gestione NIS 2, e in quello più circoscritto riferito a tale Policy, intende individuare le minacce che possono compromettere il regolare, sicuro e continuativo funzionamento dei processi e gestirle affinché, anche a seguito di eventuali incidenti, non comportino danni.

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
GOVERNARE - GV La strategia di gestione del rischio di cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate	**Contesto organizzativo (GV.OC):** Il contesto - missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali - che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso	**GV.OC-04** Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati
	Strategia di gestione del rischio (GV.RM): Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo	**GV.RM-03** Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione
IDENTIFICARE - ID I rischi attuali di cybersecurity dell'organizzazione sono compresi	**Valutazione del rischio (Risk Assessment) (ID.RA):** È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti	**ID.RA-05** Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio
		ID.RA-06 Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate

3. Attività operative e registrazioni

Relativamente alla gestione del rischio perciò l'organizzazione procede, sistematicamente, a eseguire le attività riportate e attuare i seguenti controlli:

GV.OC-04 - Controllo 1

Mantenere un elenco aggiornato dei sistemi informativi e di rete rilevanti, che costituiscono gli asset strategici, grazie ai quali l'organizzazione eroga il servizio secondo quanto concordato.

Il registro è documentato nel modulo **MOD-01-Rischio Cyber** alla scheda **Rischio** e riporta:

- L'id dell'asset
- La denominazione
- Il tipo
- La funzione eseguita
- L'ubicazione
- Il responsabile
- Eventuali funzioni dipendenti dal funzionamento dell'asset

GV.RM-03 - Controllo 1

Definire, attuare, aggiornare e documentare un Piano di gestione dei rischi per la sicurezza informatica, **MOD-02-Piano di gestione rischi**, che stabilisce come:

- Identificare i rischi
- Analizzare la probabilità e l'impatto
- Valutare l'entità dei rischi
- Monitorare l'evoluzione di tali rischi

ID.RA-05 - Controllo 1

Eseguire e documentare, nel **MOD-01-Rischio Cyber** alla scheda **Rischio,** la valutazione del rischio riferito ai sistemi informativi e di rete che l'organizzazione ha individuato come asset strategici, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi attraverso le seguenti operazioni:

- Determinare la rilevanza dell'asset strategico per ottenere il valore di Impatto
- Determinare le entità delle minacce interne ed esterne presenti nel contesto per ottenere il valore medio di tali minacce e stimare il valore della Probabilità
- Determinare il valore del rischio per ciascun asset strategico attraverso il prodotto Probabilità x Impatto = Rischio

- Valutare il rischio cyber riferito a ciascun asset strategico e al loro insieme secondo quanto definito dal **MOD-02-Piano di gestione rischi**

ID.RA-05 - Controllo 2

Eseguire la valutazione del rischio, nel **MOD-01-Rischio Cyber,** a seguito di:

- Incidenti significativi
- Variazioni organizzative inerenti a ruoli e mansioni
- Mutamenti nell'esposizione alle minacce interne ed esterne individuate e valutate
- Almeno ogni 2 anni, a prescindere dal contesto, come stabilito nel **MOD-02-Piano di gestione rischi**

ID.RA-05 - Controllo 3

Approvare, mediante gli organi di amministrazione e direttivi, la valutazione del rischio i cui risultati sono cronologicamente documentati nel modulo **MOD-01-Rischio Cyber** alla scheda **Monitoraggio**.

ID.RA-05 - Controllo 4 [Soggetti essenziali]

Quando si manifestano e rilevano vulnerabilità, la Probabilità che le minacce interne ed esterne "vadano a segno" aumenta e dunque aumenta il Rischio Cyber.

L'organizzazione perciò procede a ri-valutare il rischio nel modulo **MOD-01-Rischio Cyber** alla scheda **Rischio** considerando le vulnerabilità non risolte e gli impatti conseguenti ad eventuali incidenti nel modulo **MOD-01-Rischio Cyber**, nella scheda **Vulnerabilità**, nel quale provvede a:

- Rilevare la vulnerabilità riscontrata definendone la natura tra:
  - Fisica
  - Organizzativa
  - Umana
  - Tecnologica
  - Asset (Tecnica riferita ad un asset specifico)
- Riferire la vulnerabilità ad un oggetto o un elemento ispezionato ai fini della rintracciabilità
- Descrivere la funzione assolta dall'oggetto / elemento reso vulnerabile
- Riferire la vulnerabilità all'asset strategico maggiormente interessato
- Stabilire il livello della vulnerabilità

- Rivalutare il rischio considerando che l'incremento di Probabilità (che una minaccia possa colpire) possa essere causato dalla temporanea presenza della vulnerabilità
- Rivalutare il rischio a seguito del trattamento della

vulnerabilità NOTE:

L'organizzazione procede sistematicamente alla ricerca delle vulnerabilità presenti e, per facilitarne l'individuazione e la rilevazione, si avvale di un elenco strutturato presente nella scheda **Vulnerabilità** del modulo **MOD-01-Rischio Cyber** nel quale sono già predeterminati gli "elementi da ispezionare" che caratterizzano il contesto tecnico e operativo dell'organizzazione.

La rilevazione della vulnerabilità, con l'imputazione all'asset di riferimento e la determinazione del livello di vulnerabilità, nella scheda **Vulnerabilità**, modifica il rischio cyber nella scheda **Rischio**.

In assenza di vulnerabilità registrate il livello massimo della vulnerabilità registrata, nella scheda Rischio, è posto a 1 per convenzione e non altera la valutazione del rischio.

Tale livello di vulnerabilità massimo invece aumenta se sono presenti una o più vulnerabilità presso l'asset e assume, delle vulnerabilità rilevate, il valore più alto.

La probabilità nella scheda Rischio è calcolata considerando la presenza e l'entità delle vulnerabilità presenti.

Se le vulnerabilità sono assenti la Probabilità è uguale all'entità media delle minacce a cui l'asset è esposto, moltiplicato il valore 1, che non altera il risultato.

Se le vulnerabilità sono presenti la Probabilità è uguale all'entità media delle minacce a cui l'asset è esposto, moltiplicato il valore più alto delle vulnerabilità riscontrate. Il rischio quindi aumenta moltissimo, perché le minacce trovano il varco per arrecare danni.

Nonostante il rischio possa superare il valore massimo 25, restano comunque validi (e fermi) i criteri della sua valutazione stabiliti nel modulo **MOD-02-Piano di gestione rischi.**

I picchi di rischio, ovviamente, sono momentanei e inevitabili ma sono tempestivamente calmierati a seguito della rimozione della vulnerabilità.

ID.RA-06 - Controllo 1

Definire, documentare, eseguire e monitorare il piano di trattamento del rischio, nel modulo **MOD-02-Piano di gestione rischi** stabilendo:

- Le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità

- Le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione
- La descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento

ID.RA-06 - Controllo 2

L'organizzazione, in riferimento al Framework Cybersecurity Nazionale, attua i requisiti seguenti relativi ad altre Policy:

Codice del controllo previsto dal requisito	Azivalutazione di attuazione dell'organizzazione
GV.SC-05: punto 1.	Inserisce i requisiti di sicurezza nei documenti aziendali inerenti a richieste di offerta, bandi di gara, contratti, accordi e convenzioni inerenti alle forniture con potenziale impatto sulla sicurezza
ID.RA-01: punto 2.	Esegue l'analisi delle vulnerabilità degli asset prima della messa in esercizio
PR.AA-01: punto 1.	Censisce ed approva tutte le utenze utilizzate (anche quelle con privilegi) per l'accesso remoto ai sistemi informativi e alle reti
PR.DS-01: punti 1 e 2.	Prprovvede alla cifratura di dispositivi e supporti attraverso protocolli aggiornati e sicuri Disabilita l'esecuzione automatica di supporti rimovibili ed effettua la scansione prima dell'attivazione
PR.DS-02: punto 1.	Provvede alla cifratura dei dati che transitano nei sistemi informativi e nelle reti, da e verso l'esterno, attraverso protocolli aggiornati e sicuri
PR.PS-02: punti 1, 2 e 4.	Assicura di installare software e sistemi operative per i quali sono garantiti disponibilità e aggiornamenti di sicurezza Provvede ad aggiornare il software sistematicamente in relazione al piano di gestione delle vulnerabilità Verifica l'aggiornamento del software ritenuto critico in ambiente di test prima dell'effettivo impiego in ambiente operativo
DE.CM-09: punto 1.	Mantiene presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione delle postazioni terminali per il rilevamento del codice malevolo

ID.RA-06 - Controllo 3

Approvare, nel modulo **MOD-02-Piano di gestione rischi**, mediante gli organi di amministrazione e direttivi:

- Il piano di trattamento del rischio

- L'accettazione di eventuali rischi residui

Evidenze comprovanti

Ai fini della verifica di conformità alla NIS 2 e coerentemente con la codifica prevista dal Framework Nazionale Cybersecurity, l'organizzazione esibisce le seguenti evidenze che permettono di effettuare l'assessment nel modulo **MOD-00-Framework Cybersecurity** e rilevare:

- Il grado di copertura dei controlli X^A
- Il livello di maturità implementativa dei controlli Y

difica framework nazionale cybersecurity				Evidenze documentali	
Fun	**Cat**	**Sub**	**N° controllo**	**Dodocumento/scheda**	**Check**
GV	GV.OC	GV.OC-04	1	MOD-01-Rischio Cyber/Rischio	
GV	GV.RM	GV.RM-03	1	MOD-02-Piano di gestione rischi	
ID	ID.RA	ID.RA-05	1	MOD-01-Rischio Cyber/Rischio MOD-02-Piano di gestione rischi	
ID	ID.RA	ID.RA-05	2	MOD-01-Rischio Cyber/Rischio MOD-02-Piano di gestione rischi	
ID	ID.RA	ID.RA-05	3	MOD-01-Rischio cyber/Monitoraggio	
ID	ID.RA	ID.RA-05	4	MOD-01-Rischio Cyber/Vulnerabilità	
ID	ID.RA	ID.RA-06	1	MOD-02-Piano digestione rischi	
ID	ID.RA	ID.RA-06	2	Vedi altre Policy	
ID	ID.RA	ID.RA-06	3	MOD-02-Piano digestione rischi/Trattamento	

SISTEMA DI GESTIONE PER LA CYBERSECURITY - NIS 2

Policy D
Conformità e audit di sicurezza

Controllo del documento	
Rev.	1.0
Data di emissione	15.05.2026
Autore	Sibille Tschenett
Firma Autore	
Firma per approvazione	
Stato del documento	In uso ☑ Ritirato ☐

1. Scopo

L'organizzazione, per fronteggiare il rischio cyber, adotta il sistema di gestione per la cybersecurity la cui parte strutturale fondamentale è costituita da Policy.

Esse sono procedure che disciplinano l'attuazione di specifici controlli di sicurezza non elaborate arbitrariamente dall'organizzazione ma strutturate in base al Framework Nazionale Cybersecurity, che risulta un riferimento normativo cogente, nel quel sono definite "ambiti".

Lo scopo della presente policy è quello di assicurare la continuativa conformità del sistema di gestione per la cybersecurity ai contenuti prescrittivi dei controlli del Framework Nazionale da due punti di vista:

- Conformità delle Policy adottate dall'organizzazione ai contenuti prescrittivi del Framework
- Conformità dell'effettivo operato dell'organizzazione alle Policy stabilite

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
GOVERNARE - GV La strategia di gestione del rischio di cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate	**Politica (GV.PO)** La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata	**GV.PO-01** La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata
		GV.PO-02 La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione
IDENTIFICARE - ID I rischi attuali di cybersecurity dell'organizzazione sono compresi	**Miglioramento (ID.IM)** I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework	**ID.IM-01** Sono identificati miglioramenti in esito alle valutazioni

3. Attività operative e registrazioni

GV.PO-01 - Controllo 1

L'organizzazione adottata e documenta politiche di sicurezza informatica (Policy) per i seguenti "ambiti":

a) gestione del rischio
b) ruoli e responsabilità
c) affidabilità delle risorse umane
d) conformità e audit di sicurezza
e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento
f) gestione degli asset
g) gestione delle vulnerabilità
h) continuità operativa, ripristino in caso di disastro e gestione delle crisi
i) gestione dell'autenticazione, delle identità digitali e del controllo accessi
j) sicurezza fisica
k) formazione del personale e consapevolezza
l) sicurezza dei dati
m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete
n) protezione delle reti e delle comunicazioni
o) monitoraggio degli eventi di sicurezza
p) risposta agli incidenti e ripristino

Denominate "Policy" i documenti ad esse relativi, di cui il presente documento ne fa parte, riportano:

- La denominazione e lettera dell'alfabeto con cui sono identificate nel Framework Nazionale Cybersecurity alla voce "Ambiti"
- Lo scopo della Policy in relazione allo scopo più ampio del sistema di gestione
- Le funzioni, le categorie e le subcategorie del Framework a cui appartengono i controlli applicati
- La descrizione delle attività da compiere, dei controlli da attuare e dei documenti (registrazioni) con i quali creare evidenza oggettiva della conformità alla policy

L'organizzazione documenta l'adozione e il rispetto di tali policy nel modulo **MOD-05-Cybersecurity Policy**.

GV.PO-01 - Controllo 2

"Per gli ambiti di cui al punto 1 sono incluse almeno le politiche in relazione ai requisiti indicati nella tabella 1 in Appendice al presente allegato".

Il testo di questo controllo è pubblicato da un allegato al Decreto attuativo della NIS 2. Tale allegato ha la tabella 1 che riporta gli ambiti visti nel precedente controllo che vanno dalla lettera "a" alla lettera "p".

Il presente sistema di gestione include tra le proprie politiche tutti gli ambiti indicati nella tabella 1 dell'allegato in cui è documentato il controllo da attuare.

GV.PO-01 - Controllo 3

Le politiche (Policy) sono approvate dagli organi di amministrazione e direttivi, tenuto anche conto della necessità di conoscere (need to know), come comprova l'apposita sezione riservata alla gestione delle registrazioni, presente in ciascun corrispondente documento e cioè:

- Policy-A-Gestione del rischio
- Policy-B-Ruoli e responsabilità
- Policy-C-Affidabilità risorse umane
- Policy-D-Conformità e audit di sicurezza
- Ecc.

GV.PO-02 - Controllo 1

Le politiche sono riesaminate e, se opportuno, aggiornate periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Il modulo **MOD-05-Cybersecurity Policy** alla scheda **Policy** adottate riporta:

- La policy adottata dall'organizzazione
- Una breve descrizione dello scopo
- Il responsabile dell'attuazione e della conformità
- Lo score di copertura dei controlli previsti dal Framework
- Il livello di maturità implementativa dei controlli previsti dal Framework
- Il livello di priorità di intervento

Tali dati sono rilevati e forniti dal modulo **MOD-00-Framework Cybersecurity** nella sezione **Dashboard.**

GV.PO-02 - Controllo 2

Ai fini del riesame, è verificata la conformità delle politiche alla normativa in materia di sicurezza informatica. La verifica consiste nell'assicurare che ciascuna policy indicata disciplini i controlli di sicurezza da attuare, espressamente previsti come cogenti dal Framework Nazionale Cybersecurity e suddivisi per soggetti Essenziali e soggetti Importanti dalla NIS 2.

A seguito di tale verifica di conformità delle politiche alla Normativa, il riesame prosegue con:

- La valutazione di copertura dei controlli appartenenti alla specifica policy
- La valutazione di maturità implementativa di tali controlli
- La valutazione della priorità di intervento presso le policy che meritano maggior attenzione sia dal punto di vista dello score che dal punto di vista della maturità dei controlli.

GV.PO-02 - Controllo 3 [Soggetti essenziali]

L'organizzazione mantiene un registro aggiornato contenente gli esiti del riesame che è il modulo **MOD-05-Cybersecurity Policy** alla scheda **Policy.**

L'aggiornamento del registro (scheda Policy), che avviene periodicamente o a seguito di incidenti e modifiche degli elementi del contesto, prevede di registrare:

- La data del riesame
- Il responsabile che lo ha presieduto
- I relativi risultati

ID.IM-01 - Controllo 1

In accordo agli esiti del riesame, è definito, attuato, documentato e approvato dagli organi di amministrazioni e direttivi un piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza.

Il piano è documentato nel modulo **MOD-05-Cybersecurity Policy**, nella scheda **Policy** che riporta:

- I riferimenti di data, responsabile e oggetto di riesame e cioè le Policy riesaminate
- L'elenco delle Policy con la priorità di intervento

Poi, in corrispondenza di ciascuna Policy stabilita, il Piano determina:

- Gli interventi necessari da compiere (specificando i controlli sui quali intervenire)
- La scadenza
- I criteri per valutare l'efficacia degli interventi
- Il responsabile degli interventi da compiere
- L'impegno finanziario assunto dall'organizzazione (costi da sostenere per i controlli)

I criteri per valutare l'efficacia degli interventi sono obiettivi da raggiungere espressi in termini di:

- Score e cioè effettiva copertura
- Maturità e cioè livello di maturità implementativa del controllo

Si consideri che il modulo **MOD-05-Cybersecurity Policy**, nella scheda **Policy,** funziona sinergicamente con il modulo **MOD-00-Framework Cybersecurity.**

Il primo documenta gli avanzamenti che di volta in volta si registrano nel secondo, con specifico riferimento agli ambiti anziché alle funzioni e cioè gli avanzamenti di:

- Grado di copertura target
- Grado di copertura effettivo
- Livello di maturità
- Priorità

ID.IM-01 - Controllo 2

Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sugli esiti dei piani.

Tali relazioni periodiche sono documentate nel modulo **MOD-06-Relazione di adeguamento e efficacia**, nel quale l'organizzazione riporta:

- La data e il responsabile del Piano di adeguamento a cui si riferisce la relazione
- Gli interventi da compiere

- Gli interventi compiuti alla data della relazione
- L'efficacia in termini di score, maturità e priorità per ciascun intervento

ID.IM-01 - Controllo 3 [Soggetti essenziali]

È definito, attuato, aggiornato e documentato un piano per la valutazione dell'efficacia delle misure di gestione del rischio per la sicurezza informatica che comprenda l'indicazione delle misure da valutare e i relativi metodi di valutazione.

Tale piano di efficacia è integrato nello stesso Piano di adeguamento, e cioè nel modulo **MOD-05-Cybersecurity Policy** che stabilisce di valutare l'efficacia degli interventi da attuare presso le Policy in termini di score di copertura, maturità implementativa e priorità per ciascun intervento.

ID.IM-01 - Controllo 4 [Soggetti essenziali]

Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche del modulo **MOD-06-Relazione di adeguamento e efficacia** sul piano di valutazione dell'efficacia di cui al punto 3.

4. Evidenze comprovanti

Ai fini della verifica di conformità alla NIS 2 e coerentemente con la codifica prevista dal Framework Nazionale Cybersecurity, l'organizzazione esibisce le seguenti evidenze che permettono di effettuare l'assessment nel modulo **MOD-00-Framework Cybersecurity** e rilevare:

- Il grado di copertura dei controlli X^A
- Il livello di maturità implementativa dei controlli Y

Codifica framework nazionale cybersecurity				Evidenze documentali	
Fun	**Cat**	**Sub**	**N° controllo**	**Documento/scheda**	**Check**
GV	GV.PO	GV.PO-01	1	MOD-05-Cybersecurity Policy/Policy	
GV	GV.PO	GV.PO-01	2	Policy-D-Conformità e audit di sicurezza	
GV	GV.PO	GV.PO-01	3	MOD-05-Cybersecurity Policy/Policy	
GV	GV.PO	GV.PO-02	1	MOD-05-Cybersecurity Policy/Policy	
GV	GV.PO	GV.PO-02	2	Policy-D-Conformità e audit di sicurezza	
GV	GV.PO	GV.PO-02	3	MOD-05-Cybersecurity Policy/Policy	
ID	ID.IM	ID.IM-01	1	MOD-05-Cybersecurity Policy/Policy	
ID	ID.IM	ID.IM-01	2	MOD-06-Relazione di adeguamento e efficacia	
ID	ID.IM	ID.IM-01	3	MOD-05-Cybersecurity Policy/Policy	
ID	ID.IM	ID.IM-01	4	MOD-06-Relazione di adeguamento e efficacia	

SISTEMA DI GESTIONE PER LA CYBERSECURITY - NIS 2

Policy H
Continuità operativa

Controllo del documento	
Rev.	1.0
Data di emissione	15.05.2026
Autore	Sibille Tschenett
Firma Autore	
Firma per approvazione	
Stato del documento	In uso ☑ Ritirato ☐

1. Scopo

Lo scopo della Policy è quello di assicurare l'erogazione del servizio verso gli utenti anche nelle ipotesi in cui l'organizzazione dovesse subire l'effetto di fenomeni di qualunque natura che ne possano alterare il compiuto e regolare funzionamento.

La procedura impegna il personale a mantenere e a riesaminare sistematicamente tre documenti di pianificazione che corrispondono alle risposte che l'organizzazione ha prefigurato per i seguenti scenari differenti:

- Continuità operativa a seguito di compromissione parziale
- Disaster recovery a seguito di eventi disastrosi
- Gestione della crisi a seguito di episodi che intaccano oltre alla struttura anche le strategie

La procedura in pratica, a seconda del caso "patologico" vissuto dall'organizzazione, prevede un piano di azione. Il mantenimento dei piani indicati sopra è descritto nella procedura, mentre i singoli piani elaborati, costituiscono le registrazioni connesse alla procedura.

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
IDENTIFY (ID): I rischi attuali di cybersecurity dell'organizzazione sono compresi	**Miglioramento (ID.IM):** I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework	**ID.IM-04:** I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati

3. Attività operative e registrazioni

Relativamente alla gestione del rischio l'organizzazione procede, sistematicamente, a eseguire le attività riportate e attuare i seguenti controlli:

ID.IM-04 - Controllo 1

Per almeno i sistemi informativi e di rete rilevanti, quelli cioè documentati all'interno del modulo **MOD-01-Rischio Cyber**, alla scheda **Rischio,** definire, attuare, aggiornare e documentare un piano di continuità operativa nel modulo **MOD-11-Piano di continuità operativa** che comprende almeno:

- Le finalità
- L'ambito di applicazione
- I ruoli e le responsabilità
- I canali di comunicazione da impiegare per il suo funzionamento
- La priorità dei canali di comunicazione da impiegare
- Le condizioni di attivazione del piano
- Le condizioni per la disattivazione del piano
- Asset di riferimento
- Le azioni da compiere

Tale piano è concepito qualora l'organizzazione subisse una temporanea interruzione connessa a mal funzionamenti degli asset o a casi di degrado che non permettono il regolare svolgimento delle operazioni con le modalità tipiche e cioè fisiologiche.

ID.IM-04 - Controllo 2

Per i sistemi informativi e di rete rilevanti, quelli cioè documentati all'interno del modulo **MOD-01-Rischio Cyber**, alla scheda **Rischio,** definire, attuare, aggiornare e documentare un piano di ripristino in caso di disastro, nel modulo **MOD-12-Disaster recovery** che comprende:

- Finalità
- Ruoli e responsabilità
- Contatti principali e canali di comunicazione (interni ed esterni)
- Condizioni per l'attivazione e la disattivazione del piano
- Risorse necessarie, ivi compresi i backup e le ridondanze
- L'ordine di ripristino delle operazioni
- Le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino

Le procedure di ripristino per i singoli asset strategici sono documentate nel modulo:
MOD-13-Procedure di ripristino

ID.IM-04 - Controllo 3

Per i sistemi informativi e di rete rilevanti, quelli cioè documentati all'interno del modulo **MOD-01-Rischio Cyber**, alla scheda **Rischio** c'è da definire, attuare, aggiornare e documentare un piano per la gestione delle crisi, nel modulo **MOD-14-Piano gestione crisi** che comprende:

- Le finalità
- I casi di crisi
- Le responsabilità
- Le comunicazioni
- La procedura di esecuzione

ID.IM-04 - Controllo 4

L'organizzazione per i piani di cui ai punti 1, 2 e 3 e cioè i documenti:

- **MOD-11-Piano di continuità operativa**
- **MOD-12-Disaster recovery**
- **MOD-13-Procedure di ripristino**
- **MOD-14-Piano gestione crisi**

provvede all'approvazione da parte degli organi di amministrazione e direttivi.

ID.IM-04 - Controllo 5

I piani di cui ai punti 1, 2 e 3 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.

4. Evidenze comprovanti

Ai fini della verifica di conformità alla NIS 2 e coerentemente con la codifica prevista dal Framework Nazionale Cybersecurity, l'organizzazione esibisce le seguenti evidenze che permettono di effettuare l'assessment nel modulo **MOD-00-Framework Cybersecurity** e rilevare:

- II grado di copertura dei controlli X^A
- Il livello di maturità implementativa dei controlli Y

Codifica framework nazionale cybersecurity				Evidenze documentali	
Fun	**Cat**	**Sub**	**N° controllo**	**Documento/scheda**	**Check**
ID	ID.IM	ID.IM-04	1	MOD-11-Piano di continuità operativa	
ID	ID.IM	ID.IM-04	2	MOD-12-Disaster recovery MOD-13-Procedure di ripristino	
ID	ID.IM	ID.IM-04	3	MOD-14-Piano gestione crisi	
ID	ID.IM	ID.IM-04	4	MOD-11-Piano di continuità operativa MOD-12-Disaster recovery MOD-14-Piano gestione crisi	
ID	ID.IM	ID.IM-04	5	MOD-11-Piano di continuità operativa MOD-12-Disaster recovery MOD-14-Piano gestione crisi	

SISTEMA DI GESTIONE PER LA CYBERSECURITY - NIS 2

Policy L
Sicurezza dei dati

Controllo del documento	
Rev.	1.0
Data di emissione	15/05/2026
Autore	Sibille Tschenett
Firma Autore	
Firma per approvazione	
Stato del documento	In uso ☑ Ritirato ☐

1. Scopo

Lo scopo della Policy è quello proteggere i dati e le informazioni che sono presenti sugli asset operativi e in particolare sull'hardware dell'organizzazione. Per la protezione di tali dati l'organizzazione considera:

- La cifratura per impedirne l'utilizzo
- Protocolli di trasmissione sicuri per impedirne l'intercettazione e la compromissione
- Il back up sistematico e periodico per prevenirne l'indisponibilità

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
PROTECT (PR): Sono adottate misure di protezione per gestire i rischi di cybersecurity dell'organizzazione	**Sicurezza dei dati (PR.DS):** I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni	**PR.DS-01:** La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette
		PR.DS-02: La riservatezza, l'integrità e la disponibilità dei dati in transito (data-in-transit) sono protette
		PR.DS-11: I backup dei dati sono creati, protetti, mantenuti e verificati

3. Attività operative e registrazioni

Relativamente alla gestione del rischio l'organizzazione procede, sistematicamente, a eseguire le attività riportate e attuare i seguenti controlli:

PR.DS-01- Controllo 1

Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, i dati memorizzati sui dispositivi portatili, ivi inclusi laptop, smartphone e tablet, e sui supporti removibili, sono cifrati con protocolli e algoritmi allo stato dell'arte e considerati sicuri.

L'organizzazione, nel modulo **MOD-0G-Inventario** alla scheda **Hardware**, censisce tutti i dispositivi mobili e portatili. Questi dispositivi possono contenere, elaborare e trasmettere dati.

Tali dati sono protetti dalle misure indicate alla scheda Hardware e riguardano:

- La password per l'accesso al dispositivo
- La cifratura dei dati contenuti

PR.DS-01- Controllo 2

Fatte salve e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti rimovibili ed è effettuata la loro scansione al fine di rilevare codici malevoli prima che siano utilizzati nei sistemi informativi e di rete.

Tutti i dispositivi riportati alla scheda **Hardware** sono sottoposti alla scansione antivirus.

PR.DS-02- Controllo 1

Per almeno i sistemi informativi e di rete rilevanti, ivi inclusi quelli di comunicazione vocale, video e testuale, e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, sono utilizzati, per la trasmissione dei dati da e verso l'esterno del soggetto NIS, protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri.

La cifratura degli asset alla scheda **Hardware** considera algoritmi di cifratura valutati e selezionati dal personale tecnico adeguatamente formato.

PR.DS-11- Controllo 1

In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.

Nella scheda **Hardware** i dati e le informazioni contenuti nei dispositivi risultano protetti dalla sistematica e periodica esecuzione del backup.

PR.DS-11- Controllo 3 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, in accordo con la valutazione dei rischi, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.

I supporti indicati nella scheda **Hardware** includono i supporti rigidi e i server presso i quali l'organizzazione mantiene in sicurezza i dati di backup.

PR.DS-11- Controllo 4 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, in accordo con la valutazione dei rischi, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.

La misura di backup indicata nella scheda Hardware è sottoposta alla sistematica verifica del ripristino dei dati.

4. Evidenze comprovanti

Ai fini della verifica di conformità alla NIS 2 e coerentemente con la codifica prevista dal Framework Nazionale Cybersecurity, l'organizzazione esibisce le seguenti evidenze che permettono di effettuare l'assessment nel modulo **MOD-00-Framework Cybersecurity** e rilevare:

- Il grado di copertura dei controlli X^A
- Il livello di maturità implementativa dei controlli Y

Codifica framework nazionale cybersecurity				Evidenze documentali	
Fun	**Cat**	**Sub**	**N° controllo**	**Documento/scheda**	**Check**
PR	PR.DS	PR.DS-01	1	MOD-09-Inventario/Hardware	
PR	PR.DS	PR.DS-01	2	MOD-09-Inventario/Hardware	
PR	PR.DS	PR.DS-02	1	MOD-09-Inventario/Hardware	
PR	PR.DS	PR.DS-11	1	MOD-09-Inventario/Hardware	
PR	PR.DS	PR.DS-11	3	MOD-09-Inventario/Hardware	
PR	PR.DS	PR.DS-11	4	MOD-09-Inventario/Hardware	

SISTEMA DI GESTIONE PER LA CYBERSECURITY - NIS 2

Policy M
Gestione sistemi informativi e reti

Controllo del documento	
Rev.	1.0
Data di emissione	15/05/2026
Autore	Sibille Tschenett
Firma Autore	
Firma per approvazione	
Stato del documento	In uso ☑ Ritirato ☐

1. Scopo

Lo scopo della Policy è quello assicurare, attraverso la protezione degli asset e cioè la strumentazione hardware e software, il regolare funzionamento delle attività intese a fornire i servizi all'utenza.

Software e hardware rappresentano gli asset operativi grazie ai quali funzionano reti e sistemi che invece sono asset strategici.

1. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
PROTECT (PR): Sono adottate misure di protezione per gestire i rischi di cybersecurity dell'organizzazione	**Sicurezza delle piattaforme (PR.PS):** L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità	**PR.PS-01:** Sono stabilite e applicate pratiche di gestione della configurazione
		PR.PS-02: Il software è mantenuto, sostituito e rimosso in base al rischio
		PR.PS-03: L'hardware è mantenuto, sostituito e rimosso in base al rischio
		PR.PS-04: I registri di log sono generati e resi disponibili per il monitoraggio continuo
		PR.PS-06: Le pratiche di sviluppo sicuro del software sono integrate e le loro prestazioni sono monitorate durante l'intero ciclo di vita del software

2. Attività operative e registrazioni

Relativamente alla gestione del rischio l'organizzazione procede, sistematicamente, a eseguire le attività riportate e attuare i seguenti controlli:

PR.PS-01- Controllo 1 [Soggetti essenziali]

In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04 documentati nei moduli:

- **MOD-11-Piano di continuità operativa**
- **MOD-12-Disaster recovery**
- **MOD-13-Procedure di ripristino**
- **MOD-14-Piano gestione crisi**

sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.

Tali backup sono documentati nel modulo **MOD-0G-Inventario** alla scheda **Hardware** e alla scheda **Software**

PR.PS-02- Controllo 1

Fatte salve motivate e documentate ragioni normative o tecniche, in accordo agli esiti della valutazione del rischio, è installato esclusivamente software, ivi compresi i sistemi operativi, per il quale è garantita la disponibilità di aggiornamenti di sicurezza.

Nel modulo **MOD-0G-Inventario** alla scheda **Software** l'organizzazione dichiara tutto il software installato e lo riferisce, nella colonna Asset strategico associato, alla rete o al sistema informativo di riferimento principale dell'organizzazione. L'approvazione del software è subordinata alla disponibilità dei corrispondenti aggiornamenti di sicurezza.

PR.PS-02- Controllo 2

Fatte salve motivate e documentate ragioni normative o tecniche, sono installati, senza ingiustificato ritardo, gli ultimi aggiornamenti di sicurezza rilasciati dal produttore in coerenza con il piano di gestione delle vulnerabilità di cui alla misura ID.RA-08.

L'approvazione del software documentato alla scheda **Software** del modulo **MOD-0G-Inventario** è subordinata all'installazione degli ultimi aggiornamenti di sicurezza in coerenza con il piano del modulo **MOD-10-Piano gestione vulnerabilità**

PR.PS-02- Controllo 4 [Soggetti essenziali]

Fatte salve motivate e documentate ragioni normative o tecniche e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, l'aggiornamento del software ritenuto critico è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.

Nel modulo **MOD-0G-Inventario** alla scheda **Software**, l'approvazione è subordinata al test prima dell'effettivo impiego in ambiente operativo.

PR.PS-03- Controllo 1 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, sono adottate e documentate procedure per il trasferimento fisico e la dismissione di dispositivi atti alla memorizzazione di dati in modo sicuro.

L'organizzazione adotta la procedura **PRO-01-Trasferimento e dismissione sicura** che ha lo scopo di assicurare che, durante il trasferimento fisico e la dismissione di qualsiasi dispositivo di memorizzazione, i dati sensibili in esso contenuti siano resi irrecuperabili in modo permanente.

PR.PS-03- Controllo 2 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, sono mantenuti uno o più registri delle manutenzioni effettuate sull'hardware.

Le registrazioni connesse alle manutenzioni e tutte le altre operazioni/interventi che riguardano gli asset e la loro sicurezza sono documentate al modulo **MOD-16-Registro manutenzione** che documenta:

- L'identificazione dell'asset
- I dettagli dell'intervento
- L'impatto sulla sicurezza
- La responsabilità e l'approvazione

PR.PS-04- Controllo 1

Tutti gli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi sono registrati.

L'organizzazione ha installato presso i propri sistemi e le proprie reti il software di log management che prevede la rilevazione e la rintracciabilità di tutti gli eventi e cioè gli ingressi nella rete e nei sistemi, i percorsi di navigazione e le azioni compiute.

Il log management, relativamente alle applicazioni controllate, è documentato alla scheda **Software** del modulo **MOD-0G-**

Inventario PR.PS-04- Controllo 2

Per almeno i sistemi informativi e di rete rilevanti, sono acquisiti e, in modo sicuro e possibilmente centralizzato, conservati almeno i log necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto 1.

I file di log sono registrati e riportati su backup (Vedi schede **Hardware** e **Software**)

PR.PS-04- Controllo 3

In accordo agli esiti della valutazione rischio di cui alla misura ID.RA-05, sono definite e documentate le tempistiche di conservazione dei log di cui al punto 2.

I file di backup inerenti alle operazioni compiute sui software inerenti agli asset strategici sono conservati per 192 ore lavorative.

PR.PS-06- Controllo 1

Sono adottate e documentate pratiche di sviluppo sicuro del codice nello sviluppo del software.

Tali pratiche sicure sono elencate e documentate nel modulo **MOD-17-Sviluppo sicuro.**

3. Evidenze comprovanti

Ai fini della verifica di conformità alla NIS 2 e coerentemente con la codifica prevista dal Framework Nazionale Cybersecurity, l'organizzazione esibisce le seguenti evidenze che permettono di effettuare l'assessment nel modulo **MOD-00-Framework Cybersecurity** e rilevare:

- II grado di copertura dei controlli X^A
- II livello di maturità implementativa dei controlli Y

Codifica framework nazionale cybersecurity				Evidenze documentali	
Fun	**Cat**	**Sub**	**N° controllo**	**Documento/scheda**	**Check**
PR	PR.PS	PR.PS-01	1	MOD-09-Inventario/Hardware MOD-09-Inventario/Software	
PR	PR.PS	PR.PS-02	1	MOD-09-Inventario/Software	
PR	PR.PS	PR.PS-02	2	MOD-09-Inventario/Software	
PR	PR.PS	PR.PS-02	4	MOD-09-Inventario/Software	
PR	PR.PS	PR.PS-03	1	PRO-01-Trasferimento e dismissione sicura	
PR	PR.PS	PR.PS-03	2	MOD-16-Registro manutenzione	
PR	PR.PS	PR.PS-04	1	MOD-09-Inventario/Software	
PR	PR.PS	PR.PS-04	2	MOD-09-Inventario/Hardware MOD-09-Inventario/Software	
PR	PR.PS	PR.PS-04	3	Nessuno	
PR	PR.PS	PR.PS-06	1	MOD-17-Sviluppo sicuro	

SISTEMA DI GESTIONE PER LA CYBERSECURITY - NIS 2

Policy O
Monitoraggio eventi sicurezza

Controllo del documento	
Rev.	1.0
Data di emissione	15.05.2026
Autore	Sibille Tschenett
Firma Autore	
Firma per approvazione	
Stato del documento	In uso ☑ Ritirato ☐

1. Scopo

Lo scopo della Policy è quello di proteggere le reti e i sistemi da attacchi e da compromissioni attraverso un monitoraggio costante inteso a prevenire e neutralizzare gli eventi avversi. La policy stabilisce l'applicazione dei seguenti dispositivi di sicurezza spiegati nelle attività operative e nei moduli della policy:

- IPS - Intrusion Prevention System
- IDS - Intrusion Detection System
- Filtraggio posta
- SIEM (Con analisi quali-quantitativa degli eventi)
- Antivirus

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
DETECT (DE): Possibili attacchi e compromissioni di cybersecurity sono rilevati e analizzati	**Monitoraggio continuo (DE.CM):** Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi	**DE.CM-01:** Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi
		DE.CM-0G: L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi

3. Attività operative e registrazioni

Relativamente alla gestione del rischio l'organizzazione procede, sistematicamente, a eseguire le attività riportate e attuare i seguenti controlli:

DE.CM-01- Controllo 1

Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi.

Tali incidenti sono eventi che comportano l'insorgenza di vulnerabilità di natura fisica, organizzativa, tecnologica, ecc., che aumentano il rischio cyber insistente sui sistemi e sulle reti intesi come asset strategici.

La registrazione di incidenti significativi avviene mediante la registrazione delle vulnerabilità conseguenti nel modulo **MOD-01-Rischio Cyber** alla scheda **Vulnerabilità.**

DE.CM-01- Controllo 2

Sono definiti e documentati i livelli di servizio attesi (SL) dei servizi e delle attività del soggetto NIS anche ai fini di rilevare tempestivamente gli incidenti significativi.

L'organizzazione ha documentato i livelli di servizio, attesi dall'utenza, che si è impegnata a rispettare in relazione ai contratti di servizio (Agreement) nel modulo **MOD-1G-Service level agreement** per garantire il corretto funzionamento dei processi e, allo stesso tempo, per rilevare tempestivamente eventuali incidenti significativi quando tali indicatori non sono in linea con i risultati attesi.

DE.CM-01- Controllo 4 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (ivi inclusa la posta elettronica).

Nel modulo **MOD-20-Analisi e filtraggio** l'organizzazione documenta a quali asset strategici sono applicati i sistemi di:

- IPS - Intrusion Prevention System
- IDS - Intrusion Detection System
- Filtraggio posta

DE.CM-01- Controllo 5 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono monitorati gli accessi da remoto, le attività dei sistemi perimetrali (ad esempio router e firewall), gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete, ai punti terminali (endpoint) e agli applicativi al fine di rilevare gli eventi di sicurezza informatica.

Tale monitoraggio è affidato al controllo del log management, documentato nel modulo **MOD-0G-Inventario** alla scheda **Software** per il quale qualunque attività eseguita come l'accesso, il tentativo di accesso e le operazioni compiute sono rilevate, registrate grazie ai file di log il cui controllo è esercitato dall'amministratore di sistema.

L'organizzazione inoltre per il monitoraggio di tali eventi ricorre alla soluzione SIEM e cioè Security Information and Event Management documentata nel modulo **MOD-20-Analisi e filtraggio.**

DE.CM-01- Controllo 6 [Soggetti essenziali]

Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono definiti, monitorati e documentati parametri quali-quantitativi per rilevare gli accessi non autorizzati o con abuso dei privilegi concessi.

L'organizzazione ha stabilito parametri quali-quantitativi inerenti al comportamento degli utenti che accedono alle reti e ai sistemi (asset strategici) per identificare e controllare le anomalie. Tali paramenti sono documentati al modulo **MOD-20-Analisi e filtraggio.**

L'attuazione di questo controllo è strettamente legata al log management e all'utilizzo di un sistema SIEM, che raccoglie e analizza i log da tutte le fonti.

DE.CM-0G- Controllo 1

Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione dei punti terminali (endpoint) per il rilevamento del codice malevolo.

L'installazione del software antivirus è documenta nel modulo **MOD-0G-Inventario** alla scheda **Hardware**. Il controllo dell'approvazione, presente nella medesima scheda, assicura:

- L'installazione dell'antivirus
- L'aggiornamento e il mantenimento
- L'adeguata configurazione

4. Evidenze comprovanti

Ai fini della verifica di conformità alla NIS 2 e coerentemente con la codifica prevista dal Framework Nazionale Cybersecurity, l'organizzazione esibisce le seguenti evidenze che permettono di effettuare l'assessment nel modulo **MOD-00-Framework Cybersecurity** e rilevare:

- Il grado di copertura dei controlli X^A
- Il livello di maturità implementativa dei controlli Y

difica framework nazionale cybersecurity				Evidenze documentali	
Fun	**Cat**	**Sub**	**N° controllo**	**Documento/scheda**	**Check**
DE	DE.CM	DE.CM-01	1	MOD-01-Rischio Cyber/Vulnerabilità	
DE	DE.CM	DE.CM-01	2	MOD-19-Service level agreement	
DE	DE.CM	DE.CM-01	4	MOD-20-Analisi e filtraggio	
DE	DE.CM	DE.CM-01	5	MOD-09-Inventario/Software	
DE	DE.CM	DE.CM-01	6	MOD-20-Analisi e filtraggio	
DE	DE.CM	DE.CM-09	1	MOD-09-Inventario/Hardware	