Agenzia per la Cybersicurezza Nazionale

# LINEE GUIDA

## Per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90.

NOVEMBRE 2024

# Controllo di versione

| VERSIONE | DATA DI PUBBLICAZIONE | NOTE |
|---|---|---|
| 1.0 | Novembre 2024 | Prima pubblicazione. |
| 1.1 | Gennaio 2025 | Modificato “Politiche e processi relativi ai requisiti 1 e 2” con “Politiche e processi relativi ai requisiti 1, 2 e 3” a pag. 31. Corretti refusi a pag. 58 e pag. 73. |

# SOMMARIO

# Introduzione

## Premessa

La legge 28 giugno 2024, n. 90 – da qui in poi indicata come **legge** – recante "disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" mira a rafforzare la cybersicurezza nazionale e a contrastare i reati informatici, articolandosi in 24 articoli suddivisi in due Capi:

- **Capo I** (articoli 1-15): disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici.
- **Capo II** (articoli 16-24): disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari.

Tra le varie disposizioni, la legge prevede degli obblighi specifici per i soggetti individuati dall'articolo 1 comma 1 – da qui in poi indicati come **soggetti** – ossia le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali. Sono altresì comprese le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al precedente periodo ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

In particolare, per i soggetti sopra indicati la legge prevede:

- l'obbligo di segnalazione e notifica degli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105 aventi impatto su reti, sistemi informativi e servizi informatici;
- l'adozione tempestiva degli interventi risolutivi segnalati dall'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultino potenzialmente esposti;
- l'individuazione di una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provvede a quanto indicato all'articolo 8, comma 1, della legge.

Le presenti linee guida sono tese al rafforzamento della resilienza dei soggetti in coerenza con tali disposizioni, nonché con quanto previsto dalla Direttiva del Presidente del Consiglio dei ministri del 29 dicembre 2023.

# Scopo del documento

Il presente documento indirizza i soggetti verso il rafforzamento della propria resilienza tramite l'individuazione di misure di sicurezza e fornendo indicazioni per la loro implementazione nel rispetto di quanto previsto all'articolo 8, lettera f), della legge.

# Soggetti destinatari

I destinatari delle presenti linee guida sono i soggetti individuati dall'articolo 1 comma 1, della legge 28 giugno 2024, n. 90, ossia le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali. Sono altresì comprese tra i soggetti destinatari le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al precedente periodo ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

# Termini e definizioni

Ai fini del presente documento verranno usati i seguenti termini:

| TERMINE | RIFERIMENTO |
|---|---|
| Legge | Legge 28 giugno 2024, n. 90, disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. |
| Referente per la cybersicurezza | Il referente per la cybersicurezza di cui all'articolo 8, comma 2, della legge 28 giugno 2024, n. 90. |
| Soggetti | I soggetti individuati dall'articolo 1, comma 1, della legge 28 giugno 2024, n. 90. |
| Struttura | La struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90. |

# Campo di applicazione

Le misure di sicurezza del presente documento si applicano ai sistemi informativi e di rete del soggetto, ossia:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;
2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;
3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione.

# Organizzazione del documento

Il presente documento è organizzato in parti, capitoli, paragrafi e appendici.

La prima parte individua le misure di sicurezza che i soggetti adottano per il rafforzamento della propria resilienza e dedica per ogni misura un capitolo articolato nei seguenti paragrafi:

- **requisiti implementazione minima attesa**, elenca i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura;
- **descrizione**, illustra la misura evidenziandone le peculiarità ai fini della sua implementazione;
- **evidenze documentali**, elenca i contenuti che devono essere presenti nell'impianto documentale prodotto dal soggetto.

La seconda parte è dedicata alla descrizione delle modalità di implementazione raccomandate per l'attuazione delle misure, indicando, altresì, i processi di cybersecurity da istituire per corrispondere alle misure di sicurezza.

Al riguardo, si osserva che i soggetti possono implementare le misure di sicurezza secondo modalità alternative a quelle indicate, purché idonee a soddisfare le implementazioni minime attese.

Il documento contiene inoltre le seguenti appendici:

- **appendice A: implementazioni minime attese**, indica le implementazioni minime attese per l'attuazione di ogni misura di sicurezza;
- **appendice B corrispondenza ambiti misure**, riporta la mappatura tra le misure di sicurezza individuate e gli ambiti di cui all'articolo 8, comma 1, della legge 28 giugno 2024, n. 90 e alla Direttiva del Presidente del Consiglio dei ministri del 29 dicembre 2023;
- **appendice C: glossario**, elenca le definizioni dei termini peculiari usati nel documento.

All'interno del documento sono presenti riquadri di approfondimento recanti diverse tipologie di contenuto informativo secondo la seguente legenda:


Note e osservazioni.


Indicazioni ed esempi.


Definizioni dei termini peculiari usati nel documento.

Le definizioni sono riportate all'interno dei paragrafi *descrizione misura* la prima volta che viene usato uno specifico termine. I termini già definiti, eventualmente ripetuti nei paragrafi successivi, presentano un collegamento ipertestuale che rimanda alle relative definizioni presenti nel glossario.

# Impianto documentale

Il soggetto, ai fini dell'attuazione delle misure di sicurezza e dell'attestazione dell'effettiva implementazione delle stesse, deve essere in possesso o provvedere all'elaborazione di una serie di documenti – qui denominata

**Impianto documentale** – che devono trattare almeno i contenuti indicati all'interno dei paragrafi *Evidenze documentali* presenti in ogni capitolo dedicato alle misure di sicurezza.

In base al proprio contesto, il soggetto può decidere come organizzare il proprio impianto documentale, ad esempio raggruppando i contenuti in un unico documento o distribuendoli tra più documenti. L'impianto documentale può essere reso disponibile in formato cartaceo o digitale, purché facilmente fruibile da chi ha la necessità di conoscerlo e consultarlo.

Ogni documento dell'impianto documentale deve in ogni caso rispettare le seguenti caratteristiche:

- essere approvato dal vertice, o rappresentante legale, del soggetto o da una figura da lui formalmente delegata (come, ad esempio, quella del referente per la cybersicurezza), in quest'ultimo caso l'impianto documentale deve contenere la delega del vertice per l'approvazione del documento.
- riprodurre la situazione corrente ed essere aggiornato in caso di variazioni dello stato di fatto;
- essere sottoposto a revisione periodica e al verificarsi di eventi interni (come, ad esempio, l'aggiornamento di piani strategici o modifiche organizzative), eventi esterni (come l'evoluzione del conteso normativo e legislativo) o mutamenti dell'esposizione alle minacce e ai relativi rischi;
- dare evidenza della corrispondenza dei propri contenuti con quelli richiesti dai paragrafi *Evidenze documentali* di ogni capitolo dedicato alle misure di sicurezza. In tal senso è possibile, ad esempio, predisporre una tabella con la mappatura tra i paragrafi del documento redatto dal soggetto e la colonna *Contenuto documento* delle tabelle dei predetti paragrafi.

Laddove un requisito di una misura di sicurezza indichi espressamente l'esistenza di un documento recante determinati contenuti (es., "esiste un documento aggiornato che descrive le politiche di cybersecurity") significa che detti contenuti devono far parte dell'impianto documentale del soggetto e, pertanto, possono essere organizzati in uno o anche più documenti.

## Norme di riferimento

| TERMINE | RIFERIMENTO |
|---|---|
| Legge 28 giugno 2024, n. 90. | Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. |
| Direttiva del Presidente del Consiglio dei Ministri 29 dicembre 2023. | Resilienza cibernetica del Paese - Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici. |
| Decreto-legge 21 settembre 2019, n. 105 | Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica. |
| Decreto legislativo 18 maggio 2018, n. 65 | Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. |

# Il referente per la cybersicurezza

L'articolo 8 della legge prevede l'individuazione di una struttura – da qui in poi indicata come **struttura** – che provvede a:

a) lo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;

b) la produzione e l'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;

c) la produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

d) la produzione e l'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;

e) la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);

f) la pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;

g) il monitoraggio e la valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Presso la struttura opera il **referente per la cybersicurezza** che deve essere individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

Le disposizioni dell'articolo 8 della legge non si applicano ai soggetti di cui all'articolo 1, comma 2-bis, del decreto-legge 105, ai quali continuano ad applicarsi gli obblighi previsti dalla richiamata disciplina, e agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124.

# Parte I: Misure di sicurezza

## per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90

**Sinossi**

In questa parte sono elencate le misure di sicurezza che i soggetti adottano per il rafforzamento della propria resilienza. Per ogni misura è presente un capitolo in cui sono indicati i requisiti per l'implementazione minima, la descrizione della misura e le evidenze documentali che devono essere presenti nell'impianto documentale prodotto dal soggetto.

# Elenco delle misure di sicurezza

Le misure di sicurezza per il rafforzamento della resilienza dei soggetti sono di seguito riportate e rappresentano un insieme di misure di base che devono essere adottate da tutti i soggetti.

| CODICE | DESCRIZIONE |
|---|---|
| ID.AM-1 | Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione. |
| ID.AM-2 | Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione. |
| ID.AM-3 | I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati. |
| ID.AM-6 | Sono definiti e resi noti ruoli e responsabilità inerenti alla cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner). |
| ID.GV-1 | È identificata e resa nota una policy di cybersecurity. |
| ID.GV-4 | La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity. |
| ID.RA-1 | Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate. |
| ID.RA-5 | Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio. |
| ID.RA-6 | Sono identificate e prioritizzate le risposte al rischio. |
| ID.SC-2 | I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber. |
| PR.AC-1 | Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit sicurezza. |
| PR.AC-3 | L'accesso remoto alle risorse è amministrato. |
| PR.AC-4 | I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni. |
| PR.AT-1 | Tutti gli utenti sono informati e addestrati. |
| PR.AT-2 | Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità. |
| PR.DS-1 | I dati memorizzati sono protetti. |
| PR.IP-4 | I backup delle informazioni sono eseguiti, amministrati e verificati. |
| PR.IP-9 | Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro. |
| PR.IP-12 | Viene sviluppato e implementato un piano di gestione delle vulnerabilità. |
| PR.MA-1 | La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati. |

| CODICE | DESCRIZIONE |
|---|---|
| PR.PT-4 | Le reti di comunicazione e controllo sono protette. |
| DE.CM-1 | Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity. |
| DE.CM-4 | Il codice malevolo viene rilevato. |
| RS.RP-1 | Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente. |
| RS.AN-5 | Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza). |
| RC.RP-1 | Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity. |

Resta in capo a ciascun soggetto la valutazione, in esito alla differente esposizione alle minacce e alla propria analisi del rischio, in merito all'individuazione e conseguente adozione di ulteriori misure di sicurezza per il rafforzamento della propria resilienza.

L'adozione delle misure di sicurezza non esenta i soggetti dagli adempimenti derivanti dalle ulteriori normative in materia di cybersicurezza come, ad esempio, quelle relative al decreto-legge 21 settembre 2019, n. 105 (Perimetro di Sicurezza Nazionale Cibernetica) o al decreto legislativo 18 maggio 2018, n. 65 (direttiva NIS).

Le misure di sicurezza sono organizzate nelle funzioni, categorie e sottocategorie del Framework Nazionale per la Cybersecurity e la Data Protection (FNCS). In particolare, ogni misura è identificata da un codice univoco del tipo **XX.YY-N,** dove **XX** rappresenta la funzione, **YY** la categoria ed **N** la sottocategoria del FNCS.

Il Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) è uno strumento di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. L'elemento principale è il cosiddetto *Framework Core* strutturato in funzioni, categorie e sottocategorie (https://www.cybersecurityframework.it/framework2).

Per ogni misura sono indicate in Appendice A le implementazioni minime attese che i soggetti devono garantire per la conformità alle misure.

Le misure di sicurezza sono state definite in coerenza con gli ambiti individuati dall'articolo 8, comma 1, della legge 28 giugno 2024, n. 90 e dalla Direttiva del Presidente del Consiglio dei ministri 29 dicembre 2023 *Resilienza cibernetica del Paese - Protocolli di intesa per irrobustire la capacità di risposta agli incidenti informatici*.

In Appendice B è riportata la corrispondenza delle misure di sicurezza con tali ambiti.

Si noti che nella precedente tabella, nonché in Appendice A, le misure di sicurezza sono elencate secondo un ordine coerente con quello delle relative sottocategorie del FNCS.

Nei prossimi paragrafi, nonché nella **parte II** dedicata alle modalità di implementazione, invece, l'ordine con il quale sono riportate le misure di sicurezza indica una possibile roadmap di implementazione.

# ID.AM-6

Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner).

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | È definita e resa nota alle articolazioni del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti. |
| 2 | All'interno dell'organizzazione di cui al punto 1, è istituita e resa nota alle articolazioni del soggetto la struttura di cui all'articolo 8, comma 1, della Legge 28 giugno 2024, n. 90 e sono assegnati, nell'ambito di tale struttura, ruoli e responsabilità per almeno le attività indicate nel medesimo comma. |
| 3 | È nominato, nell'ambito della struttura di cui al punto 2, il referente per la cybersicurezza di cui all'articolo 8, comma 2, della Legge 28 giugno 2024, n. 90, in possesso di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. |
| 4 | Sono comunicati all'Agenzia per la cybersicurezza nazionale il nominativo e gli estremi di contatto del referente di cui al punto 3 secondo le modalità rese note attraverso il sito dell'Agenzia per la cybersicurezza nazionale. |
| 5 | Esiste un elenco del personale interno ed esterno dell'organizzazione di cui al punto 1, ivi incluso quello della struttura di cui al punto 2, avente specifici ruoli e responsabilità. |

## Descrizione

La misura richiede di definire e rendere nota alle articolazioni del soggetto l'**organizzazione di cybersecurity** e di assegnare i ruoli e le responsabilità per tutto il personale e per eventuali **terze parti** comprese nell'organizzazione.

L'**organizzazione di cybersecurity** è l'insieme delle articolazioni preposte al **governo** (o *governance*) e alla gestione della sicurezza dei sistemi informativi e di rete del soggetto. Questa comprende, altresì, le articolazioni di eventuali terze parti coinvolte nelle attività di cybersecurity.

Le **terze parti** sono gli operatori pubblici e/o privati diversi dal soggetto caratterizzati da una dipendenza esterna con il soggetto, come ad esempio i fornitori di beni e servizi informatici.

Le **articolazioni del soggetto** sono le unità organizzative del soggetto che compongono la struttura gerarchica dell'organigramma del soggetto (quali ad esempio, dipartimenti, direzioni generali, uffici, unità, ecc.).

La *governance* o governo guida e indirizza l'approccio alla cybersecurity dell'organizzazione definendo, ad esempio, piani strategici in linea con gli obiettivi dell'organizzazione in termini di sicurezza dei propri sistemi informativi e di rete.

All'interno dell'organizzazione di cybersecurity deve essere poi individuata e resa nota alle articolazioni del soggetto la **struttura** che provvede almeno alle attività indicate all'articolo 8, comma 1 della legge ed assegnati i ruoli e le responsabilità per tali attività.

Tra i ruoli e le responsabilità da assegnare – anche in accordo a quanto previsto dalle misure ID.AM-1, ID.AM-2, ID.AM-3 e PR.AC-4 – devono essere previsti, tra gli altri, quelli concernenti, rispettivamente, l'approvazione di: sistemi e apparati fisici che accedono alla rete, piattaforme e applicazioni software che sono installate, flussi informativi, credenziali con privilegi.

Nell'ambito di questa struttura, deve essere quindi individuato il **referente per la cybersicurezza**, il cui nominativo ed estremi di contatto sono comunicati all'Agenzia per la cybersicurezza nazionale secondo le modalità indicate sul sito dell'Agenzia.

La struttura e il referente di cui ai commi 1 e 2 possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione al digitale previsti dall'articolo 17 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.

[*v. articolo 8, comma 3, della legge*].

La misura richiede infine, con riferimento all'organizzazione di cui al precedente punto 1, inclusa la struttura di cui al precedente punto 2, di redigere l'elenco del personale interno ed esterno avente specifici ruoli e responsabilità.

La **specificità** dei ruoli e delle responsabilità del personale da censire è definita dal soggetto in linea con il proprio contesto tecnico-organizzativo.

Il personale esterno è quello di non diretta dipendenza del soggetto ma che risulta impiegato per le attività di cybersecurity del soggetto tramite le terze parti.

Si consideri, ad esempio, il caso in cui un soggetto abbia affidato la gestione operativa di un sistema informativo e di rete, o di una sua porzione, a un fornitore esterno e che quest'ultimo abbia affidato la responsabilità delle diverse attività (come, per esempio, il processo di patch management, il monitoraggio degli eventi di sicurezza o la risposta agli incidenti) a più gruppi. In tale contesto il soggetto dovrebbe individuare le figure del fornitore che rivestono specifici ruoli e responsabilità, quali, ad esempio, il responsabile principale dell'erogazione del servizio verso il soggetto e i responsabili dei citati gruppi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Descrizione dell'organizzazione di cybersecurity comprensiva di ruoli e responsabilità per tutto il personale e per le eventuali terze parti dell'organizzazione, nonché delle modalità di comunicazione dell'organizzazione alle articolazioni del soggetto. | 1 |
| Descrizione della struttura di cui all'articolo 8, comma 1, della legge comprensiva di ruoli e responsabilità per le attività previste dal medesimo comma, nonché delle modalità di comunicazione della struttura alle articolazioni del soggetto. | 2 |
| Nomina del referente per la cybersicurezza firmata dal rappresentante legale del soggetto o da persona da lui delegata e indicazione delle professionalità e competenze. | 3 |
| Attestazione della comunicazione all'Agenzia per la cybersicurezza nazionale del nominativo e degli estremi di contatto del referente per la cybersicurezza. | 4 |
| Elenco del personale interno ed esterno dell'organizzazione di cui al punto 1, ivi incluso quello della struttura di cui al punto 2, avente specifici ruoli e responsabilità. | 5 |

# ID.GV-1

È identificata e resa nota una policy di cybersecurity.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Le politiche e i processi di cybersecurity sono definiti per almeno i seguenti ambiti:<br>a) governo;<br>b) gestione del rischio;<br>c) gestione degli asset;<br>d) gestione del rischio di cybersecurity della catena di approvvigionamento;<br>e) gestione delle vulnerabilità;<br>f) business continuity e disaster recovery;<br>g) gestione delle identità digitali e del controllo accessi;<br>h) sicurezza dei dati;<br>i) manutenzione e riparazione dei sistemi;<br>j) protezione delle reti;<br>k) monitoraggio degli eventi di sicurezza;<br>l) risposta e ripristino agli incidenti;<br>m) formazione del personale. |
| 2 | Esiste un documento aggiornato che descrive le politiche di cybersecurity di cui al punto 1. |
| 3 | Esiste un documento aggiornato che descrive i processi di cybersecurity di cui al punto 1. |
| 4 | Le politiche e i processi di cui al punto 1 sono revisionati periodicamente e quando necessario. |
| 5 | Esiste un piano programmatico aggiornato per la sicurezza di dati, sistemi e infrastrutture in accordo alle politiche di cui al punto 1. |

## Descrizione

La misura richiede di definire e documentare le **politiche** e i **processi di cybersecurity** per almeno gli ambiti indicati al punto 1 lettere da a) a m) del paragrafo *requisiti implementazione minima* attesa della presente misura.

La misura richiede inoltre di revisionare periodicamente e *quando necessario* le politiche e i processi di cybersecurity e di redigere e, conseguentemente, mantenere aggiornati i documenti che li descrivono.



*Quando necessario* significa, ad esempio, al verificarsi di eventi interni (come l'aggiornamento di piani strategici o modifiche organizzative), eventi esterni (come l'evoluzione del conteso normativo e legislativo) o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Le **politiche di cybersecurity** sono l'insieme di regole e disposizioni definite da un'organizzazione, e approvate dai vertici, per salvaguardare la sicurezza dei propri sistemi informativi e di rete. Le politiche guidano le decisioni e sono attuate tramite processi, procedure, standard e linee guida definiti in accordo e nel rispetto delle politiche.

I **processi di cybersecurity** sono le fasi e attività relazionate tra loro ed eseguite per raggiungere specifici obiettivi in un determinato ambito della cybersecurity, come ad esempio la risposta agli incidenti, la sicurezza dei dati e la gestione delle vulnerabilità.

La misura richiede infine di predisporre un **piano programmatico per la sicurezza di dati, sistemi e infrastrutture** definito in accordo alle politiche di cybersecurity.

Il **piano programmatico per la sicurezza di dati, sistemi e infrastrutture** è un documento che esplicita le linee strategiche, gli obiettivi prefissati e le conseguenti attività da porre in essere in merito alla sicurezza di dati, sistemi e infrastrutture.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche di cybersecurity per almeno gli ambiti indicati al punto 1 della presente misura. | 1, 2 |
| Processi di cybersecurity per almeno gli ambiti indicati al punto 1 della presente misura. | 1, 3 |
| Modalità di revisione delle politiche e dei processi di cybersecurity. | 4 |
| Piano programmatico per la sicurezza di dati, sistemi e infrastrutture. | 5 |

# ID.GV-4

La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Esiste un piano aggiornato per la gestione del rischio informatico. |

## Descrizione

La misura richiede di definire un piano per la gestione del rischio informatico.

Il **piano per la gestione del rischio informatico** è il documento comprensivo di linee di indirizzo, obiettivi e conseguenti azioni, definito dal soggetto per identificare, valutare e trattare il rischio informatico.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Piano per la gestione del rischio informatico. | 1 |

# ID.AM-1

Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | DESCRIZIONE |
|---|---|
| 1 | Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90. |
| 2 | L'accesso alla rete è consentito esclusivamente ai soli sistemi e apparati fisici approvati. |

## Descrizione

La misura richiede di redigere e mantenere aggiornato l'inventario dei sistemi e degli apparati fisici e di permettere l'accesso alla rete esclusivamente a quelli autorizzati da attori incardinati presso la struttura.

I ruoli e le responsabilità degli attori interni alla struttura deputati all'approvazione sono definiti nell'ambito della misura ID.AM-6.

L'inventario dei sistemi e degli apparati fisici è essenziale ai fini dell'adozione e attuazione delle varie misure di sicurezza: senza avere, ad esempio, contezza degli apparati perimetrali presenti sulla rete, il soggetto non sarà in grado di determinare l'impatto di un'eventuale vulnerabilità su un determinato modello di firewall e le conseguenti attività da porre in essere.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Inventario dei sistemi e degli apparati fisici comprensivo di quelli che hanno accesso alla rete e della relativa autorizzazione. | 1, 2 |

# ID.AM-2

Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90. |
| 2 | L'installazione è consentita esclusivamente alle piattaforme e applicazioni software approvate. |

## Descrizione

La misura richiede di redigere e mantenere aggiornato l'inventario delle piattaforme e delle applicazioni software e di permettere l'accesso alla rete esclusivamente a quelle autorizzate da attori incardinati presso la struttura.

I ruoli e le responsabilità degli attori interni alla struttura deputati all'approvazione sono definiti nell'ambito della misura ID.AM-6.

L'inventario delle piattaforme e applicazioni software è essenziale ai fini dell'adozione e attuazione delle varie misure di sicurezza: senza avere, ad esempio, contezza delle piattaforme applicative installate, il soggetto non sarà in grado di determinare l'impatto di un'eventuale vulnerabilità di una determinata piattaforma applicativa e le conseguenti attività da porre in essere.

Esempi di piattaforme e applicazioni software sono i sistemi operativi, i programmi di *office automation*, i *database*, i software commerciali e quelli sviluppati internamente, ecc.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Inventario delle piattaforme e applicazioni software comprensivo di quelle installate e della relativa autorizzazione. | 1, 2 |

# ID.AM-3

I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Tutti i flussi informativi tra i sistemi informativi e di rete del soggetto e l'esterno sono identificati ed esiste un elenco di quelli approvati da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90. |
| 2 | Le comunicazioni sono consentite esclusivamente per i flussi informativi approvati. |

## Descrizione

La misura richiede di redigere e mantenere un inventario dei flussi informativi tra i sistemi informativi e di rete del soggetto e l'esterno e di permettere le comunicazioni esclusivamente per i flussi autorizzati da attori incardinati presso la struttura.

I ruoli e le responsabilità degli attori interni alla struttura deputati all'approvazione sono definiti nell'ambito della misura ID.AM-6.

I **flussi informativi** sono l'insieme di dati scambiati in una rete tra una sorgente e un destinatario. Possono essere rappresentati tramite le connessioni, in ingresso o in uscita, e/o i protocolli tramite i quali avvengono le comunicazioni.

Ad esempio, il flusso informativo conseguente alla navigazione sul Web è rappresentato da una connessione in uscita su protocollo HTTPS, mentre il flusso informativo conseguente alla ricezione di mail è rappresentato da un flusso in ingresso su protocollo SMTP.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Inventario dei flussi informativi comprensivo di quelli approvati e della relativa autorizzazione. | 1, 2 |

# ID.SC-2

I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Esiste un elenco aggiornato dei fornitori e partner terzi affidatari di forniture di beni, sistemi e servizi di information and communication technology (ICT). |

## Descrizione

La misura richiede di redigere e mantenere un inventario dei fornitori e partner terzi di beni, sistemi e servizi ICT.

La **catena di approvvigionamento** (o *supply chain*) è l'insieme di individui, organizzazioni, risorse e attività coinvolte nella creazione e fornitura di un prodotto o un servizio.

La protezione della catena di approvvigionamento assume un ruolo cruciale per la resilienza: un incidente che occorre su un singolo elemento della filiera (ad esempio un fornitore software) può infatti ripercuotersi e compromettere l'intera catena.

In considerazione di ciò e della necessità di mitigare i rischi derivanti dalla catena di approvvigionamento, la misura ID.GV-1 prevede che siano definite politiche in tale ambito.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Inventario dei fornitori e partner terzi di sistemi informatici, componenti e servizi. | 1 |

# ID.RA-5

Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4, esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno:<br>a) l'identificazione del rischio;<br>b) l'analisi del rischio;<br>c) la ponderazione del rischio. |
| 2 | La valutazione del rischio di cui al punto 1 è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti. |

## Descrizione

La misura richiede di eseguire, in accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4, il processo di valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete del soggetto, documentandone gli esiti, prevedendo almeno le fasi di identificazione, analisi e ponderazione del rischio e considerando le minacce interne ed esterne, le vulnerabilità, le relative probabilità di accadimento e i conseguenti impatti.

In coerenza con quanto indicato per la misura ID.GV-4, la *valutazione del rischio* è una fase del processo di gestione del rischio che prevede le seguenti fasi: *identificazione del rischio* (i rischi sono identificati in termini di minacce e vulnerabilità), *analisi del rischio* (il livello di rischio è calcolato come combinazione degli impatti e delle probabilità di accadimento) e *ponderazione del rischio* (il livello di rischio è confrontato con i criteri di rischio per determinare se è accettabile o tollerabile).

La *valutazione del rischio* deve essere condotta periodicamente sui sistemi informativi e di rete del soggetto.

In accordo a quanto previsto dal punto 1 della misura ID.RA-1, dal punto 2 della misura PR.AC-1, dai punti 1 e 2 della misura PR.AC-3, dal punto 1 della misura PR.DS-1, dai punti 1, 2 e 3 della misura PR.IP-4, dai punti 1 e 2 della misura PR.MA-1, dal punto 1 della misura PR.PT-4, dai punti 1 e 2 della misura DE.CM-1 e dal punto 2 della misura DE.CM-4, gli esiti dell'analisi del rischio sono utilizzati per determinare le politiche e le misure di sicurezza in relazione ai medesimi punti.

# Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Esiti della valutazione del rischio in accordo ai requisiti indicati. | 1, 2 |

# ID.RA-6

Sono identificate e prioritizzate le risposte al rischio.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorità. |
| 2 | Per il rischio residuo successivo al trattamento di cui al punto precedente, esiste un documento aggiornato che ne contiene la chiara descrizione. Il documento, con il quale si accetta il rischio residuo, è approvato da parte dei vertici del soggetto. |

## Descrizione

La misura richiede di definire e documentare le scelte effettuate per trattare i rischi individuati a seguito dalla fase di valutazione del rischio e quali sono le relative priorità.

La fase di trattamento del rischio è la fase del processo di gestione del rischio successiva alla valutazione del rischio ed è effettuata sulla base del confronto del rischio determinato con l'analisi del rischio con i criteri di accettazione del rischio.

Le possibili scelte in termini di trattamento del rischio sono: mitigare il rischio (ad esempio tramite l'implementazione di misure di sicurezza che hanno come obiettivo ridurre la probabilità di accadimento), condividere il rischio (ad esempio tramite assicurazioni), evitare il rischio, accettare il rischio.

La misura richiede inoltre che il rischio residuo, ovvero quello risultante dopo il trattamento del rischio, sia descritto e accettato dai vertici del soggetto.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Descrizione degli interventi di trattamento del rischio con indicazione delle priorità. | 1 |
| Descrizione del rischio accettato e relativa approvazione da parte dei vertici del soggetto. | 2 |

# ID.RA-1

Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, esiste un piano aggiornato che descrive l'insieme delle attività finalizzate all'identificazione delle vulnerabilità contenente almeno:<br>a) le modalità per l'identificazione delle vulnerabilità;<br>b) la pianificazione delle attività per l'identificazione delle vulnerabilità. |
| 2 | Sono eseguite periodicamente le attività per identificare le vulnerabilità di cui al punto 1 e predisposte apposite relazioni che contengono almeno:<br>a) la descrizione generale delle attività effettuate e gli esiti delle stesse;<br>b) la descrizione delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza. |

## Descrizione misura

La misura richiede di definire – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – un piano delle attività volte a individuare le vulnerabilità dei sistemi informativi e di rete descrivendo almeno le modalità con le quali sono individuate le vulnerabilità e la pianificazione delle relative attività.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di sistema informativo e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che presentano rischi maggiori in termini di esposizione alle vulnerabilità e alle minacce (si pensi ad esempio ai sistemi esposti su Internet come i *web server*) per i quali dovranno essere adottate politiche specifiche in termini, ad esempio, di installazione degli aggiornamenti software.

La misura richiede inoltre di eseguire periodicamente le attività di individuazione delle vulnerabilità e di predisporre, agli esiti delle attività, apposite relazioni che contengono almeno i seguenti elementi: descrizione e risultati delle attività, descrizione delle vulnerabilità rilevate e conseguente livello di impatto sulla sicurezza dei sistemi informativi e di rete.

Esempi di attività volte a individuare vulnerabilità sono i Vulnerability Assessment (VA) e i Penetretion Test (PT): i VA effettuano una ricognizione delle vulnerabilità (già note) di un sistema, i PT simulano un attacco informatico e provano a sfruttare le vulnerabilità individuate.

# Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Piano aggiornato delle attività volte a identificare le vulnerabilità contenente almeno le modalità per l'identificazione delle vulnerabilità e la pianificazione delle relative attività | 1 |
| Relazioni periodiche contenenti almeno la descrizione delle attività effettuate e relativi esiti, la descrizione delle vulnerabilità rilevate e relativo livello di impatto sulla sicurezza. | 2 |

# PR.IP-12

Viene sviluppato e implementato un piano di gestione delle vulnerabilità.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Le vulnerabilità emerse a seguito delle attività di cui al punto 2 della misura ID.RA-1 sono prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero accentando il rischio in accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4. |
| 2 | Le specifiche vulnerabilità segnalate puntualmente dall'Agenzia per la cybersicurezza nazionale sono risolte, senza ritardo e comunque non oltre quindici giorni dalla segnalazione, adottando gli interventi indicati dalla stessa Agenzia. Qualora dovessero sussistere motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione, o comportino il differimento oltre il termine indicato degli interventi, viene data tempestiva comunicazione all'Agenzia. |
| 3 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2. |
| 4 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2. |
| 5 | In relazione alla gestione delle vulnerabilità, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di risolvere le vulnerabilità identificate a seguito delle attività di cui al punto 2 della misura ID.RA-1, applicando gli aggiornamenti di sicurezza, facendo ricorso a misure di mitigazione ove disponibili o accettando il rischio in accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4.

Quando non è possibile eliminare una vulnerabilità (ad esempio, tramite *patching*) è necessario adottare opportune misure di mitigazione, che hanno l'obiettivo di prevenire o limitare i casi di sfruttamento della vulnerabilità o ridurne l'impatto. Il caso tipico è, ad esempio, quello di una vulnerabilità nota di un determinato prodotto per la quale non è stata ancora rilasciata una *patch* da parte del fornitore.

La misura richiede inoltre di risolvere le vulnerabilità segnalate dall'Agenzia per la cybersicurezza nazionale adottando gli interventi indicati dalla stessa Agenzia senza ritardo e comunque non oltre quindici giorni dalla segnalazione.

Qualora dovessero sussistere motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione, o comportino il differimento oltre il termine indicato degli interventi risoluti indicati dall'Agenzia per la cybersicurezza nazionale, il soggetto deve darne tempestiva comunicazione all'Agenzia.

La mancata adozione degli interventi risoluti, salvo quanto sopra indicato, comporta l'applicazione delle sanzioni di cui all'articolo 1, comma 6, della legge.

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di definire e documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione alla gestione delle vulnerabilità dei sistemi informativi e di rete.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1 e 2. | 1, 2, 3, 4 |
| Procedure, metodologie e tecnologie relative alla gestione delle vulnerabilità dei sistemi informativi e di rete. | 1, 2, 5 |

# RS.AN-5

Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza).

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In relazione alla gestione delle informazioni inerenti le vulnerabilità provenienti dal CSIRT Italia, nonché da eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento, esiste un documento aggiornato contenente almeno:<br>a) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni con particolare riferimento alle segnalazioni dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità a cui i soggetti risultano potenzialmente esposti di cui all'articolo 2 della legge 28 giugno 2024, n. 90;<br>b) le procedure, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui alla lettera a) nel rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di redigere e mantenere aggiornato un **piano** in relazione alla gestione delle informazioni inerenti le vulnerabilità provenienti dal CSIRT Italia, nonché da eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento.

Gli ISAC sono centri di raccolta e condivisione delle informazioni relative alla cybersecurity. Gli ISAC di riferimento trattano le informazioni relative a specifici settori come ad esempio quello sanitario, energetico, finanziario, ecc.

L'Agenzia per la cybersicurezza nazionale promuove la creazione di una rete nazionale di ISAC settoriali integrati con ISAC Italia (ISAC istituito presso l'Agenzia), così da favorire il potenziamento dello scambio informativo e di best practice a servizio della Pubblica Amministrazione e dell'industria nazionale.

Per approfondimenti è possibile consultare la pagina web https://www.acn.gov.it/portale/isac-italia.

Il **piano** deve contenere almeno i seguenti elementi:

- le modalità previste per monitorare, ricevere, analizzare e rispondere alle informazioni e in particolare alle segnalazioni con particolare riferimento alle segnalazioni dell'Agenzia per la cybersicurezza nazionale sulle specifiche vulnerabilità alle quali si è potenzialmente esposti;
- le procedure, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività sopra indicate nel rispetto delle politiche di cybersecurity e nell'ambito dei processi di cui alla misura ID.GV-1.

# Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Piano di gestione delle informazioni inerenti le vulnerabilità | 1 |

# PR.IP-9

Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Esistono piani aggiornati di continuità operativa/disaster recovery redatti in accordo alle relative politiche e ai relativi processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di redigere e mantenere aggiornati i piani di continuità operativa e disaster recovery.

Il piano di **continuità operativa** descrive i processi e le procedure che un'organizzazione adotta per continuare a svolgere le proprie attività durante il verificarsi di un disastro.

Il piano di **disaster recovery**, generalmente parte integrante del piano di continuità operativa, descrive i processi e le procedure che un'organizzazione adotta per ripristinare i sistemi informativi e di rete nel caso in cui si verifichi un disastro.

Due parametri tipicamente considerati nell'ambito del disaster recovery (o ripristino da un disastro) sono RPO e RTO.

**RTO** (Recovery Time Object): intervallo di tempo che intercorre tra il verificarsi di un evento di disastro e il completo ripristino dell'operatività dei sistemi informativi e di rete.

**RPO** (Recovery Point Object), intervallo di tempo che intercorre tra quando il dato viene generato e quando può essere recuperato con successo (ovvero il tempo trascorso dall'ultimo backup disponibile), indica la quantità massima di dati che si possono perdere a seguito di un evento imprevisto.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Piano di continuità operativa | 1 |
| Piano di disaster recovery | 1 |

# PR.AC-1

Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Salvo motivate e documentate ragioni di natura organizzativa o tecnica, le identità digitali sono individuali per gli utenti. |
| 2 | Le credenziali di accesso relative alle identità digitali sono robuste e aggiornate con una cadenza proporzionata ai privilegi dell'utenza. |
| 3 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono verificate periodicamente le identità digitali e le credenziali di accesso, aggiornandole/revocandole in caso di variazioni (es. trasferimento o cessazione di personale). |
| 4 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3. |
| 5 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3. |
| 6 | In relazione all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso degli utenti, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di assegnare identità digitali individuali agli utenti e di motivare e documentare eventuali ragioni di natura organizzativa o tecnica per le quali non possa essere garantito tale requisito.

L'**identità digitale** è l'insieme di dati e informazioni che identificano univocamente un'entità (persone, sistemi e servizi informatici, ecc.).

Per accedere a un sistema, l'identità digitale deve essere prima *autenticata* (verifica dell'identità) e poi *autorizzata* (assegnazione del livello di accesso alle risorse informatiche).

Le identità digitali hanno quindi associate *credenziali di accesso* (costituite, ad esempio, da username e password, certificati digitali, ecc.) per l'autenticazione e *utenze* (o *account*) per l'autorizzazione.

La misura richiede inoltre che le credenziali di accesso, quali password, siano robuste e aggiornate con cadenza proporzionata alla tipologia di utenza (ad esempio le credenziali relative a utenze con privilegi sono aggiornate con cadenza superiore rispetto alle credenziali relative a utenze senza privilegi).

La robustezza di una password misura l'efficacia di una password contro attacchi come quelli a *dizionario* (un tipo di attacco in cui l'avversario prova a individuare la password usando elenchi di frasi comuni) o *brute-force* (nel quale l'attaccante prova a individuare la password provando tutte le possibili combinazioni).

Le utenze associate alle identità digitali possono essere distinte in utenze con privilegi e utenze senza privilegi (o *standard*). Le utenze con privilegi hanno livelli di accesso alle risorse informatiche superiori rispetto a quelle standard. Esempi di utenze con privilegi sono quelle relative agli amministratori dei sistemi operativi, agli amministratori di database, agli utenti con privilegi applicativi, agli utenti in grado di creare/cancellare e profilare altri utenti.

La misura richiede inoltre – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di verificare periodicamente le identità digitali e le credenziali di accesso e aggiornarle o revocarle in caso di variazioni.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda, ad esempio, della tipologia di credenziale. Tipicamente utenze con privilegi presentano rischi maggiori rispetto a quelle senza privilegi e verranno di conseguenza verificate con frequenza maggiore.

*Verifica periodica delle identità digitali e delle credenziali di accesso* significa accertarsi che le identità digitali esistenti siano necessarie ed effettivamente in uso. Non devono essere quindi presenti, ad esempio, identità associate a personale non più in servizio o a sistemi e servizi informatici dismessi.

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di definire e documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso degli utenti.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi all'*amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso agli utenti* (tipicamente compresi nell'ambito della *gestione delle identità digitali e del controllo accessi*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1, 2 e 3. | 1, 2, 3, 4, 5 |
| Procedure, metodologie e tecnologie relative all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso degli utenti. | 1, 2,3, 6 |

# PR.AC-3

L'accesso remoto alle risorse è amministrato.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono monitorati gli accessi da remoto ed esiste un log degli accessi da remoto eseguiti. |
| 2 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono definite le attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso. |
| 3 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2. |
| 4 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2. |
| 5 | In relazione alla gestione degli accessi da remoto, esiste un documento aggiornato contenente almeno:<br>a) l'elenco dei sistemi informativi e di rete ai quali è possibile accedere e le relative modalità;<br>b) le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di monitorare gli accessi da remoto tenendo traccia degli accessi eseguiti, definire quali sono le attività consentite da remoto e implementare adeguate misure di sicurezza per l'accesso.

Gli accessi effettuati da remoto sono quelli effettuati dagli utenti tramite una rete esterna a quella in cui si trovano i sistemi informativi e di rete del soggetto. Esempi di accesso remoto sono quelli effettuati per fornire assistenza o per le attività lavorative a distanza (*smart working*).

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda, ad esempio, della tipologia di sistema informativo e di rete al quale si accede da remoto. Verosimilmente saranno presenti sistemi informativi e di rete per i quali l'accesso remoto presenta rischi elevati (si pensi ad esempio alla console di management di un firewall), di conseguenza si adotteranno politiche e misure di sicurezza proporzionate al livello di rischio (ad esempio accesso con autenticazione multi-fattore, notifica degli accessi eseguiti, ecc.).

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di definire e documentare:

- l'elenco dei sistemi informativi e di rete ai quali è possibile accedere e le relative modalità di accesso;
- le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione alla gestione degli accessi da remoto.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi alla *gestione degli accessi da remoto* (tipicamente compresi nell'ambito della *gestione delle identità digitali e del controllo accessi*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1 e 2. | 1, 2, 3, 4 |
| Procedure, metodologie e tecnologie relative alla gestione degli accessi da remoto. | 1, 2, 5 |
| Elenco dei sistemi informativi e di rete ai quali è possibile accedere da remoto e descrizione delle relative modalità di accesso. | 5 |

# PR.AC-4

I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Le identità digitali sono assegnate in accordo al principio del privilegio minimo e nel rispetto del principio di separazione delle funzioni. |
| 2 | È assicurata la completa distinzione tra utenze con e senza privilegi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse. |
| 3 | Tutte le utenze con privilegi sono censite, approvate e utilizzate quando necessario registrando ogni accesso effettuato. |
| 4 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3. |
| 5 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3 |
| 6 | In relazione alla gestione dei diritti di accesso e alle relative autorizzazioni, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di assegnare le identità digitali in accordo al principio del privilegio minimo e nel rispetto del principio di separazione delle funzioni, ogni utente deve quindi accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.

La misura richiede inoltre di:

- assicurare la completa distinzione tra utenze con e senza privilegi degli amministratori di sistema;

> ⟷ Si prenda il caso dell'amministratore di sistema Mario Rossi. Nel rispetto di tale requisito, Mario Rossi dovrà avere due utenze distinte (alle quali corrisponderanno credenziali di accesso differenti): un'utenza con privilegi dedicata all'amministrazione dei sistemi e un'utenza senza per le ordinarie attività di ufficio come la consultazione della posta elettronica e l'accesso alla rete Internet.

- censire e approvare tutte le utenze con privilegi che devono essere usate solo quando necessario registrando ogni accesso effettuato e implementare adeguate misure di sicurezza per l'accesso.

I ruoli e le responsabilità degli attori deputati all'approvazione delle utenze con privilegi sono definiti nell'ambito della misura ID.AM-6.

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di definire e documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione alla gestione dei diritti di accesso e alle relative autorizzazioni.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi alla *gestione dei diritti di accesso e alle relative autorizzazioni* (tipicamente compresi nell'ambito della *gestione delle identità digitali e del controllo accessi*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1, 2 e 3. | 1, 2, 3, 4, 5 |
| Inventario delle utenze con privilegi comprensivo delle informazioni relative alla loro approvazione. | 3 |
| Procedure, metodologie e tecnologie relative alla gestione dei diritti di accesso e alle relative autorizzazioni. | 1, 2, 3, 6 |

# PR.DS-1

I dati memorizzati sono protetti.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 e ove applicabile, sono utilizzati sistemi di cifratura dei dati e in particolare per i dispositivi portatili e quelli removibili. |
| 2 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1. |
| 3 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1. |
| 4 | In relazione alla memorizzazione e protezione dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di utilizzare, ove applicabile, sistemi di cifratura per i sistemi informativi e di rete e in particolare per i dispositivi portatili e quelli removibili come, ad esempio, memorie di archiviazione di massa.

L'Agenzia per la cybersicurezza nazionale promuove l'uso della crittografia come strumento di cybersicurezza capace di assicurare un livello di protezione efficace e duraturo. Per ulteriori indicazioni, si prenda visione delle linee guida delle funzioni crittografiche reperibili all'indirizzo https://www.acn.gov.it/portale/crittografia.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda, ad esempio, della tipologia di dati trattati dai sistemi informativi e di rete e del contesto di utilizzo degli stessi (i dispositivi portatili, ad esempio, presentano rischi elevati di furto e smarrimento).

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di definire e documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione alla memorizzazione e protezione dei dati.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi alla *memorizzazione dei dati* (tipicamente compresi nell'ambito della *sicurezza dei dati*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi al requisito 1. | 1, 2, 3 |
| Procedure, metodologie e tecnologie relative alla memorizzazione e protezione dei dati. | 1, 4 |

# PR.IP-4

I backup delle informazioni sono eseguiti, amministrati e verificati.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono effettuati periodicamente i backup dei dati. |
| 2 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è assicurata la riservatezza delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. |
| 3 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino. |
| 4 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3. |
| 5 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3. |
| 6 | In relazione al backup dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di effettuare periodicamente i backup dei dati dei sistemi informativi e di rete, assicurare la riservatezza delle informazioni contenute nei backup proteggendo adeguatamente i supporti (anche tramite cifratura) e verificare periodicamente la correttezza dei backup mediante test di ripristino.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di dati trattati dai sistemi informativi e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che trattano dati per i quali sono state definite politiche più stringenti in termini di RTO e RPO, di conseguenza si adotteranno strategie di backup differenti (ad esempio in termini di frequenza oppure numero di copie di backup conservate anche offline).

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

È opportuno altresì prevedere backup dei dati relativi al monitoraggio di cui alla misura DE.CM-1.

La misura richiede infine di documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione al backup dei dati.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi al *backup dei dati* (tipicamente compresi nell'ambito della *sicurezza dei dati*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1, 2 e 3. | 1, 2, 3, 4, 5 |
| Procedure, metodologie e tecnologie relative al backup dei dati. | 1, 2, 3, 6 |

# PR.MA-1

La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, i sistemi informativi e di rete sono aggiornati all'ultima versione raccomandata dal produttore. L'aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo. |
| 2 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1. |
| 3 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1. |
| 4 | In relazione alla manutenzione e riparazione dei sistemi informativi e di rete, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di aggiornare i sistemi informativi e di rete all'ultima versione raccomandata dal produttore e di verificare, fatte salve motivate esigenze di tempestività relative alla sicurezza, gli aggiornamenti dei software ritenuti critici in ambiente di test e prima dell'effettivo impiego in ambiente operativo,

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di sistema informativo e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che presentano rischi maggiori in termini di esposizione alle vulnerabilità e alle minacce (si pensi ad esempio ai sistemi esposti su Internet come i *web server* o gli apparati perimetrali) per i quali dovranno essere adottate politiche specifiche in termini, ad esempio, di installazione degli aggiornamenti software.

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione alla manutenzione e riparazione dei sistemi informativi e di rete.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi alla *manutenzione e riparazione dei sistemi* e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

La **manutenzione dei sistemi informativi e di rete** comprende tutte quelle attività che sono poste in essere per prevenire guasti e malfunzionamenti o per ripristinare le funzionalità dei sistemi informativi e di rete.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi a requisito 1. | 1, 2, 3 |
| Procedure, metodologie e tecnologie relative alla manutenzione e riparazione dei sistemi informativi e di rete. | 1, 4 |

# PR.PT-4

Le reti di comunicazione e controllo sono protette.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presente e aggiornati i sistemi perimetrali, quali firewall, anche a livello applicativo. |
| 2 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1. |
| 3 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1 |
| 4 | In relazione alla protezione delle reti, esiste un documento aggiornato contenente almeno le procedure e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di prevedere sistemi perimetrali, quali ad esempio firewall, e di aggiornare tali sistemi.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di sistema informativo e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che presentano rischi maggiori in termini di esposizione alle vulnerabilità e alle minacce (si pensi ad esempio ai sistemi di posta elettronica) per i quali dovranno essere adottate politiche specifiche in termini, ad esempio, di configurazione dei sistemi perimetrali.

I **sistemi perimetrali** sono sistemi di sicurezza a protezione di due o più reti (tipicamente una rete privata e una rete pubblica) controllano il traffico in ingresso e in uscita dalle reti. Esempi di sistemi perimetrali sono *firewall*, *reverse proxy*, *secure email gateway*, ecc.

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione alla protezione delle reti.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi alla *protezione delle reti* e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi al requisito 1. | 1, 2, 3 |
| Procedure, metodologie e tecnologie relative alla protezione delle reti. | 1, 4 |

# DE.CM-1

Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presenti e aggiornati sistemi di rilevamento delle intrusioni (intrusion detection systems - IDS). |
| 2 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è monitorato il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali al fine di rilevare gli eventi di cybersecurity. |
| 3 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2. |
| 4 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2. |
| 5 | In relazione al monitoraggio degli eventi di sicurezza, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede – in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 – di prevedere sistemi di rilevamento delle intrusioni e di aggiornare tali sistemi.

I **sistemi di rilevamento delle intrusioni** sono sistemi di sicurezza che monitorano e analizzano gli eventi sui sistemi informativi e di rete con l'obiettivo di rilevare tentativi di accesso non autorizzato.

La misura richiede inoltre di monitorare – al fine di rilevare gli eventi di cybersecurity – le connessioni in ingresso e in uscita, le attività dei sistemi perimetrali (come, ad esempio, router e firewall), gli eventi amministrativi di rilievo, gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di sistema informativo e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che presentano rischi maggiori in termini di esposizione alle vulnerabilità e alle minacce (si pensi ad esempio ai sistemi esposti su Internet come i *web server*) per i quali dovranno essere adottate politiche specifiche in termini, ad esempio, di tipologia di eventi da monitorare.

Per monitorare gli elementi indicati, è tenuta traccia delle relative attività tramite i cosiddetti log (registri degli eventi).

Per il rilevamento degli eventi di cybersecurity possono essere utilizzati strumenti quali, ad esempio, i SIEM (Security information and event management) che sono soluzioni software in grado di acquisire, aggregare e analizzare informazioni da più fonti dati (le sorgenti da monitorare).

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione al monitoraggio degli eventi di sicurezza.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi al *monitoraggio degli eventi di sicurezza* e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1 e 2. | 1, 2, 3, 4 |
| Procedure, metodologie e tecnologie relative al monitoraggio degli eventi di sicurezza. | 1, 2, 5 |

# DE.CM-4

Il codice malevolo viene rilevato.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Sono presenti e aggiornati sistemi di protezione delle postazioni terminali. |
| 2 | In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.). |
| 3 | Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2. |
| 4 | I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2. |
| 5 | In relazione al rilevamento del codice malevolo, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di prevedere sistemi di protezione delle postazioni terminali e di aggiornare tali sistemi.

I **sistemi di protezione delle postazioni terminali** sono soluzioni di sicurezza che proteggono le postazioni terminali (o *endpoint*) dagli attacchi come ad esempio gli *antivirus*, antimalware, gli HIPS/HIDS (*Host Intrusion Prevention System*, *Host Intrusion Detection System*).

La misura richiede inoltre di analizzare e filtrare il traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.) ai sistemi informativi e di rete.

L'analisi del rischio condotta sui sistemi informativi e di rete può infatti determinare rischi differenti a seconda della tipologia di sistema informativo e di rete. Verosimilmente saranno presenti sistemi informativi e di rete che presentano rischi maggiori in termini di esposizione alle vulnerabilità e alle minacce (si pensi ad esempio ai sistemi di posta elettronica) per i quali dovranno essere adottate politiche specifiche in termini, ad esempio, di regole di filtraggio da applicare.

I sistemi di analisi e filtraggio del traffico in ingresso sono soluzioni di sicurezza che analizzano i file scaricati, le mail in ingresso, ecc. per rilevare e rimuovere/mettere in quarantena eventuali contenuti malevoli presenti. Il rilevamento avviene tipicamente utilizzando le cosiddette *sandbox*, (ambienti virtuali nei quali è possibile eseguire applicazioni potenzialmente malevole o delle quali non è nota l'attendibilità),

La misura richiede quindi di definire politiche e processi rispetto ai requisiti sopra indicati e di includerli nelle politiche e nei processi di cui alla misura ID.GV-1.

La misura richiede infine di documentare le procedure, metodologie e tecnologie adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1 in relazione al rilevamento del codice malevolo.

A tal fine, si individuano le politiche e i processi di cui alla misura ID.GV-1 relativi al *rilevamento del codice malevolo* (tipicamente compresi nell'ambito del *monitoraggio degli eventi di sicurezza*) e si definiscono, e documentano, le procedure, indicanti anche le metodologie e tecnologie impiegate, che implementano tali politiche e processi.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Politiche e processi relativi ai requisiti 1 e 2. | 1, 2, 3, 4 |
| Procedure, metodologie e tecnologie relative al rilevamento del codice malevolo. | 1, 2, 5 |

# RS.RP-1

Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente.

## Requisiti implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| PUNTO | REQUISITO |
|---|---|
| 1 | Esiste un piano aggiornato di risposta agli incidenti all'interno del quale siano definiti almeno:<br>a) le articolazioni preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche;<br>b) le procedure per la notifica degli incidenti di cui all'articolo 1 della legge 28 giugno 2024, n. 90;<br>c) le procedure adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1. |

## Descrizione

La misura richiede di redigere e mantenere aggiornato un piano di risposta agli incidenti che contenga almeno i seguenti elementi:

- le articolazioni preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche;
- le procedure per la notifica degli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105;
- le procedure adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1, in relazione alla risposta agli incidenti.

In accordo a quanto indicato dall'articolo 1 commi 1 e 2 della legge, i soggetti segnalano, senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili. La segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale.

Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica, l'Agenzia applica, nel rispetto delle disposizioni dell'articolo 17, comma 4-quater, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti. La violazione delle disposizioni può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.

È stata predisposta ed è disponibile al seguente indirizzo la guida alla notifica degli incidenti al CSIRT Italia: https://www.acn.gov.it/portale/w/acn-pubblica-la-guida-alla-notifica-degli-incidenti-informatici.

# Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| CONTENUTO DOCUMENTO | REQUISITO |
|---|---|
| Piano di risposta agli incidenti | 1 |

# RC.RP-1

Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity.

## Implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| Punto | Requisito |
|---|---|
| 1 | Esiste un piano di ripristino che prevede almeno, le procedure necessarie al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidente di cybersecurity. |
| 2 | Il piano di ripristino prevede anche le procedure per il ripristino a seguito degli incidenti di cui all'articolo 1, comma 1 della legge 28 giugno 2024, n. 90. |

## Descrizione misura

La misura richiede di redigere e mantenere aggiornato un piano di ripristino prevedendo, almeno, le procedure necessarie al ripristino dei sistemi informativi e di rete al funzionamento antecedente agli incidenti di cybersecurity.

La misura richiede inoltre di prevedere le procedure per il ripristino a seguito degli incidenti di cui all'articolo 1, comma 1 della legge 28 giugno 2024, n. 90.

⇆ L'articolo 1, comma 1 della legge prevede la segnalazione e notifica degli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105 aventi impatto su reti, sistemi informativi e servizi informatici.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| Contenuto documento | Requisito |
|---|---|
| Piano di ripristino dagli incidenti | 1, 2 |

# PR.AT-1

Tutti gli utenti sono informati e addestrati.

## Implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| Punto | Requisito |
|---|---|
| 1 | Esiste un documento aggiornato che indica i contenuti della formazione fornita agli utenti e le modalità di verifica dell'acquisizione dei contenuti. |
| 2 | Esiste un registro aggiornato recante l'elenco degli utenti che hanno ricevuto la formazione e i relativi contenuti. |

## Descrizione misura

La misura richiede di prevedere un percorso di formazione per gli utenti e di redigere un documento che riporti i contenuti delle attività formative effettuate e che descriva le modalità con le quali è verificato l'apprendimento dei contenuti.

La misura richiede inoltre di tenere un registro recante l'elenco degli utenti che hanno ricevuto la formazione e i relativi contenuti.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| Contenuto documento | Requisito |
|---|---|
| Indicazione dei contenuti della formazione impartita agli utenti. | 1 |
| Modalità di verifica dell'acquisizione dei contenuti. | 1 |
| Registro contenente l'elenco degli utenti che hanno ricevuto la formazione e i relativi contenuti. | 2 |

# PR.AT-2

Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità.

## Implementazione minima attesa

La seguente tabella riporta i requisiti che devono essere soddisfatti per l'implementazione minima attesa della misura.

| Punto | Requisito |
|---|---|
| 1 | Esiste un documento aggiornato che indica i contenuti della formazione fornita agli utenti con privilegi e le modalità di verifica dell'acquisizione dei contenuti. |
| 2 | Esiste un registro aggiornato recante l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti. |

## Descrizione misura

La misura richiede di prevedere un percorso di formazione per gli utenti con privilegi e di redigere un documento che riporti i contenuti delle attività formative effettuate e che descriva le modalità con le quali è verificato l'apprendimento dei contenuti.

La misura richiede inoltre di tenere un registro recante l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti.

## Evidenze documentali

L'impianto documentale prodotto dal soggetto deve prevedere almeno i contenuti elencati nella seguente tabella, che riporta, oltre all'indicazione dei contenuti richiesti, i requisiti dell'implementazione minima della misura ai quali i contenuti fanno riferimento.

| Contenuto documento | Requisito |
|---|---|
| Indicazione dei contenuti della formazione impartita agli utenti con privilegi. | 1 |
| Modalità di verifica dell'acquisizione dei contenuti. | 1 |
| Registro contenente l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti. | 2 |

# Parte II: Modalità di implementazione

## delle misure di sicurezza per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90

**Sinossi**

In questa parte sono indicati i processi di cybersecurity da istituire per corrispondere alle misure di sicurezza individuate nella prima parte e le modalità di implementazione raccomandate per l'attuazione delle misure stesse. Al riguardo, si osserva che i soggetti possono implementare le misure di sicurezza secondo modalità alternative a quelle indicate, purché idonee a soddisfare le implementazioni minime attese.

# Processi di cybersecurity

La misura ID.GV-1 richiede, tra le altre cose, la definizione di processi di cybersecurity per almeno i seguenti ambiti:

a) governo;
b) gestione del rischio;
c) gestione degli asset;
d) gestione del rischio di cybersecurity della catena di approvvigionamento;
e) gestione delle vulnerabilità;
f) business continuity e disaster recovery;
g) gestione delle identità digitali e del controllo accessi;
h) sicurezza dei dati;
i) manutenzione e riparazione dei sistemi;
j) protezione delle reti;
k) monitoraggio degli eventi di sicurezza;
l) risposta e ripristino dagli incidenti;
m) formazione del personale.

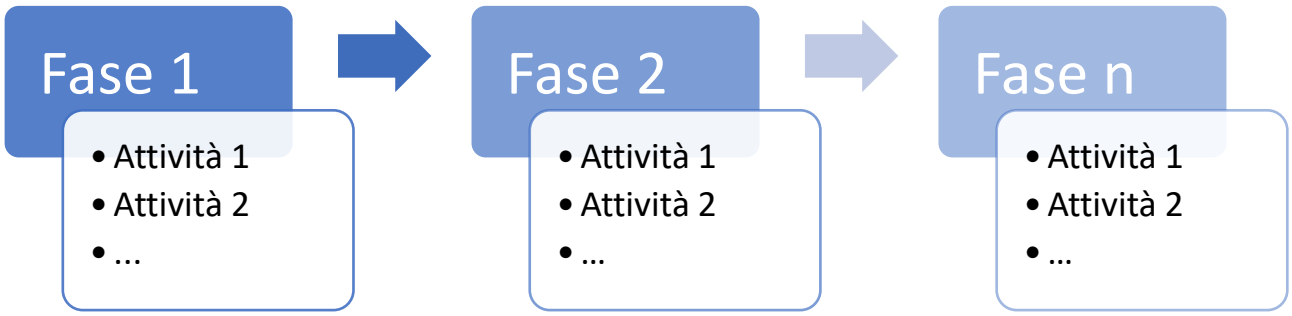
Un **processo di cybersecurity** è l'insieme delle fasi e attività relazionate tra loro ed eseguite per raggiungere specifici obiettivi in un determinato ambito della cybersecurity, come ad esempio la risposta agli incidenti, la sicurezza dei dati e la gestione delle vulnerabilità.

L'istituzione e adozione dei processi sopra indicati è necessaria per l'attuazione delle misure di sicurezza contenute nel presente documento. A seguire è riportato l'elenco dei processi di cybersecurity previsti dalla misura ID.GV-1 con l'indicazione, per ciascun processo, delle misure di sicurezza interessate.

a) **governo**: ID.AM-6, ID.GV-1;
b) **gestione del rischio**: ID.GV-4, ID.RA-5, ID.RA-6;
c) **gestione degli asset**: ID.AM-1, ID.AM-2, ID.AM-3;
d) **gestione del rischio di cybersecurity della catena di approvvigionamento**: ID.SC-2;
e) **gestione delle vulnerabilità**: ID.RA-1, PR.IP-12, RS.AN-5;
f) **business continuity e disaster recovery**: PR.IP-9;
g) **gestione delle identità digitali e del controllo accessi**: PR.AC-1, PR.AC-3, PR.AC-4;
h) **sicurezza dei dati**: PR.DS-1, PR.IP-4;
i) **manutenzione e riparazione dei sistemi**: PR.MA-1;
j) **protezione delle reti**: PR.PT-4;
k) **monitoraggio degli eventi di sicurezza**: DE.CM-1, DE.CM-4;
l) **risposta e ripristino dagli incidenti**: RS.RP-1, RC.RP-1;
m) **formazione del personale**: PR.AT-1, PR.AT-2.

## Struttura di un processo

Un processo è composto da una o più fasi che comprendono a loro volta una o più attività e può essere rappresentato tramite appositi diagrammi come, ad esempio, quello riprodotto nella seguente figura in cui sono riportate generiche fasi e attività.




## Ruoli e responsabilità

Per ogni attività di un processo sono assegnati i corrispondenti ruoli e responsabilità. Uno degli strumenti più utilizzati per questo scopo è la matrice di assegnazione responsabilità (anche denominata matrice RACI) che prevede i ruoli di seguito riportati.

- **Responsible (R)**: fa riferimento all'attore che esegue operativamente l'attività.
- **Accountable (A)**: fa riferimento all'attore che ha la responsabilità sul risultato dell'attività.
- **Consulted (C)**: fa riferimento all'attore che aiuta e collabora con il *Responsible* per l'esecuzione dell'attività in quanto possiede conoscenze necessarie al completamento dell'attività.
- **Informed (I)**: fa riferimento all'attore che deve essere informato sull'avanzamento e il completamento dell'attività.

Per ogni attività deve essere presente almeno un attore *Responsible* in modo da individuare chi ha il compito di eseguire operativamente l'attività ed un solo attore *Accountable* in modo da definire chiaramente chi ha la responsabilità sul risultato dell'attività. Per definire i ruoli e le responsabilità di un processo tramite matrici RACI sono preliminarmente individuati gli attori coinvolti – intesi come articolazioni del soggetto o specifiche figure quale, ad esempio quella del referente per la cybersicurezza – e quindi assegnati i ruoli agli attori per le varie attività. La seguente tabella mostra un generico esempio di matrice RACI.

| Fase | Attività | Attore 1 | Attore 2 | Attore n |
|---|---|---|---|---|
| Fase 1 | Attività 1 | A, R | C | I |
| Fase 1 | Attività 2 | R | A, R | // |
| Fase 1 | Attività n | A | R | C |
| Fase 2 | Attività 1 | A, R | I | C |
| Fase 2 | Attività 2 | I | // | A, R |
| Fase 2 | Attività n | A, R | I | I |
| Fase n | Attività 1 | C | I | A, R |
| Fase n | Attività 2 | R | // | A |
| Fase n | Attività n | A, R | C | C |

# ID.AM-6

Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner).

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Definire l'organizzazione di cybersecurity. A tal fine:
   - identificare le strutture, comprese eventuali terze parti, preposte al governo e alla gestione della sicurezza dei sistemi informativi e di rete del soggetto;

> ⟷ Per identificare le strutture bisogna sostanzialmente capire *chi fa cosa* nell'ambito della cybersecurity, identificando determinate macroaree di responsabilità. Come elenco di base per l'identificazione di tali macroaree si può fare riferimento, ad esempio, alle categorie del Framework Nazionale per la Cybersecurity e la Data Protection.

   - assegnare i ruoli e responsabilità del personale dell'organizzazione facendo riferimento anche a quelli di eventuali terze parti comprese nell'organizzazione.

> ⟷ Per l'assegnazione di ruoli e responsabilità, far riferimento al sotto-paragrafo Ruoli e responsabilità del capitolo Processi di cybersecurity.

2. Individuare, all'interno dell'organizzazione di cybersecurity, una **struttura** che provveda almeno alle seguenti attività:
   a) sviluppo delle politiche e delle procedure di sicurezza delle informazioni;
   b) produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
   c) produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni del soggetto;
   d) produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture del soggetto;
   e) pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);
   f) pianificazione e attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
   g) monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.
3. Assegnare, nell'ambito della struttura di cui al precedente punto 2, i ruoli e le responsabilità per le attività elencate.

Per l'assegnazione di ruoli e responsabilità, far riferimento al sotto-paragrafo Ruoli e responsabilità del capitolo Processi di cybersecurity.

4. Individuare, nell'ambito della struttura di cui al precedente punto 2, il **referente per la cybersicurezza**, in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

Il referente svolge anche la funzione di punto di contatto unico del soggetto con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla legge e dalle normative settoriali in materia di cybersicurezza alle quali deve adempiere il medesimo soggetto.

[*v. articolo 8, comma 2, della legge*].

5. Rendere note alle articolazioni del soggetto l'organizzazione di cui al precedente punto 1 e la struttura di cui al precedente punto 2.

Ferma restando la competenza del soggetto sull'individuazione delle modalità più idonee a rendere note l'organizzazione e la struttura alle articolazioni del soggetto, una possibile modalità potrebbe consistere nella pubblicazione di tali informazioni sulla *intranet* del soggetto e la contestuale notifica tramite, per esempio, mail circolare.

6. Comunicare il nominativo e gli estremi di contatto del referente per la cybersicurezza di cui al precedente punto 4 all'Agenzia per la cybersicurezza nazionale secondo le modalità indicate sul sito dell'Agenzia.

7. Redigere l'elenco del personale interno ed esterno dell'organizzazione di cui al precedente punto 1, ivi incluso quello della struttura di cui al precedente punto 2, avente specifici ruoli e responsabilità.

8. Revisionare i ruoli e le responsabilità assegnati nell'ambito dell'organizzazione di cui al precedente punto 1 e della struttura di cui al precedente punto 2, a intervalli pianificati e al verificarsi di specifici eventi, come ad esempio: variazioni del quadro normativo o regolamentare, cambiamenti interni all'organizzazione, incidenti di sicurezza, mutamenti dell'esposizione alle minacce e ai relativi rischi.

In considerazione della loro rilevanza, l'organizzazione di cybersecurity, la struttura e il referente per la cybersicurezza devono essere nominati formalmente – ad esempio tramite appositi *Ordini di Servizio* – dal vertice del soggetto o da una figura da lui delegata.

# ID.GV-1

È identificata e resa nota una policy di cybersecurity.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Definire e documentare le politiche per la sicurezza dei sistemi informativi e di rete per almeno i seguenti ambiti:
   a) governo;
   b) gestione del rischio;
   c) gestione degli asset;
   d) gestione del rischio di cybersecurity della catena di approvvigionamento;
   e) gestione delle vulnerabilità;
   f) business continuity e disaster recovery;
   g) gestione delle identità digitali e del controllo accessi;
   h) sicurezza dei dati;
   i) manutenzione e riparazione dei sistemi;
   j) protezione delle reti;
   k) monitoraggio degli eventi di sicurezza;
   l) risposta e ripristino agli incidenti;
   m) formazione del personale.

Gli ambiti sopra elencati forniscono un primo livello di strutturazione delle politiche. Ulteriori livelli di strutturazione dipendono dalle specifiche politiche e dal loro livello di granularità. È opportuno, in generale, identificare e organizzare le politiche secondo una struttura gerarchica di ambiti e sotto-ambiti di riferimento. Allo scopo risulta utile identificarle tramite uno schema che permetta di ricondurre ciascuna politica al sotto-ambito di riferimento, come, ad esempio, attraverso uno schema del tipo **X.Y.Z**, dove **X** rappresenta il codice identificativo dell'ambito, **Y** il codice identificativo del sotto-ambito (è possibile eventualmente prevedere più livelli gerarchici modificando di conseguenza lo schema di identificazione) e **Z** il numero incrementale della politica nel sotto-ambito.

Se, ad esempio, viene definita una politica che riguarda l'etichettatura dei sistemi e degli apparati fisici, si potrà prevedere un sotto ambito *sistemi e apparati fisici*, questa potrà essere identificata da **c.1.1**, con **c** ambito *gestione degli asset*, **1** sotto-ambito *sistemi e apparati fisici* e **1** numero incrementale della politica nel sotto-ambito (l'ambito è stato rappresentato tramite le medesime lettere usate al punto 1 della presente misura per indicare gli ambiti, il sotto-ambito è stato rappresentato tramite il codice numerico **1** e si è assunto che la politica sia la prima definita nel sotto-ambito).

2. Ottenere l'approvazione dei vertici sulle politiche definite.

3. Rendere note le politiche alle articolazioni del soggetto interessate.
4. Definire e documentare i processi di cybersecurity per almeno i seguenti ambiti e in aderenza alle politiche di cui al precedente punto 1:
   a) governo;
   b) gestione del rischio;
   c) gestione degli asset;
   d) gestione del rischio di cybersecurity della catena di approvvigionamento;
   e) gestione delle vulnerabilità;
   f) business continuity e disaster recovery;
   g) gestione delle identità digitali e del controllo accessi;
   h) sicurezza dei dati;
   i) manutenzione e riparazione dei sistemi;
   j) protezione delle reti;
   k) monitoraggio degli eventi di sicurezza;
   l) risposta e ripristino agli incidenti;
   m) formazione del personale.
5. Revisionare le politiche e i processi di cybersecurity a intervalli pianificati e al verificarsi di specifici eventi, come ad esempio: variazioni del quadro normativo o regolamentare, cambiamenti interni all'organizzazione, incidenti di sicurezza, mutamenti dell'esposizione alle minacce e ai relativi rischi.
6. Redigere il piano programmatico per la sicurezza di dati, sistemi e infrastrutture. A tal fine:
   a) definire gli obiettivi strategici in termini di sicurezza di dati, sistemi e infrastrutture in coerenza con le politiche di cybersecurity;
   b) pianificare le attività per raggiungere gli obiettivi definiti.

# ID.GV-4

La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione del rischio di cui alla misura ID.GV-1, redigere e mantenere aggiornato un piano per la gestione del rischio informatico.

Un modello che può essere usato come riferimento per la redazione del piano di gestione del rischio informatico è quello indicato dalla norma ISO/IEC 27005 *gestione dei rischi per la sicurezza delle informazioni* che prevede le seguenti fasi:

a) **definizione del contesto**: sono stabiliti i criteri di identificazione e accettazione dei rischi, i ruoli e le responsabilità per la gestione dei rischi, le metriche di calcolo degli impatti e delle probabilità;
b) **valutazione del rischio**: sono identificati, analizzati e ponderati i rischi;
c) **trattamento del rischio**: il rischio risultante in esito alla valutazione è opportunamente trattato (le tipologie di trattamento tipicamente prevedono che il rischia possa essere mitigato, condiviso, evitato oppure mantenuto);
d) **accettazione del rischio**: il rischio residuo in esito al trattamento è formalmente accettato dai vertici del soggetto;
e) **comunicazione e consultazione**: gli esiti delle varie fasi sono comunicati e condivisi tra gli attori coinvolti;
f) **monitoraggio e revisione**: i rischi, in considerazione della loro natura dinamica, sono continuamente monitorati e revisionati per identificarne i cambiamenti.

Le prime quattro fasi sono sequenziali mentre le ultime due sono trasversali alle precedenti.

# ID.AM-1

Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito e nell'ambito del processo di *governance*, definire politiche e processi relativi alla gestione delle identità digitali e del controllo accessi che prevedano l'accesso alla rete esclusivamente a sistemi e apparati fisici approvati dagli attori interni alla struttura.
2. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione degli asset, redigere l'inventario dei sistemi e degli apparati fisici.
3. Con riferimento all'inventario di cui al precedente punto 2, censire almeno le seguenti categorie di sistemi e apparati e le relative informazioni, ove presenti e disponibili:
   a) **server**: funzione, nome macchina, marca, modello, indirizzo/i IP, versione sistema/i operativo/i, occupazione disco (GB di dati occupati e percentuale di occupazione);
   b) **postazioni di lavoro** (laptop e desktop): nome macchina, marca, modello, indirizzo/i IP, sistema/i operativo/i;
   c) **soluzioni di sicurezza** (firewall, SIEM, sandbox, ecc.): nome soluzione, funzione, marca, versione, indirizzo/i IP;
   d) **apparati di rete** (switch, router, ecc.): nome apparato, funzione, tipologia di apparato, marca, modello, indirizzo/i IP;
   e) **reti**: nome rete, classe di indirizzamento, tipologia rete;
   f) **connettività**: fornitore, larghezza di banda, tipologia (ad es. ADSL, fibra, satellitare);
   g) **centralini di telecomunicazione**: marca, modello, numero di utenti serviti, tipologia centralino;
   h) **dispositivi mobili** (smartphone/tablet): nome dispositivo, tipologia dispositivo, marca, modello;
   i) **apparati di videosorveglianza**: nome apparato, tipologia apparato, marca, modello, indirizzo/i IP;
   j) **apparati di videoconferenza**: nome apparato, tipologia apparato, marca, modello, indirizzo/i IP;
   k) **apparati per il controllo degli accessi**: nome apparato, tipologia apparato, marca, modello, indirizzo/i IP;
   l) **periferiche** (stampanti, scanner, multifunzione, ecc.): nome periferica, tipologia periferica, marca, modello, indirizzo IP, nominativo assegnatario, ufficio responsabile;
   m) qualunque tipo di sistema/apparato non rientrante nelle precedenti categorie ma connesso alla rete informatica del soggetto: nome sistema/apparato, tipologia sistema/apparato, marca, modello, indirizzo/i IP.
4. Prevedere, per ogni sistema e apparato fisico presente nell'inventario di cui al precedente punto 2, il censimento anche delle seguenti informazioni, ove disponibili:

a) nominativo assegnatario;
b) nominativo responsabile gestione;
c) nominativo responsabile per l'autorizzazione all'accesso alla rete;
d) esito e data del processo di autorizzazione;
e) fornitore/partner terzo;
f) informazioni sulle licenze;
g) informazioni sulla garanzia;
h) versioni di software, hardware e firmware.

5. Ottenere l'approvazione dagli attori interni alla struttura per i sistemi e gli apparati fisici che accedono alla rete.
6. Revisionare e aggiornare periodicamente l'inventario di cui al precedente punto 2. A tal fine prevedere quanto più possibile l'uso di strumenti automatici.

# ID.AM-2

Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito e nell'ambito del processo di *governance*, definire politiche e processi relativi alla gestione delle identità digitali e del controllo accessi che prevedano l'installazione esclusivamente delle piattaforme e delle applicazioni software approvate.
2. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione degli asset, redigere l'inventario delle piattaforme e delle applicazioni software.
3. Con riferimento all'inventario di cui al precedente punto 2, censire almeno le seguenti informazioni, ove presenti e disponibili:
   a) nome piattaforma/applicazione software;
   b) elenco dei sistemi e apparati fisici sui quali è installata la piattaforma/applicazione software;
   c) licenze;
   d) tipologie di autenticazione (ad es. locale o di dominio);
   e) utenti amministrativi;
   f) fornitore/partner terzo;
   g) nominativo responsabile gestione;
   h) nominativo responsabile per l'autorizzazione all'installazione;
   i) esito e data del processo di autorizzazione;
4. Ottenere l'approvazione dagli attori interni alla struttura per le piattaforme e le applicazioni software installate.
5. Revisionare e aggiornare periodicamente l'inventario di cui al precedente punto 2 tal fine prevedere quanto più possibile l'uso di strumenti automatici.

# ID.AM-3

I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito e nell'ambito del processo di *governance*, definire politiche e processi relativi alla gestione delle identità digitali e del controllo accessi che prevedano che le comunicazioni siano consentite esclusivamente per i flussi informativi approvati.
2. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione degli asset, redigere l'inventario dei flussi informativi.
3. Con riferimento all'inventario di cui al precedente punto 2, censire almeno le seguenti informazioni, ove presenti e disponibili:
   a) sorgente del flusso;
   b) destinatario del flusso,
   c) protocolli e servizi di rete abilitati sul flusso (ad esempio HTTPS, DNS; NTP, ecc.).
   d) nominativo responsabile gestione;
   e) nominativo responsabile per l'autorizzazione alla comunicazione;
   f) esito e data del processo di autorizzazione;
4. Ottenere l'approvazione dagli attori interni alla struttura i flussi per i flussi informativi.
5. Revisionare e aggiornare periodicamente l'inventario di cui al precedente punto 2, a tal fine prevedere quanto più possibile l'uso di strumenti automatici.

# ID.SC-2

I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione del rischio di cybersecurity della catena di approvvigionamento redigere l'inventario dei fornitori e partner terzi affidatari di forniture di beni, sistemi e servizi ICT.
2. Con riferimento all'inventario di cui al precedente punto 1, censire almeno le seguenti informazioni, ove presenti e disponibili:
   a) nome fornitore/partner terzo;
   b) identificativo bene/sistema informatico/servizio ICT;
   c) informazioni contrattuali.
3. Revisionare e aggiornare periodicamente l'inventario di cui al precedente punto 1.

# ID.RA-5

Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo a quanto previsto dal piano di gestione del rischio informatico di cui alla misura ID.GV-4, eseguire periodicamente la valutazione del rischio sui sistemi informativi e di rete.
2. Con riferimento alla valutazione del rischio di cui al punto 1:
   a) identificare i rischi in considerazione delle minacce (interne ed esterne), delle vulnerabilità e degli asset che compongono i sistemi informativi e di rete;
   b) analizzare i rischi calcolando il livello di rischio come combinazione dell'impatto e della probabilità di accadimento;
   c) ponderare il rischio, confrontando il livello di rischio risultante dall'analisi con i criteri di accettazione del rischio.

L' *identificazione dei rischi* può essere basata sugli asset oppure sugli eventi, anche declinati per il tramite di scenari di rischio, a seconda dell'elemento a partire dal quale sono individuate le minacce e le vulnerabilità.

# ID.RA-6

Sono identificate e prioritizzate le risposte al rischio.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo a quanto previsto dal piano di gestione del rischio informatico di cui alla misura ID.GV-4 e sulla base degli esiti della valutazione del rischio di cui alla misura ID.RA-5, definire e documentare:
   a) il piano di trattamento (mitigare/condividere/evitare/accettare) per ogni rischio individuato nella fase di valutazione;
   b) le priorità di trattamento.
2. Ottenere l'approvazione dei vertici del soggetto dell'accettazione del rischio residuo.

# ID.RA-1

Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity, nell'ambito del processo di gestione delle vulnerabilità e in accordo agli esisti dell'analisi del rischio di cui alla misura ID.RA-5, redigere e mantenere aggiornato un piano delle attività per individuare le vulnerabilità dei sistemi informativi e di rete prevedendo almeno i seguenti contenuti:
   a) modalità con le quali sono identificate le vulnerabilità;
   b) pianificazione delle attività di cui alla precedente lettera a).
2. Eseguire periodicamente le attività in accordo alla pianificazione di cui al precedente punto 1.
3. Predisporre, in esito alle attività di cui al precedente punto 3, apposite relazioni periodiche contenenti almeno:
   a) descrizione e risultati delle attività effettuate;
   b) descrizione delle vulnerabilità rilevate e relativo impatto sulla sicurezza.

Per le vulnerabilità note esistono database pubblicamente accessibili, quali il **CVE** (*Common Vulnerabilities and Exposures*) della MITRE Corporation che associa un identificativo univoco a ciascuna vulnerabilità presente nel database e gli associa una serie di informazioni. Il **CVSS** (*Common Vulnerability Scoring System*) è un sistema di valutazione che associa a ciascuna vulnerabilità del database CVE una serie di parametri per valutarne la sua severità, tra i quali un indice, in una scala da 1 a 10, che ne sintetizza la gravità.

L'elenco pubblico delle CVE e corrispondenti CVSS è accessibile all'indirizzo https://cve.mitre.org/.

# PR.IP-12

Viene sviluppato e implementato un piano di gestione delle vulnerabilità.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Definire le politiche in relazione ai seguenti requisiti:
   a) risoluzione delle vulnerabilità emerse a seguito delle attività di cui al punto 2 della misura ID.RA-1;
   b) adozione degli interventi indicati dall'Agenzia per la cybersicurezza nazionale per la risoluzione delle specifiche vulnerabilità segnalate dall'Agenzia.
2. Includere le politiche e i processi relativi al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione delle vulnerabilità di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione a tale ambito.
4. Eseguire quando previsto ogni fase del processo di gestione delle vulnerabilità.

# RS.AN-5

Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza).

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione delle vulnerabilità di cui alla misura ID.GV-1, redigere e mantenere aggiornato un piano che descriva la gestione delle informazioni inerenti le vulnerabilità provenienti dal CSIRT Italia e/o da eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento prevedendo almeno i seguenti contenuti:
    a) modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità e in particolare quelle segnalate dell'Agenzia per la cybersicurezza nazionale sulle specifiche vulnerabilità alle quali si è potenzialmente esposti;
    b) procedure, ruoli, responsabilità e strumenti tecnici utilizzati per lo svolgimento delle attività di cui alla precedente lettera a).

Nel piano è opportuno anche indicare i criteri con i quali è stabilità la priorità per la risoluzione delle vulnerabilità. Fatto salvo quanto previsto dalla legge in merito alle segnalazioni dell'Agenzia per la cybersicurezza nazionale, possibili criteri per l'assegnazione delle priorità sono definiti sulla base della classificazione della gravità (tramite ad esempio il parametro **CVSS** che su una scala da 1 a 10 assegna 10 alle vulnerabilità con gravita massima), del contesto e del fatto che la vulnerabilità sia *exploit in the wild* (ovvero si ha contezza, ad esempio tramite i bollettini di sicurezza rilasciati dal fornitore in occasione degli aggiornamenti, che la vulnerabilità sia stata già sfruttata per condurre attacchi).

# PR.IP-9

Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di continuità operativa e disaster recovery, definire e documentare i piani di:
   a) continuità operativa;
   b) disaster recovery.
2. Revisionare i piani a intervalli pianificati e al verificarsi di specifici eventi, come ad esempio: variazioni del quadro normativo o regolamentare, cambiamenti interni all'organizzazione, incidenti di sicurezza, mutamenti dell'esposizione alle minacce e ai relativi rischi.

# PR.AC-1

Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Definire le politiche e i processi in relazione ai seguenti requisiti:
    a) assegnazione di credenziali di accesso individuali agli utenti;
    b) robustezza delle credenziali di accesso e aggiornamento con cadenza proporzionata ai privilegi dell'utenza;
    c) in accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, verifica periodica delle identità digitali e delle credenziali di accesso e/o revoca in caso di variazioni.
2. Includere le politiche e i processi relativi al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione delle identità digitali e del controllo accessi di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso agli utenti.
4. Eseguire quando previsto ogni fase del processo di *gestione delle identità digitali e del controllo accessi* relativa all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso agli utenti.

# PR.AC-3

L'accesso remoto alle risorse è amministrato.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, definire le politiche e i processi in relazione ai seguenti requisiti:
   a) monitoraggio degli accessi da remoto;
   b) tracciamento degli accessi eseguiti da remoto;
   c) definizione delle attività consentire da remoto;
   d) definizione e implementazione delle misure di sicurezza per l'accesso remoto.
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Redigere e mantenere aggiornato l'elenco dei sistemi informativi e di rete ai quali è possibile accedere da remoto e le relative modalità di accesso.
4. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione delle identità digitali e del controllo accessi di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate relative alla gestione degli accessi da remoto.
5. Eseguire quando previsto ogni fase del processo di gestione delle identità digitali e del controllo accessi in relazione alla gestione degli accessi da remoto.

# PR.AC-4

I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Definire le politiche e i processi in relazione ai seguenti requisiti:
    a) assegnazione delle credenziali di accesso in accordo al principio del minimo privilegio e nel rispetto della separazione delle funzioni;
    b) distinzione tra utente con e senza privilegi degli amministratori di sistema;
    c) censimento e approvazione delle utenze con privilegi;
    d) uso delle credenziali di accesso solo se necessario e registrazione degli accessi effettuati.
2. Includere le politiche e i processi relativi al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Redigere e mantenere aggiornato il censimento delle utenze con privilegi riportando le informazioni relative alla loro autorizzazione.
4. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di gestione delle identità digitali e del controllo accessi di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione alla gestione dei diritti di accesso e alle relative autorizzazioni.
5. Eseguire quando previsto ogni fase del processo di gestione delle identità digitali e del controllo accessi relativa alla gestione dei diritti di accesso e alle relative autorizzazioni.

# PR.DS-1

I dati memorizzati sono protetti.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Definire le politiche e i processi in relazione all'uso di sistemi di cifratura per i sistemi informativi e di rete.
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di sicurezza dei dati di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione alla memorizzazione e protezione dei dati.
4. Eseguire quando previsto ogni fase del processo di sicurezza dei dati relativa alla memorizzazione e protezione dei dati.

# PR.IP-4

I backup delle informazioni sono eseguiti, amministrati e verificati.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, definire le politiche in relazione ai seguenti requisiti:
   a) esecuzione periodica dei backup;
   b) protezione fisica dei supporti di backup;
   c) verifica periodica dell'utilizzabilità dei backup;
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di sicurezza dei dati di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione al backup dei dati.
4. Eseguire quando previsto ogni fase del processo di sicurezza dei dati relativa al backup dei dati.

# PR.MA-1

La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, definire le politiche e i processi in relazione all'aggiornamento dei sistemi informativi e di rete.
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di manutenzione e riparazione dei sistemi di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione a tale ambito.
4. Eseguire quando previsto ogni fase del processo di manutenzione e riparazione dei sistemi.

# PR.PT-4

Le reti di comunicazione e controllo sono protette.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, definire le politiche e i processi in relazione all'impiego dei sistemi perimetrali e alla modalità con le quali sono aggiornati.
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di protezione delle reti di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione a tale ambito.
4. Eseguire quando previsto ogni fase del processo di protezione delle reti.

# DE.CM-1

Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, definire le politiche e i processi in relazione ai seguenti requisiti:
   a) impiego di sistemi di rilevamento delle intrusioni e loro aggiornamenti;
   b) monitoraggio del traffico in ingresso e in uscita, delle attività dei sistemi perimetrali, degli eventi amministrativi di rilievo, degli access eseguiti o falliti alle risorse di rete;
   c) rilevamento degli eventi di cybersecurity sulla base degli elementi di cui alla precedente lettera b).
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di monitoraggio degli eventi di sicurezza e di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione a tale ambito.
4. Eseguire quando previsto ogni fase del processo di monitoraggio degli eventi di sicurezza.

# DE.CM-4

Il codice malevolo viene rilevato.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, definire le politiche e i processi in relazione ai seguenti requisiti:
   a) impiego di sistemi di protezione delle postazioni terminali e loro aggiornamenti;
   b) uso degli strumenti di analisi e filtraggio sul flusso di traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.).
2. Includere le politiche e i processi di cui al precedente punto 1 nelle politiche e nei processi di cui alla misura ID.GV-1.
3. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di monitoraggio degli eventi di sicurezza di cui alla misura ID.GV-1, definire e documentare procedure, metodologie e tecnologie impiegate, in relazione al rilevamento del codice malevolo.
4. Eseguire quando previsto ogni fase del processo di monitoraggio degli eventi di sicurezza relativa al rilevamento del codice malevolo.

# RS.RP-1

Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nell'ambito del processo di risposta e ripristino dagli incidenti, redigere e mantenere aggiornato il piano di risposta agli incidenti, prevedendo almeno i seguenti contenuti:
   a) descrizione delle articolazioni preposte all'attuazione del piano con l'indicazione delle competenze decisionali, finanziarie e tecniche;
   b) le procedure per la notifica degli incidenti di cui all'articolo 1 della legge 28 giugno 2024, n. 90;
   c) le procedure adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1, in relazione alla risposta agli incidenti.
2. Revisionare il piano a intervalli pianificati e al verificarsi di specifici eventi, come ad esempio: variazioni del quadro normativo o regolamentare, cambiamenti interni all'organizzazione, incidenti di sicurezza, mutamenti dell'esposizione alle minacce e ai relativi rischi.

Un modello che può essere usato come riferimento per la redazione del piano di risposta è quello indicato nel documento del NIST *Computer Secuirity Incident Handling Guide SP.800-61 r.2* (accessibile all'indirizzo https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf) che prevede le seguenti quattro fasi: **preparazione** (in cui sono definiti e allestiti gli strumenti e le risorse che verranno poi utilizzati nel corso dell'incidente), **rilevamento e analisi** (in cui sono rilevati gli eventi di sicurezza ed è dichiarato e analizzato l'incidente), **contenimento, eradicazione e ripristino** (in cui viene gestito l'incidente tramite contenimento e rimozione della minacce e successivo ripristino allo stato antecedente l'incidente) e **attività post-incidente** (in cui è documentato l'incidente e migliorato, tramite la cosiddetta *lesson learned*, il processo di risposta alla luce di quanto emerso durante la gestione dell'incidente).

# RC.RP-1

Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nell'ambito del processo di risposta e ripristino dagli incidenti, redigere e mantenere aggiornato il piano di ripristino dagli incidenti, prevedendo almeno i seguenti contenuti:
   a) procedure necessarie al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidente di cybersecurity;
   b) procedure per il ripristino a seguito degli incidenti di cui all'articolo 1, comma 1 della legge.
2. Revisionare il piano a intervalli pianificati e al verificarsi di specifici eventi, come ad esempio: variazioni del quadro normativo o regolamentare, cambiamenti interni all'organizzazione, incidenti di sicurezza, mutamenti dell'esposizione alle minacce e ai relativi rischi.

# PR.AT-1

Tutti gli utenti sono informati e addestrati.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di formazione del personale, definire un percorso didattico che, a partire dall'analisi del fabbisogno formativo degli utenti, definisca i contenuti della formazione e ne preveda la verifica dell'apprendimento.
2. Condurre le attività di formazione verificandone l'apprendimento.
3. Redigere e mantenere aggiornato il registro con l'elenco degli utenti che hanno ricevuto la formazione e i relativi contenuti.

# PR.AT-2

Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità.

## Modalità di implementazione

In questo paragrafo sono riportate, sotto forma di indicazioni operative e di dettaglio, le modalità di implementazione raccomandate per l'attuazione della misura.

1. Nel rispetto delle politiche di cybersecurity e nell'ambito del processo di formazione del personale, definire un percorso didattico che, a partire dall'analisi del fabbisogno formativo degli utenti con privilegi, definisca i contenuti della formazione e ne preveda la verifica dell'apprendimento.
2. Condurre le attività di formazione verificandone l'apprendimento.
3. Redigere e mantenere aggiornato il registro con l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti.

# Appendice A: implementazioni minime attese

## ID.AM-1

**Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione.**

1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90.
2. L'accesso alla rete è consentito esclusivamente ai soli sistemi e apparati fisici approvati.

## ID.AM-2

**Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione.**

1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90.
2. L'installazione è consentita esclusivamente alle piattaforme e applicazioni software approvate.

## ID.AM-3

**I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.**

1. Tutti i flussi informativi tra i sistemi informativi e di rete del soggetto e l'esterno sono identificati ed esiste un elenco di quelli approvati da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90.
2. Le comunicazioni sono consentite esclusivamente per i flussi informativi approvati.

## ID.AM-6

**Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner).**

1. È definita e resa nota alle articolazioni del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.
2. All'interno dell'organizzazione di cui al punto 1, è istituita e resa nota alle articolazioni del soggetto la struttura di cui all'articolo 8, comma 1, della Legge 28 giugno 2024, n. 90 e sono assegnati, nell'ambito di tale struttura, ruoli e responsabilità per almeno le attività indicate nel medesimo comma.
3. È nominato, nell'ambito della struttura di cui al punto 2, il referente per la cybersicurezza di cui all'articolo 8, comma 2, della Legge 28 giugno 2024, n. 90, in possesso di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

4. Sono comunicati all'Agenzia per la cybersicurezza nazionale il nominativo e gli estremi di contatto del referente di cui al punto 3 secondo le modalità rese note attraverso il sito dell'Agenzia per la cybersicurezza nazionale.
5. Esiste un elenco del personale interno ed esterno dell'organizzazione di cui al punto 1, ivi incluso quello della struttura di cui al punto 2, avente specifici ruoli e responsabilità.

## ID.GV-1

**È identificata e resa nota una policy di cybersecurity.**

1. Le politiche e i processi di cybersecurity sono definiti per almeno i seguenti ambiti:
   a) governo;
   b) gestione del rischio;
   c) gestione degli asset;
   d) gestione del rischio di cybersecurity della catena di approvvigionamento;
   e) gestione delle vulnerabilità;
   f) business continuity e disaster recovery;
   g) gestione delle identità digitali e del controllo accessi;
   h) sicurezza dei dati;
   i) manutenzione e riparazione dei sistemi;
   j) protezione delle reti;
   k) monitoraggio degli eventi di sicurezza;
   l) risposta e ripristino agli incidenti;
   m) formazione del personale.
2. Esiste un documento aggiornato che descrive le politiche di cybersecurity di cui al punto 1.
3. Esiste un documento aggiornato che descrive i processi di cybersecurity di cui al punto 1.
4. Le politiche e i processi di cui al punto 1 sono revisionati periodicamente e quando necessario.
5. Esiste un piano programmatico aggiornato per la sicurezza di dati, sistemi e infrastrutture in accordo alle politiche di cui al punto 1.

## ID.GV-4

**La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity.**

1. Esiste un piano aggiornato per la gestione del rischio informatico.

## ID.RA-1

**Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, esiste un piano aggiornato che descrive l'insieme delle attività finalizzate all'identificazione delle vulnerabilità contenente almeno:
   a) le modalità per l'identificazione delle vulnerabilità;
   b) la pianificazione delle attività per l'identificazione delle vulnerabilità.
2. Sono eseguite periodicamente le attività per identificare le vulnerabilità di cui al punto 1 e predisposte apposite relazioni che contengono almeno:
   a) la descrizione generale delle attività effettuate e gli esiti delle stesse;
   b) la descrizione delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza.

## ID.RA-5

**Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio.**

1. In accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4, esiste un documento aggiornato di valutazione del rischio (risk assessment) che comprende almeno:
   a) l'identificazione del rischio;
   b) l'analisi del rischio;
   c) la ponderazione del rischio;
2. La valutazione del rischio di cui al punto 1 è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti.

## ID.RA-6

**Sono identificate e prioritizzate le risposte al rischio.**

1. Esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorità.
2. Per il rischio residuo successivo al trattamento di cui al punto precedente, esiste un documento aggiornato che ne contiene la chiara descrizione. Il documento, con il quale si accetta il rischio residuo, è approvato da parte dei vertici del soggetto.

## ID.SC-2

**I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber.**

1. Esiste un elenco aggiornato dei fornitori e partner terzi affidatari di forniture di beni, sistemi e servizi di information and communication technology (ICT).

## PR.AC-1

**Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza.**

1. Salvo motivate e documentate ragioni di natura organizzativa o tecnica, le identità digitali sono individuali per gli utenti.
2. Le credenziali di accesso relative alle identità digitali sono robuste e aggiornate con una cadenza proporzionata ai privilegi dell'utenza.
3. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono verificate periodicamente le identità digitali e le credenziali di accesso, aggiornandole/revocandole in caso di variazioni (es. trasferimento o cessazione di personale).
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
6. In relazione all'amministrazione, verifica e revoca delle identità digitali e delle credenziali di accesso degli utenti, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV 1.

## PR.AC-3

**L'accesso remoto alle risorse è amministrato.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono monitorati gli accessi da remoto ed esiste un log degli accessi da remoto eseguiti.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono definite le attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso.
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione alla gestione degli accessi da remoto, esiste un documento aggiornato contenente almeno:
   a) l'elenco dei sistemi informativi e di rete ai quali è possibile accedere e le relative modalità;
   b) le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## PR.AC-4

**I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.**

1. Le identità digitali sono assegnate in accordo al principio del privilegio minimo e nel rispetto del principio di separazione delle funzioni.
2. È assicurata la completa distinzione tra utenze con e senza privilegi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.
3. Tutte le utenze con privilegi sono censite, approvate e utilizzate quando necessario registrando ogni accesso effettuato.
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3,
6. In relazione alla gestione dei diritti di accesso e alle relative autorizzazioni, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## PR.AT-1

**Tutti gli utenti sono informati e addestrati.**

1. Esiste un documento aggiornato che indica i contenuti della formazione fornita agli utenti e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato recante l'elenco degli utenti che hanno ricevuto la formazione e i relativi contenuti.

## PR.AT-2

**Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità.**

1. Esiste un documento aggiornato che indica i contenuti della formazione fornita agli utenti con privilegi e le modalità di verifica dell'acquisizione dei contenuti.
2. Esiste un registro aggiornato recante l'elenco degli utenti con privilegi che hanno ricevuto la formazione e i relativi contenuti.

## PR.DS-1

**I dati memorizzati sono protetti.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5 e ove applicabile, sono utilizzati sistemi di cifratura dei dati e in particolare per i dispositivi portatili e quelli removibili.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.

3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
4. In relazione alla memorizzazione e protezione dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## PR.IP-4

**I backup delle informazioni sono eseguiti, amministrati e verificati.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono effettuati periodicamente i backup dei dati.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è assicurata la riservatezza delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.
3. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.
4. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1, 2 e 3.
5. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1, 2 e 3.
6. In relazione al backup dei dati, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## PR.IP-9

**Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro.**

1. Esistono piani aggiornati di continuità operativa/disaster recovery redatti in accordo alle relative politiche e ai relativi processi di cui alla misura ID.GV-1.

## PR.IP-12

**Viene sviluppato e implementato un piano di gestione delle vulnerabilità.**

1. Le vulnerabilità emerse a seguito delle attività di cui al punto 2 della misura ID.RA-1 sono prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero accentando il rischio in accordo al piano di gestione del rischio informatico di cui alla misura ID.GV-4.
2. Le specifiche vulnerabilità segnalate puntualmente dall'Agenzia per la cybersicurezza nazionale sono risolte, senza ritardo e comunque non oltre quindici giorni dalla segnalazione, adottando gli interventi indicati dalla stessa Agenzia. Qualora dovessero sussistere motivate esigenze di natura tecnico-organizzativa che impediscano l'adozione, o comportino il differimento oltre il termine indicato degli interventi, viene data tempestiva comunicazione all'Agenzia.

3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione alla gestione delle vulnerabilità, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## PR.MA-1

**La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, i sistemi informativi e di rete sono aggiornati all'ultima versione raccomandata dal produttore. L'aggiornamento dei software ritenuti critici, fatte salve motivate esigenze di tempestività relative alla sicurezza, dovrà essere verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1.
4. In relazione alla manutenzione e riparazione dei sistemi informativi e di rete, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## PR.PT-4

**Le reti di comunicazione e controllo sono protette.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presente e aggiornati i sistemi perimetrali, quali firewall, anche a livello applicativo.
2. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione al punto 1.
3. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione al punto 1
4. In relazione alla protezione delle reti, esiste un documento aggiornato contenente almeno le procedure e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## DE.CM-1

**Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity.**

1. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono presenti e aggiornati sistemi di rilevamento delle intrusioni (intrusion detection systems - IDS).
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, è monitorato il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché

gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali al fine di rilevare gli eventi di cybersecurity.

3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione al monitoraggio degli eventi di sicurezza, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

### DE.CM-4:

**Il codice malevolo viene rilevato.**

1. Sono presenti e aggiornati sistemi di protezione delle postazioni terminali.
2. In accordo agli esiti dell'analisi del rischio di cui alla misura ID.RA-5, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.).
3. Le politiche di cybersecurity di cui alla misura ID.GV-1 includono le politiche in relazione ai punti 1 e 2.
4. I processi di cybersecurity di cui alla misura ID.GV-1 includono i processi in relazione ai punti 1 e 2.
5. In relazione al rilevamento del codice malevolo, esiste un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

### RS.RP-1

**Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente.**

1. Esiste un piano aggiornato di risposta agli incidenti all'interno del quale siano definiti almeno:
   a) le articolazioni preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche;
   b) le procedure per la notifica degli incidenti di cui all'articolo 1 della legge 28 giugno 2024, n. 90;
   c) le procedure adottate per il rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

### RS.AN-5

**Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza).**

1. In relazione alla gestione delle informazioni inerenti le vulnerabilità provenienti dal CSIRT Italia, nonché da eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento, esiste un documento aggiornato contenente almeno:

a) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni con particolare riferimento alle segnalazioni dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità a cui i soggetti risultano potenzialmente esposti di cui all'articolo 2 della legge 28 giugno 2024, n. 90;

b) le procedure, i ruoli, le responsabilità e gli strumenti tecnici per lo svolgimento delle attività di cui alla lettera a) nel rispetto delle politiche e nell'ambito dei processi di cui alla misura ID.GV-1.

## RC.RP-1

**Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity.**

1. Esiste un piano di ripristino che prevede almeno, le procedure necessarie al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidente di cybersecurity.
2. Il piano di ripristino prevede anche le procedure per il ripristino a seguito degli incidenti di cui all'articolo 1, comma 1 della legge 28 giugno 2024, n. 90.

# Appendice B: corrispondenza ambiti misure

## Legge 28 giugno 2024, n. 90

| AMBITO | CODICE MISURA |
|---|---|
| Sviluppo delle politiche e delle procedure di sicurezza delle informazioni. | ID.GV-1. |
| Produzione e aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico. | ID.GV-4, ID.RA-5, ID.RA-6, DE.CM-1, DE.CM-4. |
| Produzione e aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione. | ID.AM-6. |
| Produzione e aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione. | PR.AC-1, PR.AC-3, PR.AC-4, PR.AT-1, PR.AT-2, PR.IP-9, PR.DS-1, PR.MA-1, PR.PT-4. |
| Pianificazione e attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani per la gestione del rischio e per la sicurezza di dati, sistemi e infrastrutture. | ID.GV-4, ID.RA-5, ID.RA-6. |
| Monitoraggio e valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza. | ID.RA-1, ID.RA-5, PR.IP-12, RS.AN-5. |

## Direttiva del Presidente del Consiglio dei Ministri 29 dicembre 2023

| AMBITO | CODICE MISURA |
|---|---|
| Censimento dei sistemi, apparati, piattaforme, applicazioni e flussi di dati utilizzati nello svolgimento delle proprie attività, oltre che dei fornitori e/o partner terzi di sistemi informatici, componenti e servizi utilizzati. | ID.AM-1, ID.AM-2, ID.AM-3, ID.SC-2. |
| Documento in cui siano definiti ruoli e responsabilità inerenti alla cybersicurezza, sia del personale interno, sia di eventuali terze parti che supportano l'amministrazione, comprensivo dell'individuazione, tra il proprio personale, di un incaricato per la cybersicurezza (quale punto di contatto cyber ai fini delle comunicazioni e del necessario raccordo con l'ACN) e di un referente tecnico per la cybersicurezza (da identificarsi tra il personale responsabile della gestione operativa dei sistemi IT). | ID.AM-6. |
| Piani per la gestione delle vulnerabilità, dei backup dei dati necessari per l'esercizio delle proprie funzioni essenziali, nonché del ciclo di vita dei sistemi, delle identità e dei relativi permessi. | PR.AC-1, PR.AC-3, PR.AC-4, PR.MA-1, PR.IP-4, PR.IP-12, RS.AN-5. |
| Piano di risposta in caso di incidente, nel quale vengano puntualmente definite le articolazioni interne che - in stretto raccordo con l'incaricato per la cybersicurezza (ove non direttamente dipendenti dallo stesso) - sono preposte all'attuazione del piano, definendone le competenze decisionali, finanziarie e tecniche, onde adeguatamente fronteggiare un incidente cibernetico. | RS.RP-1, RC.RP-1. |

# Appendice C: glossario

## Articolazioni del soggetto

Unità organizzative del soggetto che compongono la struttura gerarchica dell'organigramma del soggetto (quali ad esempio, dipartimenti, direzioni generali, uffici, unità, ecc.).

## Attori interni al soggetto

Figure del soggetto deputate alla gestione della sicurezza dei sistemi informativi e di rete come, ad esempio, quelle operanti all'interno della struttura di cui all'articolo 8, comma 1 della Lelle 28 giugno 2024, n. 90.

## Catena di approvvigionamento

Insieme di individui, organizzazioni, risorse e attività coinvolte nella creazione e vendita di un prodotto o un servizio.

## Flusso informativo

Insieme di dati scambiati in una rete tra una sorgente e un destinatario. Possono essere rappresentati tramite le connessioni, in ingresso o in uscita, e i protocolli tramite i quali avvengono le comunicazioni. Ad esempio, il flusso informativo conseguente alla navigazione Internet è una connessione in uscita su protocollo HTTPS, il flusso informativo conseguente alla ricezione di mail è un flusso informativo in ingresso su protocollo SMTP.

## Identità digitale

Insieme di dati e informazioni che identificano univocamente un'entità (persone, sistemi e servizi informatici, ecc.). Per accedere a un sistema, l'identità digitale deve essere prima autenticata (verifica dell'identità) e poi autorizzata (assegnazione del livello di accesso alle risorse informatiche). Le identità digitali hanno quindi associate *credenziali di accesso* (costituite, ad esempio, da username e password, certificati digitali, ecc.) per l'autenticazione e *utenze* (o *account*) per l'autorizzazione.

## Intrusion Detection System (IDS)

Sistemi di sicurezza che monitorano e analizzano gli eventi sui sistemi informativi e di rete con l'obiettivo di rilevare tentativi di accesso non autorizzato.

## Manutenzione dei sistemi informativi e di rete

Attività poste in essere per prevenire guasti e malfunzionamenti o per ripristinare le funzionalità dei sistemi informativi e di rete.

### Organizzazione di cybersecurity

Insieme delle articolazioni preposte al governo (o governance) e alla gestione della sicurezza dei sistemi informativi e di rete del soggetto. Questa comprende, altresì, le articolazioni di eventuali terze parti coinvolte nelle attività di cybersecurity.

### Piano per la gestione del rischio informatico

Documento comprensivo di linee di indirizzo, obiettivi e conseguenti azioni, definito dal soggetto per identificare, valutare e trattare il rischio informatico.

### Piano programmatico per la sicurezza di dati, sistemi e infrastrutture

Documento che esplicita le linee strategiche, gli obiettivi prefissati e le conseguenti attività da porre in essere in merito alla sicurezza di dati, sistemi e infrastrutture del soggetto.

### Politiche di cybersecurity

Insieme di regole e disposizioni definite da un'organizzazione, e approvate dai vertici per salvaguardare la sicurezza dei propri sistemi informativi e di rete. Le politiche guidano le *decisioni* e sono attuate tramite processi, procedure, standard e linee guida definiti in accordo e nel rispetto delle politiche.

### Processo di cybersecurity

Fasi e attività relazionate tra loro ed eseguite per raggiungere specifici obiettivi in un determinato ambito della cybersecurity, come ad esempio la risposta agli incidenti, la sicurezza dei dati e la gestione delle vulnerabilità.

### Referente per la cybersecurity

Il referente per la cybersicurezza di cui all'articolo 8, comma 2, della legge 28 giugno 2024, n. 90.

### RTO (Recovery Time Object)

Intervallo di tempo che intercorre tra il verificarsi di un evento di disastro e il completo ripristino dell'operatività dei sistemi informativi e di rete.

### RPO (Recovery Time Object)

Intervallo di tempo che intercorre tra quando il dato viene generato e quando può essere recuperato con successo (ovvero il tempo trascorso dall'ultimo backup disponibile), indica la quantità massima di dati che si possono perdere a seguito di un evento imprevisto.

## Sistemi di protezione delle postazioni terminali

Soluzioni di sicurezza che proteggono le postazioni terminali (o endpoint) dagli attacchi come ad esempio gli antivirus, antimalware, gli HIPS/HIDS (Host Intrusion Prevention System, Host Intrusion Detection System).

## Sistema informativo e di rete

1. Una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;
2. Qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;
3. I dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione.

## Sistemi perimetrali

Sistemi di sicurezza a protezione di due o più reti, tipicamente sono situati al confine tra reti private e reti pubbliche per controllano il traffico in ingresso e in uscita dalle reti. Esempi di sistemi perimetrali sono firewall, reverse proxy, secure email gateway, ecc.

## Struttura

La struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90.

## Soggetti

I soggetti individuati dall'articolo 1, comma 1, della legge 28 giugno 2024, n. 90.

## Terze parti

Operatori pubblici e/o privati caratterizzati da una dipendenza esterna con il soggetto, come ad esempio i fornitori di beni e servizi informatici.