FUNCTION	CATEGORY	CATEGORY DESCRIPTION	ID SUB-CATEGORY	SUB-CATEGORY	ID REQUISITO	REQUISITO	SOGGETTO ESSENZIALE	Applicabile ai sistemi informativi e di rete rilevanti
GOVERN	**Contesto organizzativo**	Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso1.	**GV.OC-04**	Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.	**GV.OC-04.1**	È mantenuto un **elenco** aggiornato dei **sistemi informativi e di rete rilevanti**.	X	-
GOVERN	**Strategia di gestione del rischio**	Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.	**GV.RM-03**	Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.	**GV.RM-03.1**	Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un **piano di gestione dei rischi per la sicurezza informatica** per identificare, analizzare, valutare, trattare e monitorare i rischi.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-02**	I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.	**GV.RR-02.1**	È definita, approvata dagli organi di amministrazione e direttivi, e resa nota alle articolazioni competenti del soggetto NIS, l'**organizzazione per la sicurezza informatica** e ne sono stabiliti **ruoli e responsabilità**.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-02**	I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.	**GV.RR-02.2**	È mantenuto un **elenco** aggiornato del **personale** dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità ed è reso noto alle articolazioni competenti del soggetto NIS.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-02**	I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.	**GV.RR-02.3**	All'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, sono **inclusi il punto di contatto, e almeno un suo sostituto**, di cui alla determina adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-02**	I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.	**GV.RR-02.4**	I **ruoli e le responsabilità** di cui al punto 1 sono **riesaminati** e, se opportuno, aggiornati periodicamente e comunque almeno **ogni due anni**, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-04**	La cybersecurity è inclusa nelle pratiche delle risorse umane.	**GV.RR-04.1**	*Per almeno i sistemi informativi e di rete rilevanti*, il personale autorizzato ad accedervi è individuato previa **valutazione dell'esperienza**, **capacità** e **affidabilità** e deve fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.	X	X
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-04**	La cybersecurity è inclusa nelle pratiche delle risorse umane.	**GV.RR-04.2**	Gli **amministratori di sistema** dei sistemi informativi e di rete sono individuati previa **valutazione dell'esperienza, capacità e affidabilità** e devono fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-04**	La cybersecurity è inclusa nelle pratiche delle risorse umane.	**GV.RR-04.3**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1 e 2.	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-04**	La cybersecurity è inclusa nelle pratiche delle risorse umane.	**GV.RR-04.4**	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono definiti a livello **contrattuale** gli eventuali **obblighi**, in materia di sicurezza informatica, che rimangono **validi dopo la cessazione o la modifica del rapporto di lavoro** dei dipendenti del soggetto NIS (ad esempio prevedendo clausole in materia di **riservatezza**).	X	-
GOVERN	**Ruoli, responsabilità e correlati poteri**	I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.	**GV.RR-04**	La cybersecurity è inclusa nelle pratiche delle risorse umane.	**GV.RR-04.5**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 4.	X	-

GOVERN	**Politica**	La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.	**GV.PO-01**	La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.	**GV.PO-01.1**	Sono adottate e documentate **politiche di sicurezza** informatica per almeno i seguenti ambiti: a) gestione del rischio; b) ruoli e responsabilità; c) affidabilità delle risorse umane; d) conformità e audit di sicurezza; e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento; f) gestione degli asset; g) gestione delle vulnerabilità; h) continuità operativa, ripristino in caso di disastro e gestione delle crisi; i) gestione dell'autenticazione, delle identità digitali e del controllo accessi; j) sicurezza fisica; k) formazione del personale e consapevolezza; l) sicurezza dei dati; m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete; n) protezione delle reti e delle comunicazioni; o) monitoraggio degli eventi di sicurezza; p) risposta agli incidenti e ripristino.	X	-
GOVERN	**Politica**	La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.	**GV.PO-01**	La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.	**GV.PO-01.2**	Per gli ambiti di cui al punto 1 sono incluse **almeno le politiche in relazione ai requisiti indicati nella tabella 1** in appendice al presente allegato.	X	-
GOVERN	**Politica**	La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.	**GV.PO-01**	La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.	**GV.PO-01.3**	Le politiche di cui al punto 1 sono **approvate** dagli **organi di amministrazione e direttivi**.	X	-
GOVERN	**Politica**	La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.	**GV.PO-02**	La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.	**GV.PO-02.1**	Le politiche di cui alla misura GV.PO-01 sono **riesaminate** e, se opportuno, aggiornate periodicamente e comunque almeno con **cadenza annuale**, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.	X	-
GOVERN	**Politica**	La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.	**GV.PO-02**	La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.	**GV.PO-02.2**	Ai fini del riesame di cui al punto 1, è **verificata almeno la conformità delle politiche di cui alla misura GV.PO-01** alla normativa in materia di sicurezza informatica.	X	-
GOVERN	**Politica**	La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.	**GV.PO-02**	La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.	**GV.PO-02.3**	È mantenuto un **registro** aggiornato contenente gli **esiti del riesame** di cui al punto 1.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-01**	Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.	**GV.SC-01.1**	In merito all'**affidamento di forniture** con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'allegato I.1, articolo 1, comma 1, lettera i), del decreto legislativo 31 marzo 2023, n. 36, sono previsti: a) il **coinvolgimento dell'organizzazione** per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura; b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di **requisiti di sicurezza sulla fornitura** coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-01**	Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.	**GV.SC-01.2**	Per i **requisiti di sicurezza** di cui al punto 1, lettera b), sono considerati, ove applicabile, almeno i seguenti ambiti: a) **affidabilità dei fornitori**, tenendo conto almeno delle loro eventuali vulnerabilità specifiche, della qualità complessiva dei loro prodotti e delle pratiche di sicurezza informatica, specie con riguardo all'oggetto della fornitura, della capacità di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo, nonché, ove applicabile, dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS; b) ruoli e responsabilità nell'ambito della fornitura; c) affidabilità delle risorse umane; d) conformità e audit di sicurezza; e) gestione delle **vulnerabilità**; f) continuità operativa e ripristino in caso di disastro; g) gestione dell'autenticazione, delle identità digitali e del controllo accessi; h) sicurezza fisica; i) formazione del personale e consapevolezza; j) sicurezza dei dati; k) protezione delle reti e delle comunicazioni; l) monitoraggio degli eventi di sicurezza ivi inclusi gli accessi e le attività effettuate; m) gestione e segnalazione degli incidenti; n) sviluppo sicuro del codice e sicurezza fin dalla progettazione e per impostazione predefinita; o) manutenzione ordinaria ed evolutiva ivi inclusi gli aggiornamenti di sicurezza; p) dismissione della fornitura ivi compresa la restituzione e la cancellazione dei dati; q) subappalto, subfornitura o relativi potenziali requisiti di sicurezza lungo la catena di fornitura.	X	-

GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-02**	I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.	**GV.SC-02.1**	Nell'ambito dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02, sono definiti e resi noti alle articolazioni competenti del soggetto NIS gli eventuali **ruoli e responsabilità** in materia di sicurezza informatica **assegnati al personale delle terze parti**.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-03**	I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.	**GV.SC-02.2**	Il **personale** di cui al punto 1 avente specifici ruoli e responsabilità è incluso nell'**elenco di cui al punto 2 della misura GV.RR-02**.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-04**	I fornitori sono noti e prioritizzati in base alla criticità.	**GV.SC-04.1**	1. È mantenuto un **inventario** aggiornato dei **fornitori**, le cui forniture hanno un **potenziale impatto sulla sicurezza dei sistemi informativi e di rete**, che comprende almeno: a) gli estremi di contatto del referente della fornitura; b) la tipologia di fornitura.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-05**	I requisiti per affrontare i rischi di cybersecurity nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati nei contratti e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.	**GV.SC-05.1**	Fatte salve motivate e documentate ragioni normative o tecniche, i requisiti di sicurezza di cui alla misura GV.SC-01, punto 1, lettera b) sono inseriti nelle **richieste di offerta, bandi di gara, contratti, accordi e convenzioni** relativi alle forniture con potenziali impatto sulla sicurezza dei sistemi informativi e di rete.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-07**	I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.	**GV.SC-07.1**	Nell'ambito della **valutazione del rischio** di cui alla misura ID.RA-05, è valutato e documentato il **rischio associato alle forniture**. A tal fine, sono valutati almeno: a) il **livello di accesso del fornitore** ai sistemi informativi e di rete del soggetto NIS; b) l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità; c) l'impatto di una grave **interruzione** della fornitura; d) i tempi e i costi di **ripristino** in caso di indisponibilità dei servizi; e) i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete.	X	-
GOVERN	**Gestione del rischio di cybersecurity della catena di approvvigionamento**	I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.	**GV.SC-07**	I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.	**GV.SC-07.2**	È **verificata periodicamente** e documentata la **conformità** delle **forniture** ai requisiti di cui alla misura GV.SC-05.	X	-
IDENTIFY	**Gestione degli asset**	Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.	**ID.AM-01**	Sono mantenuti gli inventari dell'hardware gestito dall'organizzazione.	**ID.AM-01.1**	È mantenuto un **inventario** aggiornato degli apparati fisici (**hardware**) che compongono i sistemi informativi e di rete, ivi inclusi i dispositivi IT, IoT, OT e mobili, approvati da attori interni al soggetto NIS.	X	-
IDENTIFY	**Gestione degli asset**	Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.	**ID.AM-02**	Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione.	**ID.AM-02.1**	È mantenuto un **inventario** aggiornato dei servizi, dei sistemi e delle applicazioni **software** che compongono i sistemi informativi e di rete, ivi incluse le applicazioni commerciali, open-source e custom, anche ccessibili tramite API, approvati da attori interni al soggetto NIS.	X	-
IDENTIFY	**Gestione degli asset**	Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.	**ID.AM-03**	Sono mantenute le rappresentazioni delle comunicazioni di rete, dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione.	**ID.AM-03.1**	È mantenuto un **inventario** aggiornato dei **flussi di rete** tra i sistemi informativi e di rete del soggetto NIS e l'esterno, approvati da attori interni al soggetto NIS.	X	-
IDENTIFY	**Gestione degli asset**	Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.	**ID.AM-04**	Sono mantenuti gli inventari dei servizi erogati dai fornitori.	**ID.AM-04.1**	È mantenuto un **inventario** aggiornato dei **servizi informatici erogati dai fornitori**, ivi inclusi i servizi **cloud**.	X	-

IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-01**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-01.1**	Le informazioni di cui al punto 1 della misura ID.RA-08 sono utilizzate per identificare eventuali vulnerabilità sui i sistemi informativi e di rete.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-01**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-01.2**	Per almeno i sistemi informativi e di rete rilevanti, in accordo al piano di gestione delle vulnerabilità di cui alla misura ID.RA-08, fatte salve motivate e documentate ragioni normative o tecniche, sono eseguite **periodicamente** e comunque **prima della loro messa in esercizio**, attività per l'identificazione delle vulnerabilità che comprendano almeno **vulnerability assessment e/o penetration test**.	X	X
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-01**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-01.3**	Le attività di cui al punto 2 sono **documentate** tramite 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.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-05**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-05.1**	In accordo al piano di gestione dei rischi per la sicurezza informatica di cui alla misura GV.RM-03, è eseguita e documentata la **valutazione del rischio** posto alla sicurezza dei **sistemi informativi e di rete**, anche con riferimento alle eventuali **dipendenze da fornitori e partner terzi**, che comprende almeno: a) l'identificazione del rischio; b) l'analisi del rischio; c) la ponderazione del rischio.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-05**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-05.2**	La **valutazione del rischio** di cui al punto 1 è eseguita a intervalli pianificati e comunque almeno **ogni due anni**, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-05**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-05.3**	La valutazione del rischio cui al punto 1 è **approvata** dagli **organi di amministrazione e direttivi**.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-05**	Le vulnerabilità negli asset sono identificate, confermate e registrate.	**ID.RA-05.4**	La **valutazione del rischio** di cui al punto 1 è effettuata considerando almeno le **minacce interne ed esterne**, le **vulnerabilità** non risolte e gli **impatti** conseguenti ad eventuali incidenti.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-06**	Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate.	**ID.RA-06.1**	È definito, documentato, eseguito e monitorato un **piano di trattamento del rischio** che comprende almeno: a) le **opzioni di trattamento** e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità; b) le articolazioni competenti per l'**attuazione delle misure di trattamento** dei rischi e le tempistiche per tale attuazione; c) la descrizione e le ragioni che giustificano l'**accettazione** di eventuali rischi residui al trattamento.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-06**	Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate.	**ID.RA-06.2**	Qualora per motivate e documentate ragioni normative o tecniche **non siano attuati i requisiti di cui alla tabella 2** in appendice al presente allegato, sono adottate, ove applicabile, **misure di mitigazione** compensative e il piano di cui al punto 1 include la descrizione di tali misure e dell'eventuale rischio residuo.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-06**	Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate.	**ID.RA-06.3**	Il **piano** di cui al punto 1, ivi compresa **l'accettazione** di eventuali rischi residui, è **approvato** dagli **organi di amministrazione e direttivi**.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-08**	Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.	**ID.RA-08.1**	Sono **monitorati** almeno i canali di comunicazione del **CSIRT** Italia, nonché di eventuali **CERT** e Information Sharing & Analysis Centre (**ISAC**) settoriali, al fine di acquisire, analizzare e rispondere alle informazioni sulle vulnerabilità.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-08**	Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.	**ID.RA-08.2**	Le **vulnerabilità**, ivi comprese quelle identificate ai sensi della misura ID.RA-01, sono **prontamente risolte** attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, **ovvero accettando** e documentando il rischio in accordo al piano di trattamento del rischio informatico di cui alla misura ID.RA-06.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-08**	Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.	**ID.RA-08.3**	È definito, attuato, aggiornato e documentato un piano di gestione delle vulnerabilità che comprende almeno: a) le modalità per **l'identificazione** delle vulnerabilità di cui alla misura ID.RA-01 e la relativa pianificazione delle attività; b) le modalità per **monitorare**, ricevere, analizzare e rispondere alle **informazioni sulle vulnerabilità**; c) le **procedure, i ruoli, le responsabilità** per lo svolgimento delle attività di cui alle lettere a) e b).	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-08**	Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.	**ID.RA-08.4**	Il **piano** di cui al punto 3 è approvato dagli **organi di amministrazione e direttivi**.	X	-
IDENTIFY	**Valutazione del rischio (Risk Assessment)**	È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.	**ID.RA-08**	Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.	**ID.RA-08.5**	Ai fini di cui al punto 1, sono **monitorati** anche i **canali dei fornitori del software** ritenuto critico.	X	-
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-01**	Sono identificati miglioramenti in esito alle valutazioni.	**ID.IM-01.1**	In accordo agli esiti del riesame di cui al punto 1 della misura GV.PO-02, è definito, attuato, documentato e approvato dagli organi di amministrazioni e direttivi un **piano di adeguamento che identifichi gli interventi necessari** ad assicurare l'attuazione delle politiche di sicurezza.	X	-
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-01**	Sono identificati miglioramenti in esito alle valutazioni.	**ID.IM-01.2**	Gli organi di amministrazione e direttivi sono informati mediante **apposite relazioni** periodiche sugli esiti dei piani di cui al punto 1.	X	-
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-01**	Sono identificati miglioramenti in esito alle valutazioni.	**ID.IM-01.3**	È definito, attuato, aggiornato e documentato un **piano per la valutazione dell'efficacia delle misure** di gestione del rischio per la sicurezza informatica che comprenda l'indicazione delle misure da valutare e i relativi metodi di valutazione.	X	-

IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-01**	Sono identificati miglioramenti in esito alle valutazioni.	**ID.IM-01.4**	Gli organi di amministrazione e direttivi sono informati mediante **apposite relazioni** periodiche sul piano di valutazione dell'efficacia di cui al punto 3.	X	-
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-04**	I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.	**ID.IM-04.1**	Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un **piano di continuità operativa**, che comprende almeno: a) le finalità e l'ambito di applicazione; b) i ruoli e le responsabilità; c) i contatti principali e i canali di comunicazione (interni ed esterni); d) le condizioni per l'attivazione e la disattivazione del piano; e) le risorse necessarie, ivi compresi i backup e le ridondanze.	X	X
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-04**	I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.	**ID.IM-04.2**	Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un **piano di ripristino in caso di disastro**, che comprende almeno: a) le finalità e l'ambito di applicazione; b) i ruoli e le responsabilità; c) i contatti principali e i canali di comunicazione (interni ed esterni); d) le condizioni per l'attivazione e la disattivazione del piano; e) le risorse necessarie, ivi compresi i backup e le ridondanze; f) l'ordine di ripristino delle operazioni; g) le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino.	X	X
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-04**	I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.	**ID.IM-04.3**	Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un **piano per la gestione delle crisi** che comprende almeno: a) i ruoli e responsabilità del personale e, se opportuno, dei fornitori, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le procedure specifiche da seguire; b) le modalità di comunicazione tra i soggetti e le autorità competenti.	X	X
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-04**	I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.	**ID.IM-04.4**	I piani di cui ai punti 1, 2 e 3 sono **approvati** dagli **organi di amministrazione e direttivi**.	X	-
IDENTIFY	**Miglioramento**	I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.	**ID.IM-04**	I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.	**ID.IM-04.5**	I **piani** di cui ai punti 1, 2 e 3 sono riesaminati e, se opportuno, **aggiornati** periodicamente e comunque almeno **ogni due anni**, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-01**	Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.	**PR.AA-01.1**	**Tutte le utenze**, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono **censite**, **approvate** da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-01**	Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.	**PR.AA-01.2**	Le **credenziali** (ad esempio nome utente e password) relative alle utenze sono **robuste** e **aggiornate** in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-01**	Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.	**PR.AA-01.3**	Per almeno i sistemi informativi e di rete rilevanti, sono **verificate periodicamente le utenze e le relative autorizzazioni**, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).	X	X
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-01**	Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.	**PR.AA-01.4**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1, 2 e 3.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-03**	Utenti, servizi e hardware sono autenticati.	**PR.AA-03.1**	Le **modalità di autenticazione** delle utenze per accedere ai sistemi informativi e di rete sono **commisurate al rischio**. A tal fine sono valutati almeno i rischi connessi: a) ai privilegi delle utenze; b) alla criticità dei sistemi informativi e di rete; c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-03**	Utenti, servizi e hardware sono autenticati.	**PR.AA-03.2**	Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità di **autenticazione multifattore**.	X	X
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-03**	Utenti, servizi e hardware sono autenticati.	**PR.AA-03.3**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1 e 2.	X	-

PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-05**	I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.	**PR.AA-05.1**	I permessi sono assegnati alle utenze in accordo ai **principi del minimo privilegio e della separazione delle funzioni**, tenuto anche conto della necessità di conoscere (need to know).	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-05**	I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.	**PR.AA-05.2**	È assicurata la completa **distinzione** tra **utenze con e senza privilegi** amministrativi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-05**	I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.	**PR.AA-05.3**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1e 2.	X	-
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-06**	L'accesso fisico agli asset è gestito, monitorato e applicato in misura appropriata al rischio.	**PR.AA-06.1**	Per almeno i sistemi informativi e di rete rilevanti, l'**accesso fisico è protetto**.	X	X
PROTECT	**Gestione delle identità, autenticazione e controllo degli accessi**	L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.	**PR.AA-06**	L'accesso fisico agli asset è gestito, monitorato e applicato in misura appropriata al rischio.	**PR.AA-06.2**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 1.	X	-
PROTECT	**Consapevolezza e formazione**	Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.	**PR.AT-01**	Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.	**PR.AT-01.1**	È definito, attuato, aggiornato e documentato un **piano di formazione** in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi, che comprende almeno: a) la **pianificazione** delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita; b) le eventuali **modalità di verifica** dell'acquisizione dei contenuti.	X	-
PROTECT	**Consapevolezza e formazione**	Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.	**PR.AT-01**	Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.	**PR.AT-01.2**	Il piano di formazione di cui al punto 1 è **approvato dagli organi di amministrazione e direttivi**.	X	-
PROTECT	**Consapevolezza e formazione**	Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.	**PR.AT-01**	Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.	**PR.AT-01.3**	È mantenuto un **registro** aggiornato recante l'elenco dei **dipendenti** che hanno **ricevuto la formazione** di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.	X	-
PROTECT	**Consapevolezza e formazione**	Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.	**PR.AT-02**	Gli individui che ricoprono ruoli specializzati sono sensibilizzati e formati in modo da possedere le conoscenze e le competenze per svolgere i pertinenti compiti tenendo conto dei rischi di cybersecurity.	**PR.AT-02.1**	Il **piano** di cui alla misura PR.AT-01 prevede una **formazione** dedicata al **personale con ruoli specializzati**, ossia che richiedono una serie di capacità e competenze attinenti alla sicurezza, ivi compresi gli amministratori di sistema, che comprende almeno: a) le **istruzioni relative alla configurazione e al funzionamento** sicuri dei sistemi informativi e di rete; b) le informazioni sulle **minacce** informatiche note; c) le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.	X	-
PROTECT	**Consapevolezza e formazione**	Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.	**PR.AT-02**	Gli individui che ricoprono ruoli specializzati sono sensibilizzati e formati in modo da possedere le conoscenze e le competenze per svolgere i pertinenti compiti tenendo conto dei rischi di cybersecurity.	**PR.AT-02.2**	È mantenuto un **registro** aggiornato recante l'elenco dei **dipendenti** che hanno **ricevuto la formazione** di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.	X	-
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-01**	La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette.	**PR.DS-01.1**	Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, i **dati memorizzati** sui dispositivi portatili, ivi inclusi laptop, smartphone e tablet, e sui supporti removibili, sono **cifrati** con protocolli e algoritmi allo stato dell'arte e considerati sicuri.	X	X
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-01**	La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette.	**PR.DS-01.2**	Fatte salve e documentate ragioni normative o tecniche, è **disabilitata l'auto esecuzione** dei supporti rimovibili ed è effettuata la loro **scansione** al fine di rilevare codici malevoli prima che siano utilizzati nei sistemi informativi e di rete.	X	-
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-01**	La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette.	**PR.DS-01.3**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1 e 2.	X	-

PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-02**	La riservatezza, l'integrità e la disponibilità dei dati in transito (data-in-transit) sono protette.	**PR.DS-02.1**	Per almeno i sistemi informativi e di rete rilevanti, ivi inclusi quelli di comunicazione vocale, video e testuale, e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05 fatte salve motivate e documentate ragioni normative o tecniche, sono utilizzati, per la **trasmissione dei dati** da e verso l'esterno del soggetto NIS, **protocolli** e **algoritmi di cifratura** allo stato dell'arte e considerati sicuri.	X	X
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-02**	La riservatezza, l'integrità e la disponibilità dei dati in transito (data-in-transit) sono protette.	**PR.DS-02.2**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 1.	X	-
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-11**	I backup dei dati sono creati, protetti, mantenuti e verificati.	**PR.DS-11.1**	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati **periodicamente i backup** dei **dati** e delle **configurazioni** e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate **copie di backup offline**.	X	-
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-11**	I backup dei dati sono creati, protetti, mantenuti e verificati.	**PR.DS-11.2**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 1.	X	-
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-11**	I backup dei dati sono creati, protetti, mantenuti e verificati.	**PR.DS-11.3**	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la **riservatezza** e **l'integrità** delle informazioni contenute nei **backup** mediante adeguata **protezione fisica** dei supporti ovvero mediante **cifratura**.	X	X
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-11**	I backup dei dati sono creati, protetti, mantenuti e verificati.	**PR.DS-11.4**	Per almeno i sistemi informativi e di rete rilevanti, è **verificata** periodicamente l'utilizzabilità dei **backup** effettuati mediante **test di ripristino**.	X	X
PROTECT	**Sicurezza dei dati**	I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.	**PR.DS-11**	I backup dei dati sono creati, protetti, mantenuti e verificati.	**PR.DS-11.5**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 3 e 4.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-01**	Sono stabilite e applicate pratiche di gestione della configurazione.	**PR.PS-01.1**	Per almeno i sistemi informativi e di rete rilevanti, sono definite, e documentate in un elenco aggiornato, le loro **configurazioni di riferimento sicure (hardened)**.	X	X
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-01**	Sono stabilite e applicate pratiche di gestione della configurazione.	**PR.PS-01.2**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 1.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-02**	Il software è mantenuto, sostituito e rimosso in base al rischio	**PR.PS-02.1**	Fatte salve motivate e documentate ragioni normative o tecniche, è installato esclusivamente **software**, ivi compresi i **sistemi operativi**, per il quale è garantita la **disponibilità di aggiornamenti di sicurezza**.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-02**	Il software è mantenuto, sostituito e rimosso in base al rischio	**PR.PS-02.2**	Fatte salve motivate e documentate ragioni normative o tecniche, sono **installati**, senza ingiustificato ritardo, gli **ultimi aggiornamenti di sicurezza rilasciati** dal produttore in coerenza con il piano di gestione delle vulnerabilità di cui alla misura ID.RA-08.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-02**	Il software è mantenuto, sostituito e rimosso in base al rischio	**PR.PS-02.3**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1e 2.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-02**	Il software è mantenuto, sostituito e rimosso in base al rischio	**PR.PS-02.4**	Fatte salve motivate e documentate ragioni normative o tecniche e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, l'**aggiornamento del software ritenuto critico** è verificato in **ambiente di test prima dell'effettivo impiego** in **ambiente operativo**.	X	-

PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-02**	Il software è mantenuto, sostituito e rimosso in base al rischio	**PR.PS-02.5**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 4.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-03**	L'hardware è mantenuto, sostituito e rimosso in base al rischio.	**PR.PS-03.1**	Per almeno i sistemi informativi e di rete rilevanti, sono adottate e documentate procedure per il **trasferimento fisico e la dismissione di dispositivi** atti alla memorizzazione di dati in modo sicuro.	X	X
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-03**	L'hardware è mantenuto, sostituito e rimosso in base al rischio.	**PR.PS-03.2**	Per almeno i sistemi informativi e di rete rilevanti, sono mantenuti uno o più **registri** delle **manutenzioni** effettuate **sull'hardware**.	X	X
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-04**	I registri di log sono generati e resi disponibili per il monitoraggio continuo.	**PR.PS-04.1**	Tutti gli **accessi** eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi sono **registrati**.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-04**	I registri di log sono generati e resi disponibili per il monitoraggio continuo.	**PR.PS-04.2**	Per almeno i sistemi informativi e di rete rilevanti, sono **conservati** in modo sicuro, e **possibilmente centralizzato**, almeno i **log necessari ai fini del monitoraggio** degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto 1.	X	X
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-04**	I registri di log sono generati e resi disponibili per il monitoraggio continuo.	**PR.PS-04.3**	In accordo agli esiti della valutazione rischio di cui alla misura ID.RA-05, sono definite e **documentate** le **tempistiche di conservazione dei log** di cui al punto 2.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-04**	I registri di log sono generati e resi disponibili per il monitoraggio continuo.	**PR.PS-04.4**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1 e 2.	X	-
PROTECT	**Sicurezza delle piattaforme**	L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.	**PR.PS-06**	Le pratiche di sviluppo sicuro del software sono integrate e le loro prestazioni sono monitorate durante l'intero ciclo di vita del software.	**PR.PS-06.1**	Sono adottate e documentate pratiche di **sviluppo sicuro del codice** nello sviluppo del software.	X	-
PROTECT	**Resilienza dell'infrastruttura tecnologica**	Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.	**PR.IR-01**	Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.	**PR.IR-01.1**	Per almeno i sistemi informativi e di rete rilevanti, sono definite e documentate le eventuali **attività consentite da remoto** e implementate adeguate misure di sicurezza per l'accesso.	X	X
PROTECT	**Resilienza dell'infrastruttura tecnologica**	Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.	**PR.IR-01**	Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.	**PR.IR-01.2**	È mantenuto un **elenco** aggiornato dei sistemi informativi e di rete ai quali è possibile **accedere da remoto** con la descrizione delle relative modalità di accesso.	X	-
PROTECT	**Resilienza dell'infrastruttura tecnologica**	Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.	**PR.IR-01**	Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.	**PR.IR-01.3**	Sono presenti, aggiornati, mantenuti e configurati i sistemi perimetrali, quali **firewall**.	X	-
PROTECT	**Resilienza dell'infrastruttura tecnologica**	Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.	**PR.IR-01**	Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.	**PR.IR-01.4**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1, 2 e 3.	X	-
PROTECT	**Resilienza dell'infrastruttura tecnologica**	Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.	**PR.IR-03**	Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.	**PR.IR-03.1**	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono utilizzati **sistemi di comunicazione di emergenza** protetti.	X	-

PROTECT	**Resilienza dell'infrastruttura tecnologica**	Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.	**PR.IR-03**	Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.	**PR.IR-03.2**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 1.	X	-
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.1**	Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato **strumenti tecnici per rilevare tempestivamente gli incidenti** significativi.	X	X
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.2**	Sono definiti e documentati i **livelli di servizio attesi** (SL) dei servizi e delle attività del soggetto NIS anche ai fini di rilevare tempestivamente gli incidenti significativi.	X	-
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.3**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 1 e 2.	X	-
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.4**	Per almeno i sistemi informativi e di rete rilevanti, sono utilizzati strumenti di **analisi e filtraggio sul flusso di traffico in ingresso** (ivi inclusa la **posta elettronica**).	X	X
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.5**	Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono **monitorati gli accessi da remoto**, le **attività** dei **sistemi perimetrali** (ad esempio router e firewall), gli **eventi amministrativi** di rilievo, nonché gli **accessi eseguiti o falliti alle risorse di rete**, alle **postazioni terminali** e agli **applicativi** al fine di rilevare gli eventi di sicurezza informatica.	X	X
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.6**	Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono definiti, **monitorati** e documentati parametri quali-quantitativi per **rilevare** gli **accessi non autorizzati o con abuso dei privilegi** concessi.	X	X
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-01**	Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-01.7**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione ai punti 4, 5 e 6.	X	-
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-09**	L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-09.1**	Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, **sistemi di protezione** delle postazioni terminali per il rilevamento del **codice malevolo**.	X	-
DETECT	**Monitoraggio continuo**	Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.	**DE.CM-09**	L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.	**DE.CM-09.2**	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e **documentate le procedure** in relazione al punto 1.	X	-
RESPOND	**Gestione degli incidenti**	Le risposte agli incidenti di cybersecurity rilevati sono gestite.	**RS.MA-01**	Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.	**RS.MA-01.1**	È definito, attuato, aggiornato e documentato un **piano per la gestione degli incidenti** di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS, che comprende almeno: a) le **fasi e le procedure di gestione e notifica degli incident**i con l'indicazione dei relativi ruoli e delle responsabilità; b) le procedure per la predisposizione e la trasmissione delle **relazioni** di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS; c) le informazioni di **contatto** per la segnalazione degli incidenti; d) le **modalità di comunicazione interna**, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna; e) la **reportistica da utilizzare** per la documentazione dell'incidente.	X	-
RESPOND	**Gestione degli incidenti**	Le risposte agli incidenti di cybersecurity rilevati sono gestite.	**RS.MA-01**	Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.	**RS.MA-01.2**	Il piano di cui al punto 1 è **approvato** dagli **organi di amministrazione e direttivi**.	X	-
RESPOND	**Gestione degli incidenti**	Le risposte agli incidenti di cybersecurity rilevati sono gestite.	**RS.MA-01**	Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.	**RS.MA-01.3**	Il **piano** di cui al punto 1 è riesaminato e, se opportuno, **aggiornato** periodicamente e comunque almeno **ogni due anni**, nonché qualora si verifichino incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.	X	-
RESPOND	**Segnalazione e comunicazione della risposta agli incidenti**	Le attività di risposta sono coordinate con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche.	**RS.CO-02**	Gli stakeholder interni ed esterni sono informati degli incidenti.	**RS.CO-02.1**	In accordo al piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono documentate e adottate **procedure per comunicare** senza ingiustificato ritardo, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, ovvero qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'articolo 37, comma 3, lettere g) e h), del decreto NIS: a) ai destinatari dei loro servizi, gli **incidenti** significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi; b) ai **destinatari dei servizi che sono potenzialmente interessati da una minaccia informatica significativa**, le misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia e la natura di tale minaccia.	X	-
RESPOND	**Segnalazione e comunicazione della risposta agli incidenti**	Le attività di risposta sono coordinate con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche.	**RS.CO-02**	Gli stakeholder interni ed esterni sono informati degli incidenti.	**RS.CO-02.2**	Sono documentate e adottate **procedure per informare il pubblico** sugli **incidenti occorsi**, qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'art. 37, comma 3, lettera i) del decreto NIS.	X	-
RECOVER	**Esecuzione del piano di ripristino dagli incidenti**	Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cybersecurity.	**RC.RP-01**	La parte del piano di risposta agli incidenti relativa al rispristino viene eseguita una volta avviata dal processo di risposta agli incidenti.	**RC.RP-01.1**	Nell'ambito del piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono adottate e documentate **procedure per il ripristino** con riguardo almeno al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica, ivi compresi quelli di cui all'articolo 25 del decreto NIS.	X	-
RECOVER	**Comunicazione sul ripristino dagli incidenti**	Le attività di ripristino sono coordinate con le parti interne ed esterne.	**RC.CO-03**	Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati.	**RC.CO-03.1**	Sono adottate e documentate **procedure per comunicare alle parti interne interessate**, ivi incluse le articolazioni competenti del soggetto NIS, le attività di ripristino a seguito di un incidente.	X	-