

Kit Software Documentale Procedure Adempimenti Direttiva NIS2

Questo PDF contiene un esempio dei materiali Winple. Per verificare la versione, i contenuti completi, gli altri dimostrativi e la disponibilità, visita la scheda del prodotto.

APRI LA SCHEDA DEL PRODOTTO



www.winple.it/kit-procedure-modulistica-politiche-adempimenti-direttiva-nis-2/



3. Attività operative e registrazioni

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

GV.OC-04 – Controllo 1

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

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

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

GV.RM-03 – Controllo 1

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

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

ID.RA-05 - Controllo 1

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

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

1. Scopo

Lo scopo della Policy inerente ai ruoli e alle responsabilità è quello di mantenere una struttura organizzativa costituita da personale idoneo e adeguato ad affrontare il rischio cyber e a gestirlo dal punto di vista gestionale, tecnico, informatico e giuridico.

L'organizzazione perciò procede, eseguendo sistematicamente la presente policy, a:

- Stabilire
- Comunicare
- Far comprendere
- Attuare e far rispettare

i ruoli, le responsabilità e le autorità relative alla gestione del rischio cyber.

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
GOVERNARE - GV La strategia di gestione del rischio di cybersecurity dell'organizzazione, i suoi obiettivi e le relative policy sono stabilite, comunicate e monitorate	Ruoli, responsabilità e correlati poteri (GV.RR): Sono stabiliti e comunicati i ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo	GV.RR-02 I ruoli, le responsabilità e le autorità relative alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati

GV.RR-04 – Controllo 4 [Soggetti essenziali]

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.

Gli obblighi che l'organizzazione provvede a far sottoscrivere nei contratti di lavoro sono i seguenti:

- **Obbligo di riservatezza e confidenzialità**

Il dipendente si impegna a non divulgare, comunicare o utilizzare, in alcun modo, dati, informazioni, documenti, progetti o know-how aziendali di cui sia venuto a conoscenza durante il rapporto di lavoro, anche dopo la cessazione o modifica del rapporto

- **Divieto di utilizzo di credenziali e strumenti aziendali**

Dopo la cessazione, il dipendente è tenuto a non utilizzare più alcun account, accesso, dispositivo, software o applicazione fornita dall'azienda, e a restituire ogni materiale in suo possesso

- **Restituzione di dispositivi, documentazione e materiali**

Il lavoratore è obbligato a restituire tempestivamente qualsiasi strumento tecnologico, supporto digitale, documentazione cartacea o elettronica ricevuti o prodotti durante il rapporto di lavoro

- **Divieto di conservazione di copie di dati o documenti**

È vietato conservare, duplicare o trasferire informazioni riservate, archivi, backup, password o qualsiasi altro dato aziendale su dispositivi personali o di terzi

- **Obbligo di segnalazione di incidenti post-cessazione**

Qualora il dipendente venga a conoscenza, anche successivamente alla cessazione, di violazioni, incidenti o anomalie riguardanti dati o informazioni dell'organizzazione, è tenuto a darne tempestiva comunicazione all'azienda

- **Rispetto della normativa vigente**

Gli obblighi di riservatezza e protezione dei dati restano in vigore per il periodo previsto dalla normativa applicabile (es. GDPR, NIS2) e/o per il periodo contrattualmente stabilito (es. 2, 3, 5 anni dalla cessazione)

- **Divieto di concorrenza e utilizzo illecito delle informazioni**

In base agli accordi specifici, può essere previsto il divieto di utilizzare informazioni aziendali per finalità in concorrenza o comunque in modo lesivo per l'organizzazione, anche dopo la fine del rapporto

Il possesso dei requisiti previsti per l'organizzazione per la sicurezza, il personale di business e gli amministratori di sistema viene documentato sistematicamente nelle schede **“Organizzazione”** e **“Autorizzati”** del modulo **MOD-03-Personale** attraverso l'apposizione del Sì oppure del No in relazione a ciascuno. L'assenza di uno solo dei requisiti determina l'insorgenza di una vulnerabilità di natura organizzativa/umana da affrontare e risolvere.

4. Evidenze comprovanti

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

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

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



Valutazione del Rischio Associato ai Fornitori (Scala 0 - 1)

1. Livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS:

- **0:** Nessun accesso
- **0,2:** Accesso limitato e solo per scopi specifici (es. supporto tecnico supervisionato)
- **0,4:** Accesso limitato a specifici segmenti di rete non critici
- **0,6:** Accesso a sistemi non critici
- **0,8:** Accesso a sistemi e reti critiche
- **1:** Accesso illimitato a sistemi e reti critiche

2. Accesso del fornitore alla proprietà intellettuale e ai dati (anche sulla base della loro criticità):

- **0:** Nessun accesso a dati sensibili o riservati
- **0,2:** Accesso a dati pubblici o a basso impatto
- **0,4:** Accesso a dati non critici
- **0,6:** Accesso a dati a medio impatto (es. dati non personali)
- **0,8:** Accesso a dati sensibili o personali
- **1:** Accesso a dati ad alta criticità o a proprietà intellettuale (es. segreti commerciali)

3. Impatto di una grave interruzione della fornitura:

- **0:** Nessun impatto
- **0,2:** Impatto minimo, i servizi rimangono operativi senza interruzioni
- **0,4:** Impatto moderato, i servizi subiscono un lieve degrado
- **0,6:** Impatto elevato, i servizi subiscono grave degradazione con interruzioni parziali
- **0,8:** Impatto critico, grave interruzione dei servizi essenziali
- **1:** Impatto catastrofico, interruzione totale dei servizi con conseguenze significative

4. Tempi e costi di ripristino in caso di indisponibilità dei servizi:

- **0:** Ripristino immediato e a costo zero
- **0,2:** Ripristino molto rapido e a basso costo
- **0,4:** Ripristino gestibile entro tempi ragionevoli e costi contenuti
- **0,6:** Ripristino che richiede tempi e costi significativi (es. ore/giorni e spese extra)
- **0,8:** Ripristino lungo, complesso e costoso (es. settimane e ingenti investimenti)
- **1:** Ripristino estremamente difficile o impossibile, con costi proibitivi e impatto a lungo termine

5. Ruoli e responsabilità del fornitore nel governo dei sistemi informativi e di rete:

- **0:** Nessun ruolo o responsabilità nella governance
- **0,2:** Ruolo di supporto su richiesta
- **0,4:** Responsabilità limitata su componenti non critici
- **0,6:** Ruolo attivo nella gestione di componenti rilevanti
- **0,8:** Ruolo di governance su sistemi essenziali
- **1:** Il fornitore ha il controllo totale o quasi totale di sistemi critici per l'organizzazione

1. Scopo

Lo scopo della Policy inerente alla gestione degli asset è quello di effettuare periodicamente la ricognizione di tutta la strumentazione che permette all'organizzazione di funzionare.

Attuando la Policy A, che si riferisce al rischio cyber, l'organizzazione ha stabilito già quali siano gli asset strategici, e cioè le reti e i sistemi sui quali si basa il suo funzionamento e tali elementi sono già stati documentati nel modulo **MOD-01-Rischio Cyber** alla scheda **Rischio**.

Questa procedura invece guarda agli elementi costitutivi singoli degli asset strategici e cioè si riferisce:

- Ai computer, e in genere a tutti i dispositivi hardware impiegati dal personale
- Ai software che l'organizzazione impiega per produrre il servizio e ai software di supporto
- Ai flussi di rete che permettono lo scambio dei dati e delle informazioni
- Ai servizi erogati dai fornitori

In tale procedura è importante documentare e fare ricognizione sistematica di come il funzionamento di un asset strategico dipenda dalle condizioni di sicurezza dell'asset operativo che lo serve, ai fini di una più compiuta comprensione delle relazioni tra gli asset strategici e gli asset operativi.

2. Riferimenti al Framework Nazionale Cybersecurity

Funzioni interessate	Categorie	Subcategorie
IDENTIFY (ID): I rischi attuali di cybersecurity dell'organizzazione sono compresi	Gestione degli asset (ID.AM): 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-02: Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione
		ID.AM-03: Sono mantenute le rappresentazioni delle comunicazioni di rete e dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione
		ID.AM-04: Sono mantenuti gli inventari dei servizi erogati dai fornitori

ID.RA-01 – Controllo 2 [Soggetti essenziali]

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.

L'organizzazione procede ad effettuare il vulnerability assessment, e cioè la valutazione della presenza e dell'incidenza delle vulnerabilità, prima di mettere in esercizio le proprie strutture e dopo, sistematicamente.

Le vulnerabilità riscontrate nell'ambito dell'assessment oppure a seguito di segnalazione sono rilevate registrando, nel modulo **MOD-01-Rischio Cyber** alla scheda **Vulnerabilità**:

- **Vulnerabilità:**
Specifica la natura della vulnerabilità riscontrata: Fisica, Organizzativa, Umana, Tecnologica oppure riferita ad asset specifici
- **Oggetto di ispezione:**
Specifica qual è l'oggetto ispezionato a cui è riferibile la vulnerabilità
- **Descrizione:**
Descrive l'oggetto ispezionato e la sua funzione per permettere di attribuire in maniera accurata e tempestiva il livello di vulnerabilità ad esso associato
- **Asset strategico:**
Riferisce la vulnerabilità rilevata all'Asset strategico inficiato da essa (Asset strategici sono sistemi e reti)

L'organizzazione procede a valutare la vulnerabilità o le vulnerabilità riscontrate, secondo la scala seguente:

- **1 Vulnerabilità lieve:**
esistono debolezze o controlli carenti che potrebbero essere sfruttati in particolari condizioni
- **2 Vulnerabilità moderata:**
la debolezza può essere sfruttata da minacce comuni, con possibili effetti limitati anche su altri sistemi
- **3 Vulnerabilità significativa:**
la debolezza è facilmente sfruttabile
- **4 Vulnerabilità grave:**
la debolezza può portare a compromissione rilevante o perdita di controllo sull'asset, con effetto domino sul sistema
- **5 Vulnerabilità critica:**
la compromissione dell'asset causa perdita totale di riservatezza, integrità o disponibilità; rischio massimo, situazione di emergenza.

Come già indicato nella **Policy-A-Gestione del rischio**, e nel modulo **MOD-02-Piano di gestione rischi**, la valutazione dei rischi cambia in presenza della vulnerabilità e rimane tale, se non peggiora, fin quando la vulnerabilità non viene risolta.

4. Attività operative e registrazioni

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

ID.IM-04 – Controllo 3

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

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

ID.IM-04 – Controllo 4

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

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

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

ID.IM-04 – Controllo 5

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

4. Attività operative e registrazioni

PR.AA-05– Controllo 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).

Nel modulo **MOD-03-Personale** alla scheda **Utenze** i permessi sono assegnati secondo il criterio del minimo privilegio secondo la scala:

- Lettura: L'utente può visualizzare i dati, ma non può modificarli
- Scrittura: L'utente può creare, modificare o eliminare file e dati
- Esecuzione: L'utente può avviare programmi o script
- Amministrazione: L'utente ha il controllo completo del sistema, può modificare le configurazioni e gestire altri

La separazione delle funzioni è applicata in relazione ai ruoli istituiti nell'organizzazione

PR.AA-05– Controllo 2

È assicurata la completa distinzione tra utenze con e senza privilegi amministrativi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.

Tra le utenze l'organizzazione ha distinto i profili a cui ha concesso i permessi di "amministratore". Lo ha documentato nel modulo **MOD-03-Personale** alla scheda **Utenze**.

PR.IR-01– Controllo 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.

Nel modulo **MOD-03-Personale** alla scheda **Utenze**, a seguito del personale di business e del personale tecnico sono state documentate tutte le utenze remote.

Si tratta di organizzazioni fornitrici che accedono ai sistemi e alle reti dell'organizzazione per effettuare operazioni tecniche di intervento manutentivo oppure operazioni di business connesse ai contratti, all'avanzamento dei progetti e alla fatturazione.

PR.IR-01– Controllo 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. Le utenze remote sono controllate mediante approvazione sistematica la cui documentazione è presente nel modulo **MOD-03-Personale** alla scheda **Utenze**. La valutazione di rischio che concerne le utenze esterne a cui sono riconosciuti diritti di accesso e permessi avviene sulla base delle informazioni presenti della supply chain e cioè nel modulo **MOD-08-Supply chain** alla scheda **Sicurezza fornitori**

2. Attività operative e registrazioni

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

PR.AA-06– Controllo 1

Per almeno i sistemi informativi e di rete rilevanti, l'accesso fisico è protetto.

L'organizzazione ha elaborato il documento di controllo al **MOD-09-Inventario** nella scheda **Accessi fisici** nella quale determina e riesamina sistematicamente il perimetro della sicurezza fisica riferito ai luoghi fisici in cui sono presenti e custoditi gli asset.

Il documento stabilisce:

- Asset da proteggere
- Misure di protezione
- Responsabile del presidio
- Responsabile approvazione
- Data di approvazione

3. Evidenze comprovanti

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

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

Codifica framework nazionale cybersecurity				Evidenze documentali	
Fun	Cat	Sub	N° controllo	Documento/scheda	Check
PR	PR.AA	PR.AA-06	1	MOD-09-Inventario/Accessi fisici	

4. Attività operative e registrazioni

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

PR.AT-02– Controllo 1 [Soggetti essenziali]

Il piano di cui alla misura PR.AT-01, che l'organizzazione ha documentato nel modulo **MOD-15-Piano formazione**, 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:

- le istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete
- le informazioni sulle minacce informatiche note
- le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.

PR.AT-02– Controllo 2 [Soggetti essenziali]

È mantenuto un registro aggiornato nel modulo **MOD-03-Personale** alla scheda **Formazione specialistica** modulo 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.

Nel modulo sono riportati:

- I ruoli tecnici appartenenti all'organizzazione informatica
- Il modulo formativo specialistico somministrato
- La verifica di competenza eseguita
- La valutazione che esprime il livello di idoneità acquisito

4. Attività operative e registrazioni

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

PR.DS-01– Controllo 1

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

L'organizzazione, nel modulo **MOD-09-Inventario** alla scheda **Hardware**, censisce tutti i dispositivi mobili e portatili. Questi dispositivi possono contenere, elaborare e trasmettere dati.

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

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

PR.DS-11– Controllo 1

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

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

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

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

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

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

Per almeno i sistemi informativi e di rete rilevanti, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.

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

3. Attività operative e registrazioni

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

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

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

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

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

Tali backup sono documentati nel modulo **MOD-09-Inventario** alla scheda **Hardware** e alla scheda **Software**

PR.PS-02– Controllo 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.

Nel modulo **MOD-09-Inventario** alla scheda **Software** l'organizzazione dichiara tutto il software installato e lo riferisce, nella colonna Asset strategico associato, alla rete o al sistema informativo di riferimento principale dell'organizzazione. L'approvazione del software è subordinata alla disponibilità dei corrispondenti aggiornamenti di sicurezza.

PR.PS-02– Controllo 2

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

L'approvazione del software documentato alla scheda **Software** del modulo **MOD-09-Inventario** è subordinata all'installazione degli ultimi aggiornamenti di sicurezza in coerenza con il piano del modulo **MOD-10-Piano gestione vulnerabilità**

3. Attività operative e registrazioni

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

PR.IR-01- Controllo 3

Sono presenti, aggiornati, mantenuti e configurati i sistemi perimetrali, quali firewall. L'organizzazione ha documentato di aver applicato il firewall a tutti i flussi di rete in ingresso e in uscita al modulo **MOD-09-Inventario** alla scheda **Flussi rete**.

Il software inerente al firewall è aggiornato come documenta il modulo **MOD-09-Inventario** alla scheda **Software** ed è sottoposto a regolare manutenzione.

La configurazione della rete perimetrale del firewall è documentata all'interno del modulo **MOD-18-Configurazione Firewall**.

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

In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono utilizzati sistemi di comunicazione di emergenza protetti.

In presenza di vulnerabilità che insistono sulla possibilità di comunicazione all'interno e verso l'esterno dell'organizzazione il personale ricorre ai sistemi di comunicazione alternativa stabiliti nel modulo **MOD-11-Piano di continuità operativa**.

Tali canali sono:

- Sistema e-mail interno
- Sistema di ticketing tecnico
- Comunicazione telefonica
- Sistemi di messaggistica
- Posta elettronica esterna
- Punto di Contatto NIS
- Contatti informatici dei fornitori

4. Evidenze comprovanti

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

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

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

3. Attività operative e registrazioni

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

RS.MA-01 – Controllo 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:

- le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità
- 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
- le informazioni di contatto per la segnalazione degli incidenti
- le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna
- la reportistica da utilizzare per la documentazione dell'incidente

Il piano è documentato nel modulo **MOD-21-Piano gestione incidenti e ripristino** e questo stabilisce le cose da fare e la comunicazione, poi c'è il modulo **MOD-22-Registro incidenti** che riporta tutte le registrazioni inerenti all'incidente.

Le informazioni al CSIRT previste dal decreto NIS sono disciplinate dallo stesso piano e documentate:

- Dalla previsione della notifica di incidente da effettuare tramite la piattaforma web del CSIRT all'indirizzo: <https://segnalazioni.acn.gov.it/>
- Dal modulo **MOD-23-Relazione intermedia CSIRT**
- Dal modulo **MOD-24-Relazione finale CSIRT**

Nel modulo **MOD-22-Registro incidenti** l'organizzazione documenta il riesame dell'episodio incidente aggiornando eventualmente i seguenti piani della cybersecurity nell'intenzione di scongiurare un incidente analogo:

- MOD-02-Piano di gestione rischi**
- MOD-10-Piano gestione vulnerabilità**
- MOD-11-Piano di continuità operativa**
- MOD-12-Disaster recovery**
- MOD-14-Piano gestione crisi**
- MOD-15-Piano formazione**
- MOD-21-Piano gestione incidenti e ripristino**