Agenzia per la Cybersicurezza Nazionale

Linee Guida NIS

Specifiche di base

Definizione del processo di gestione degli incidenti di sicurezza informatica

Dicembre 2025

Controllo di versione

VERSIONE	DATA PUBBLICAZIONE	NOTE
1.0	Dicembre 2025	Prima pubblicazione.

INDICE

1. Introduzione

1.1. Premessa

La **gestione degli incidenti** – intesa come l'insieme delle attività volte a rilevare tempestivamente un incidente, a rispondervi in modo appropriato ed efficiente, a ripristinare la situazione allo stato antecedente al verificarsi dello stesso e a migliorare la capacità di rispondere a futuri incidenti tramite le lezioni apprese – rappresenta una capacità essenziale per garantire la continuità delle attività e dei servizi, la protezione delle informazioni e la resilienza delle organizzazioni. Gli incidenti di sicurezza possono infatti determinare impatti significativi sulle attività e i servizi di un'organizzazione in termini operativi, finanziari o reputazionali.

In ragione di tale importanza, la *gestione degli incidenti* rappresenta uno dei pilastri della direttiva NIS[1] e del decreto legislativo 4 settembre 2024, n. 138 di recepimento della direttiva NIS, da qui in poi indicato come **decreto NIS** o, ove non vi sia ambiguità, **decreto**.

La gestione degli incidenti è infatti ricompresa tra le misure in materia di gestione dei rischi che i **soggetti NIS essenziali e importanti**[2] devono adottare secondo quanto previsto dall'articolo 24 del decreto. Inoltre, ai sensi dell'articolo 25 del medesimo decreto, i soggetti NIS devono notificare al **CSIRT Italia**[3] ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi.

1.2. Scopo e organizzazione del documento

Il presente documento si propone di fornire **linee guida per la definizione del processo di gestione degli incidenti di sicurezza informatica** in conformità a quanto previsto dal decreto NIS e dalla discendente normativa di attuazione.

In particolare, viene presentato un modello di processo per la gestione degli incidenti illustrandone le relative fasi e sotto-fasi. Sono inoltre presenti le seguenti appendici:

- **appendice A – introduzione alle specifiche di base**: illustra gli elementi peculiari delle specifiche di base per una migliore comprensione del documento;
- **appendice B – misure di sicurezza gestione incidenti**: per le varie fasi e sotto-fasi del processo di gestione degli incidenti elenca le misure di sicurezza della disciplina NIS rilevanti per la gestione degli incidenti.

---

[1] La direttiva UE 2022/2555 stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno.

[2] I soggetti NIS sono i soggetti di cui all'articolo 2, comma 1, lettera hhh), del decreto, di natura giuridica pubblica o privata che rientrano nell'ambito di applicazione del decreto. Ai sensi dell'articolo 6 del decreto NIS, sono distinti tra essenziali e importanti a seconda del livello di criticità intrinseca dei settori e delle tipologie di soggetto in relazione al rischio informatico.

[3] Il gruppo nazionale di risposta agli incidenti di sicurezza informatica ai sensi dell'articolo 15, comma 1, del decreto NIS operante all'interno dell'Agenzia per la cybersicurezza nazionale.

1.3. Soggetti destinatari

I destinatari del presente documento sono i soggetti NIS essenziali ed importanti.

1.4. Termini e definizioni

Nella seguente tabella sono elencate le definizioni dei termini peculiari usati nel presente documento.

TERMINE	DEFINIZIONE
Decreto NIS	Decreto legislativo 4 settembre 2024, n. 138.
Determinazione obblighi di base	Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.
Direttiva NIS	Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.
Incidenti significativi di base	Specifiche di base che descrivono gli incidenti significativi di cui all'articolo 25 del decreto NIS.
Log	Evidenza riferita a un evento riguardante un sistema informativo e di rete e memorizzata in formato testuale o binario.
Misure di sicurezza di base	Specifiche di base per gli obblighi di cui agli articoli 23 e 24 del decreto NIS.
Punto di contatto	Persona fisica designata dal soggetto NIS ai sensi dell'articolo 7, comma 1, lettera c), del decreto NIS.
Referente CSIRT	Persone fisica designata dal Punto di contatto per interloquire con lo CSIRT Italia, ed effettuare le notifiche di cui agli articoli 25 e 26 del decreto NIS.
Soggetto NIS	Un soggetto, di cui all'articolo 2, comma 1, lettera hhh), del decreto NIS, di natura giuridica pubblica o privata che rientra nell'ambito di applicazione del decreto NIS.
Soggetti essenziali	I soggetti NIS considerati essenziali ai sensi del decreto NIS.
Soggetti importanti	I soggetti NIS considerati importanti ai sensi del decreto NIS.
Specifiche di base	Le specifiche di cui agli allegati 1, 2, 3 e 4 della determinazione obblighi di base.

1.5. Norme di riferimento

NORMA	DESCRIZIONE
Decreto legislativo 4 settembre 2024, n. 138.	Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento

	(UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.
Determinazione obblighi di base.	Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.
Determinazione adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.	Termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale.

1.6. Documenti di riferimento

I seguenti documenti possono essere consultati per ulteriori approfondimenti sui temi trattati nelle presenti linee guida.

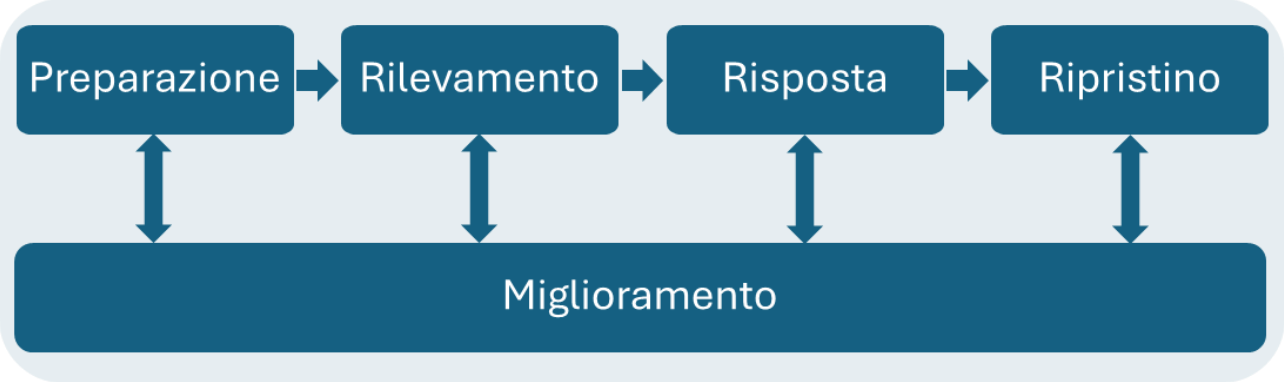
TITOLO E INDIRIZZO DI PUBBLICAZIONE
NIST SP 800-61r2. Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

2. Processo di gestione degli incidenti

Per gestire gli incidenti in modo efficace è essenziale definire un processo strutturato in modo da creare un quadro organizzativo armonizzato e assicurare la coerenza e sistematicità delle varie attività.

Quale riferimento per la definizione del processo di gestione degli incidenti, è qui presentato un modello[4] articolato nelle seguenti fasi:

- **preparazione**: precede il verificarsi di un incidente e costituisce la base per una riposta efficace degli incidenti di sicurezza, include le attività di *governo*, *identificazione* e *protezione*;
- **rilevamento**: è volta a rilevare tempestivamente il verificarsi di un incidente;
- **risposta**: riguarda le attività vere e proprie di risposta all'incidente rilevato nella fase precedente, include le attività di *investigazione*, *notifica*, *contenimento* ed *eradicazione* dell'incidente;
- **ripristino**: consiste nel ripristino dei sistemi informativi e di rete oggetto di compromissione;
- **miglioramento**: individua le azioni da realizzare per migliorare il processo di gestione degli incidenti utilizzano le conoscenze acquisite durante l'esecuzione del processo. In considerazione del fatto che può essere acquisita conoscenza durante tutte le varie fasi del processo, la fase di *miglioramento* si estende lungo tutto il processo di gestione degli incidenti.



Nelle successive sezioni del paragrafo sono descritte le fasi e sotto-fasi del processo con riferimento alle attività derivanti dall'attuazione degli adempimenti della disciplina NIS e in particolare dalle **misure di sicurezza di base** (da qui in poi indicate anche come *misure di sicurezza* o *misure*) della **determinazione obblighi di base**[5].

In Appendice A è riportata un'introduzione alle misure di sicurezza di base.

In Appendice B è riportato l'elenco delle misure di sicurezza di base relative alle varie fasi del processo di gestione degli incidenti.

[4] Il modello di processo qui presentato è definito sulla base di quello riportato nel documento del NIST *Incident Response Recommendations and Considerations for Cybersecurity Risk Management SP 800-61r3*.

[5] Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

Piano per la gestione degli incidenti

Il processo di gestione degli incidenti viene generalmente descritto e documentato nel cosiddetto *piano per la gestione degli incidenti*, all'interno del quale sono indicate, ad esempio, le attività da porre in essere per la gestione dell'incidente, le strutture organizzative e tecniche coinvolte, gli strumenti da utilizzare e la reportistica da produrre.

Il **punto 1** della misura di sicurezza **RS.MA-01** richiede di definire, attuare, aggiornare e documentare 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 comprenda almeno:

a) fasi e procedure di gestione e notifica degli incidenti e indicazione dei relativi ruoli e responsabilità;
b) procedure per la predisposizione e la trasmissione delle relazioni sugli incidenti intermedie, mensili e finali 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.

Ai sensi dei **punti 2** e **3** della medesima misura, il piano deve essere approvato dagli organi di amministrazione e direttivi, 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.

2.1. Preparazione

La fase di *preparazione* – costituita dalle sotto-fasi di *governo*, *identificazione* e *protezione* – riguarda tutte le attività propedeutiche volte a garantire una gestione strutturata ed efficace degli incidenti di sicurezza quali, ad esempio, la definizione di politiche, l'assegnazione di ruoli e responsabilità, il censimento dei sistemi informativi e di rete, la definizione di misure di sicurezza atte a prevenire il verificarsi di un incidente o a mitigarne l'impatto.

2.1.1. Governo

In questa sotto-fase, il soggetto definisce il quadro strategico e organizzativo per la gestione degli incidenti, provvedendo, in particolare, all'elaborazione delle politiche di sicurezza informatica e all'assegnazione dei ruoli e delle responsabilità per le attività del processo di gestione degli incidenti.

Politiche di sicurezza per la gestione degli incidenti

Le *politiche di sicurezza informatica* stabiliscono i principi e le regole di un'organizzazione per garantire la protezione dei sistemi informativi e di rete da ogni forma di minaccia o uso improprio e rappresentano pertanto l'impegno formale dell'organizzazione guidandone le decisioni.

Nell'ambito della gestione degli incidenti, in accordo a quanto richiesto dal **punto 1**[6] della misura **GV.PO-01**, devono essere adottate e documentare politiche di sicurezza informatica negli ambiti del *monitoraggio degli eventi di sicurezza* e della *risposta agli incidenti e ripristino*, includendo[7] almeno le politiche in relazione ai seguenti requisiti (i cui riferimenti sono riportati tra parentesi)[8]:

- strumenti tecnici per rilevare tempestivamente gli incidenti significativi (*DE.CM-01 punto 1*);
- livelli di servizio attesi (SL) dei servizi e delle attività (*DE.CM-01 punto 2*);
- sistemi di protezione dei punti terminali (endpoint) per il rilevamento del codice malevolo (*DE.CM-09 punto 1*);
- piano di gestione degli incidenti, approvazione da parte degli organi di amministrazione e direttivi, riesame ed eventuale aggiornamento (*RS.MA-01 punti 1, 2 e 3*);
- comunicazione, ai destinatari dei propri servizi, degli incidenti significativi che possono ripercuotersi negativamente sulla fornitura dei servizi, delle minacce significative cui sono potenzialmente interessati e delle relative misure correttive o di mitigazione da adottare (*RS.CO-02 punto 1*);
- comunicazione per informare il pubblico sugli incidenti occorsi (*RS.CO-02 punto 2*);
- ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza (*RC.RP-01 punto 1*);

Per i medesimi ambiti, i *soggetti essenziali* devono inoltre definire le politiche in relazione ai seguenti requisiti[9]:

- strumenti di analisi e filtraggio sul flusso di traffico in ingresso (*DE.CM-01 punto 4*);
- monitoraggio degli accessi da remoto, delle attività dei sistemi, degli eventi amministrativi di rilievo, nonché degli accessi eseguiti o falliti alle risorse di rete, ai punti terminali (*endpoint*) e agli applicativi (*DE.CM-01 punto 5*);
- parametri quali-quantitativi per rilevare gli accessi non autorizzati o con abuso dei privilegi concessi (*DE.CM-01 punto 6*);
- comunicazione alle parti interne interessate delle attività di ripristino a seguito di un incidente (*RC.CO-03 punto 1*).

In accordo a quanto previsto al punto 3 della misura GV.PO-01 le politiche di sicurezza devono essere approvate dagli organi di amministrazione e direttivi.

Ai sensi del **punto 1** della misura **GV.PO-02**, le politiche devono essere riesaminate e, se opportuno, aggiornate periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto

---

[6] Il requisito in questione richiede di adottare e documentare politiche di sicurezza informatica per almeno una serie di ambiti, tra i quali per l'appunto il monitoraggio degli eventi di sicurezza e la riposta agli incidenti e ripristino.

[7] Il punto 2 della misura GV.PO-01 richiede di includere, per i vari ambiti di cui al punto 1, almeno le politiche in relazione ai requisiti indicati nella tabella 1 in Appendice alle misure di sicurezza (allegato 1 della *determinazione obblighi di base* per i soggetti importanti, allegato 2 della medesima determinazione per i soggetti essenziali).

[8] I requisiti sono qui riportati in forma sintetica, si faccia riferimento alle misure di sicurezza di base per il testo completo.

[9] Per i soggetti essenziali sono stati definiti requisiti e misure di sicurezza aggiuntivi rispetto ai soggetti importanti, in considerazione di quanto indicato dall'articolo 31 del decreto.

normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Ruoli e responsabilità per la gestione degli incidenti

Per gestire efficacemente gli incidenti devono essere assegnati i ruoli e le relative responsabilità per le varie attività del processo di gestione degli incidenti.

Sono generalmente assegnati ruoli e responsabilità in relazione al monitoraggio e analisi degli eventi di sicurezza, al coordinamento della risposta agli incidenti, all'investigazione, al contenimento e al ripristino in caso di incidente, alla comunicazione con le parti interessate e notifica alle autorità competenti degli incidenti, alle interlocuzioni con il CSIRT Italia e alle conseguenti attività decisionali.

Con riguardo alle figure professionali coinvolte nel processo di gestione degli incidenti, si può inoltre fare riferimento alle linee guida per la realizzazione di CSIRT dell'Agenzia per la cybersicurezza nazionale[10].

Matrici RACI

Uno degli strumenti utilizzati per l'assegnazione di ruoli e responsabilità, è la matrice di assegnazione responsabilità (cosiddetta matrice RACI) che permette di definire chiaramente ruoli e responsabilità per le varie attività di un processo. Nello specifico, RACI è un acronimo le cui lettere indicano le responsabilità che un determinato ruolo ha nell'ambito di una specifica attività:

- *Responsible (R)*: chi esegue operativamente l'attività.
- *Accountable (A)*: chi ha la responsabilità sul risultato dell'attività.
- *Consulted (C)*: chi viene consultato durante l'esecuzione dell'attività in quanto possiede conoscenze necessarie al completamento dell'attività.
- *Informed (I)*: chi è informato sull'avanzamento e il completamento dell'attività.

Per ogni attività deve essere presente almeno un *Responsible* in modo da individuare chi ha il compito di eseguire operativamente l'attività ed un solo Accountable in modo da definire chiaramente chi ha la responsabilità sul risultato dell'attività.

Per assegnare i ruoli e le responsabilità di un processo tramite matrici RACI sono preliminarmente individuati i ruoli – intesi come strutture organizzative o specifiche figure quale, ad esempio, quella del *referente CSIRT* – e quindi assegnate le responsabilità per le varie attività.

In accordo a quanto previsto dalla determinazione ACN adottata ai sensi dell'articolo 7, comma 6, del decreto NIS , il *Punto di Contatto*[11] del soggetto NIS deve designare il **Referente CSIRT** per le attività di interlocuzione con lo CSIRT Italia e di notifica degli incidenti per conto del soggetto.

[10] https://www.acn.gov.it/portale/documents/d/guest/acn_linee_guida_csirt.

[11] Persona fisica designata dal soggetto NIS con il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso. Deve avere almeno un sostituto a meno che il soggetto NIS non possa materialmente effettuare tale adempimento, in quanto il Punto di contatto è l'unica persona fisica operante nell'organizzazione. Non è possibile individuare per i ruoli di Punto di contatto e sostituti personale esterno al soggetto.

Referente CSIRT

Il Referente CSIRT ha il compito di interloquire con lo CSIRT Italia ed effettuare le notifiche obbligatorie degli incidenti significativi nonché di quelle volontarie per conto del soggetto per cui opera.

Per assicurare il tempestivo svolgimento dei suoi compiti con particolare riferimento alla notifica degli incidenti significativi e ai relativi seguiti, possono inoltre essere inoltre designati uno o più sostituti.

Il Referente CSIRT deve possedere almeno competenze di base in materia di sicurezza informatica e di gestione degli incidenti informatici e una conoscenza approfondita dei sistemi informativi e di rete del soggetto per conto del quale operano.

Nelle organizzazioni complesse e articolate è possibile soddisfare tale requisito, attraverso un modello operativo che consenta al referente CSIRT di disporre delle conoscenze approfondite dei sistemi informativi e di rete, anche indirettamente, attivando caso per caso personale preposto.

Con riferimento alla sua designazione, si osserva che essa costituisce una delega operativa e non una delega di responsabilità, in quanto ai sensi dell'articolo 23 del decreto, gli organi di amministrazione e direttivi sono i responsabili delle violazioni degli adempimenti del decreto.

Per quanto non sia preferibile, può coincidere con il Punto di contatto. È inoltre possibile, seppure anche in questo caso non preferibile, individuare per il suo ruolo e/o dei sostituti personale esterno al soggetto come, ad esempio, un responsabile del SOC/CERT o della gestione dell'infrastruttura IT esternalizzati.

Sulla base di quanto previsto dal **punto 3** della misura **GV.RR-02**, il Referente CSIRT ed eventuali sostituti sono inclusi nell'*organizzazione di sicurezza informatica* definita dal soggetto NIS ai sensi della medesima misura[12].

Per ulteriori indicazioni sulla figura del Referente CSIRT (e del Punto di contatto), si può far riferimento alla determinazione ACN adottata ai sensi dell'articolo 7, comma 6, del decreto NIS e alle FAQ dedicate pubblicate all'indirizzo https://www.acn.gov.it/portale/faq/nis/aggiornamento-continuo.

Il processo di gestione degli incidenti potrebbe inoltre prevedere specifici ruoli e responsabilità per le terze parti. Si pensi, ad esempio, al Referente CSIRT e/o ai relativi sostituti esternalizzati, a un fornitore di servizi di sicurezza gestiti (*managed security service provider* – MSSP) che esegue attività di analisi degli eventi rilevanti per la sicurezza o a un fornitore di servizi *cloud* che fornisce supporto nelle attività di ripristino dagli incidenti.

A tale riguardo il **punto 1** della misura **GV.SC-02**, richiede di definire gli eventuali ruoli e responsabilità in materia di sicurezza informatica assegnati al personale delle terze parti nell'ambito dell'organizzazione per la sicurezza informatica.

2.1.2. Identificazione

In questa sotto-fase è acquisita una conoscenza del contesto operativo al fine di pianificare in modo efficace la risposta agli incidenti. Le attività di *identificazione* riguardano, ad esempio, l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità.

[12] Analoga previsione per il Punto di contatto e relativi sostituti.

Inventario dei sistemi informativi e di rete

Le informazioni relative all'inventario dei sistemi informativi e di rete permettono di individuare i sistemi da proteggere, determinare le priorità per le attività di risposta e recupero e rilevare in modo più efficace gli incidenti.

A tale riguardo, le misure di sicurezza di base **ID.AM-01**, **ID.AM-02**, **ID.AM-03**, **ID.AM-04** richiedono di mantenere rispettivamente i seguenti inventari aggiornati:

- inventario degli apparati fisici (*hardware*) che compongono i sistemi informativi e di rete, ivi inclusi i dispositivi IT, IoT, OT e mobili;
- inventario aggiornato di servizi, sistemi e applicazioni *software* che compongono i sistemi informativi e di rete, ivi incluse le applicazioni commerciali, *open-source* e *custom,* anche accessibili tramite API;
- inventario dei flussi di rete tra i sistemi informativi e di rete del soggetto NIS e l'esterno;
- inventario dei servizi informatici erogati dai fornitori, ivi inclusi i servizi *cloud*.

Individuazione di minacce e vulnerabilità

La conoscenza delle minacce e delle vulnerabilità permette di migliorare la prevenzione degli incidenti e favorire una risposta più rapida e mirata.

A tale riguardo, il **punto 1** della misura **ID.RA-01** richiede di identificare eventuali vulnerabilità sui sistemi informativi e di rete anche utilizzando le informazioni acquisite monitorando i canali di comunicazione del CSIRT Italia, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) settoriali[13].

Ai sensi di quanto previsto dai **punti 2** e **3** della medesima misura, i *soggetti essenziali*, per almeno i sistemi informativi e di rete rilevanti, in accordo al piano di gestione delle vulnerabilità[14], fatte salve motivate e documentate ragioni normative o tecniche, devono inoltre eseguire periodicamente e comunque prima della loro messa in esercizio, attività per l'identificazione delle vulnerabilità che comprendano almeno *vulnerability assessment* e/o *penetration test*.

2.1.3. Protezione

In questa sotto-fase sono stabilite le misure di protezione volte a ridurre la probabilità e limitare l'impatto degli incidenti. Ridurre la probabilità, e dunque il numero, di incidenti consente di dedicare maggiori risorse alla risposta degli incidenti più critici e complessi, mentre limitare l'impatto dell'incidente rende generalmente meno complesse le attività di contenimento ed eradicazione, oltre a mitigare le conseguenze dell'attacco, in termini non solo di sistemi informativi e di rete compromessi, ma anche operativi, economici e reputazionali.

Le misure di protezione possono essere distinte in *misure di protezione tecnologiche* e *misure di protezione organizzative*.

[13] Il **punto 1** della misura **ID.RA-08** richiede il monitoraggio almeno dei 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.

[14] Il *piano di gestione delle vulnerabilità* è definito ai sensi del **punto 3** della misura **ID.RA-08**.

Misure di protezione tecnologiche

Le misure di protezione tecnologiche comprendono, ad esempio, quelle relative all'acquisizione dei *log* per il monitoraggio degli eventi di sicurezza, alla pianificazione dei *backup* dei dati e delle configurazioni, alla predisposizione degli strumenti di sicurezza per il controllo degli accessi e all'uso di canali di comunicazione alternativi in caso di malfunzionamento dei canali di comunicazione principali.

Con riferimento alla pianificazione dei *backup*, il **punto 1** della misura **PR.DS-11** richiede di effettuare periodicamente i *backup* dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, di conservare copie di *backup offline*. Ai sensi dei **punti 3** e **4** della medesima misura, ai soggetti essenziali è inoltre richiesto, per almeno i sistemi informativi e di rete rilevanti, di assicurare la riservatezza e l'integrità delle informazioni contenute nei *backup* mediante adeguata protezione fisica dei supporti, ovvero mediante cifratura e di verificare periodicamente l'utilizzabilità dei *backup* effettuati mediante test di ripristino.

Con riferimento all'acquisizione dei log, il **punto 2** della misura **PR.PS-04** richiede di acquisire e, in modo sicuro e possibilmente centralizzato, conservare almeno i *log* necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi i *log* relativi agli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi.

Con riferimento al controllo degli accessi, il **punto 1** della misura **PR.IR-01** richiede, per almeno i sistemi informativi e di rete rilevanti, di implementare adeguate misure di sicurezza per l'accesso effettuato da remoto[15]. Il **punto 3** della medesima misura richiede che siano presenti, aggiornati, mantenuti e configurati in modo adeguato i sistemi perimetrali, quali, ad esempio, i *firewall*.

Con riferimento all'uso di canali di comunicazione alternativi, la misura **PR.IR-03** richiede che i soggetti essenziali, in accordo agli esiti della valutazione del rischio, utilizzino sistemi di comunicazione di emergenza protetti.

Misure di protezione organizzative

Le misure di protezione organizzative comprendono, ad esempio, l'elaborazione di procedure in relazione alle attività del processo di gestione degli incidenti e le attività di formazione del personale in materia di sicurezza informatica con le relative esercitazioni.

Con riferimento all'elaborazione di procedure in relazione alle attività del processo di gestione degli incidenti, sulla base di quanto previsto dalle misure di sicurezza[16], devono essere adottate e documentate le procedure almeno in relazione ai seguenti requisiti (i cui riferimenti sono riportati tra parentesi)[17]:

- esecuzione dei backup e conservazione di copie di backup offline (*PR.DS-11 punto 1*);
- acquisizione e conservazione dei *log* (*PR.OS-04 punto 2*);

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

[16] Si fa riferimento in particolare ai requisiti che richiedono l'adozione e documentazione di specifiche procedure.

[17] I requisiti sono qui riportati in forma sintetica, si faccia riferimento alle misure di sicurezza di base per il testo completo.

- aggiornamento, manutenzione e configurazione dei sistemi perimetrali (*PR.IR-03 punto 3*);
- aggiornamento, manutenzione e configurazione degli strumenti tecnici per rilevare tempestivamente gli incidenti significativi (*DE.CM-01 punto 1*);
- notifica degli incidenti (*RS.MA-01 punto 1, lettera a*);
- predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS (*RS.MA-01 punto 1, lettera b*);
- comunicazione, ai destinatari dei propri servizi, degli incidenti significativi che possono ripercuotersi negativamente sulla fornitura dei servizi e delle misure da adottare (*RS.CO-01 punto 1*);
- comunicazione per informare il pubblico sugli incidenti occorsi (*RS.CO-01 punto 2*);
- ripristino normale funzionamento sistemi informativi e di rete coinvolti da incidenti (*RC.RP-01 punto 1*);

Per i soggetti essenziali sono inoltre richieste le procedure relative ai seguenti ulteriori elementi:

- protezione dei backup (*PR.DS-11 punto 3*);
- verifica dell'utilizzabilità dei backup (*PR.DS-11 punto 4*);
- uso dei sistemi di comunicazione di emergenza protetti (*PR.IR-03 punto 1*);
- uso degli strumenti di analisi e filtraggio sul flusso di traffico in ingresso (*DE.CM-01 punto 4*);
- monitoraggio accessi da remoto, attività dei sistemi perimetrali, eventi amministrativi di rilievo e accessi eseguiti o falliti a risorse di rete, punti terminali (endpoint) e applicativi *DE.CM-01 punto 5*);
- comunicazione delle attività di ripristino a seguito di un incidente alle parti interne interessate (*RC.CO-03 punto 4*).

Procedure per la gestione degli incidenti

L'uso di procedure per la gestione degli incidenti consente di guidare le attività del processo di gestione degli incidenti in modo strutturato, migliorando l'efficienza operativa, riducendo il rischio di errori e in conformità con le politiche stabilite. L'obiettivo di una procedura è garantire una risposta coerente e ripetibile a fronte di situazioni critiche od operative.

Le procedure sono strutturate secondo un formato standard (procedure formalizzate che forniscono istruzioni dettagliate su come eseguire specifiche attività sono anche denominate SOP – Standard Operating Procedure) che prevede la presenza di elementi ricorrenti quali ad esempio:

- **titolo e versione**: indica l'oggetto della procedura e il suo numero di versione;
- **ambito di applicazione**: definisce il contesto operativo, le aree e i soggetti a cui la procedura si rivolge;
- **attività operative**: elenca in ordine sequenziale le azioni e i controlli da svolgere per garantire la corretta esecuzione della procedura;
- **strumenti utilizzati**: descrive gli strumenti necessari per l'implementazione della procedura;
- **ruoli e responsabilità**: specifica le figure coinvolte e le relative responsabilità nell'esecuzione della procedura.

Le procedure devono essere aggiornate e testate periodicamente per garantirne la coerenza con l'evoluzione del contesto tecnico e normativo e verificarne l'applicabilità, l'accuratezza e l'efficacia; possono essere inoltre utilizzate per formare il personale su come agire correttamente a fronte di specifiche attività operative.

Con riferimento alle attività di formazione del personale del personale in materia di sicurezza informatica, il **punto 1** della misura **PR.AT-01** richiede di definire, attuare, aggiornare e documentare un **piano di formazione** in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi, che comprenda almeno la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita e, qualora previste, le modalità di verifica dell'acquisizione dei contenuti.

Per i soggetti essenziali, ai sensi di quanto previsto dal **punto 2** della misura **PR.AT-02**, il *piano di formazione* deve inoltre prevedere 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 comprenda 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.

2.2. Rilevamento

La fase di *rilevamento* è finalizzata a individuare e analizzare gli **eventi rilevanti per la sicurezza informatica** con l'obiettivo di individuare tempestivamente il verificarsi di un incidente e limitarne l'impatto e l'estensione.

Gli *eventi rilevanti per la sicurezza informatica* sono eventi di natura intenzionale o accidentale che compromettono o *potrebbero* compromettere la sicurezza dei sistemi informativi e di rete e che necessitano pertanto di un'analisi (*triage*) al fine di verificare se si tratta di un incidente.

Esempi di eventi rilevanti per la sicurezza informatica includono:

- tentativi di autenticazioni su molteplici utenze di dominio da medesimi hostname/indirizzo IP;
- modifiche ai gruppi degli amministratori di dominio;
- autenticazioni da *hostname* e/o indirizzi IP identificati come IOC;
- richieste alle applicazioni web da user agent identificati come IOC;
- esecuzione di script che usano determinati comandi;
- accessi degli amministratori di dominio e/o in VPN al di fuori del normale orario lavorativo e/o da postazioni di lavoro diverse da quelle ordinarie;
- comunicazioni di rete sospette (verso *url* e/o indirizzi IP identificati come IOC);
- picco di traffico proveniente da molteplici indirizzi IP;
- saturazione della larghezza di banda in entrata.

Al fine di individuare gli eventi rilevanti per la sicurezza informatica, è necessario prevedere **attività di monitoraggio** che possono essere realizzate secondo i seguenti approcci[18];

[18] Per aumentare l'efficacia del monitoraggio, è opportuno adottare entrambi gli approcci.

- **proattivo**: gli eventi rilevanti per la sicurezza sono individuati, ad esempio, attraverso la ricerca di indizi di attività malevole sui sistemi[19], o dall'analisi dei bollettini di sicurezza condivisi dal CSIRT Italia, circa nuovi scenari di rischio, comportamenti anomali o attacchi in corso;
- **reattivo**: gli eventi rilevanti per la sicurezza sono individuati, ad esempio, in esito agli *allarmi* generati dagli strumenti di sicurezza o alle segnalazioni di attori interni (utenti che riportano malfunzionamenti o disservizi) e/o esterni come il CSIRT Italia.

La ricerca di possibili indizi di attività malevole e la configurazione degli *allarmi* generati dagli strumenti di sicurezza si basano su *logiche di rilevamento* che possono essere definite in accordo alle seguenti metodologie:

- **IOC-based**: si basa sulla ricerca di indicatori di compromissione (caratteristiche statiche del malware come *hash*, nomi di file, librerie) nei *log* dei sistemi. Non permette di rilevare minacce che non sono caratterizzate dagli indicatori noti o che li cambiano.
- **anomaly-based:** si basa sul rilevamento di deviazioni da parte dei sistemi informativi o parti di essi dal loro comportamento *standard* attraverso l'analisi statistica, il *machine learning* e altre forme di analisi di grandi quantità di dati (*big data analysis*). Richiede generalmente una modellazione molto accurata del comportamento *standard* rispetto al quale rilevare deviazioni e, pertanto, potrebbe generare molti falsi positivi e richiedere investimenti significativi in termini di acquisizione dei dati e loro processamento;
- **TTP-based**: si basa sulla conoscenza delle tattiche, tecniche e procedure (TTPs) che un attore malevolo utilizza per raggiungere i propri obiettivi. È efficace perché le TTPs non cambiano frequentemente e sono comuni ai vari attori in quanto la tecnologia sulla quale opera l'attaccante vincola il numero e il tipo di tecniche che questi può utilizzare.

Gli eventi rilevanti per la sicurezza individuati sono quindi analizzati per verificare se si riferiscono a incidenti di sicurezza.

Il numero di eventi rilevanti per la sicurezza informatica da analizzare può essere molto elevato e di complessa gestione senza il supporto di tecnologie automatizzate. A tal fine possono essere utilizzati strumenti di sicurezza come ad esempio il *SIEM*, il *SOAR* o l'*EDR*[20] che agevolano l'individuazione degli eventi rilevanti per la sicurezza informatica.

Tali strumenti devono essere opportunamente configurati al fine di ridurre gli *allarmi* che non corrispondono ad incidenti, generalmente indicati come **falsi positivi**. Per ridurre il numero di *falsi positivi*, nella fase di *miglioramento* è opportuno effettuare un *tuning* delle logiche di rilevamento sulla base dell'analisi effettuata sui falsi positivi. Ad esempio, nel caso di eventi frequentemente ricorrenti corrispondenti a falsi positivi, si potrà valutare la possibilità di aggiornare le logiche di rilevamento in modo da escludere tali eventi da quelli segnalati.

[19] Si parla anche di *Threat Hunting* per indicare quelle metodologie di rilevamento che mirano ad *anticipare* le minacce, prima che causino danni, tramite la ricerca *attiva* di segni di compromissione all'interno di una rete o di un sistema informativo.

[20] Il SIEM (*Security Information and Event Management*), il SOAR (*Security Orchestration, Automation and Response)* e l'EDR (*Endpoint Detection Response*) sono strumenti di sicurezza utilizzati, rispettivamente, per la raccolta e analisi dei log, l'automazione e il coordinamento delle attività di risposta agli incidenti e il rilevamento e la risposta delle minacce presenti sugli *endpoint*.

Nel caso in cui l'analisi di un evento rilevante per la sicurezza informatica abbia effettivamente determinato che è relativo a un incidente, viene dichiarato l'incidente e si passa alla successiva fase di *risposta*.

Con riferimento al monitoraggio e al rilevamento degli incidenti, il **punto 1** della misura **DE.CM-01** richiede che, per almeno i sistemi informativi e di rete rilevanti, siano presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi.

Il **punto 2** della medesima misura richiede di definire e documentare i *livelli di servizio attesi (SL)*[21] dei servizi e delle attività del soggetto NIS anche ai fini di rilevare tempestivamente gli incidenti significativi.

il **punto 1** della misura **DE.CM-09** richiede che, fatte salve motivate e documentate ragioni normative o tecniche, siano presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione dei punti terminali (*endpoint*) per il rilevamento del codice malevolo.

Per i soggetti essenziali, ai sensi dei punti **4**, **5** e **6** della misura **DE.CM-01** è inoltre richiesto, per almeno i sistemi informativi e di rete rilevanti, di:

- impiegare strumenti di analisi e filtraggio sul flusso di traffico in ingresso (ivi inclusa la posta elettronica);
- monitorare gli accessi da remoto, le attività dei sistemi perimetrali (ad esempio router e firewall), gli eventi amministrativi di rilievo e gli accessi eseguiti o falliti alle risorse di rete, ai punti terminali (endpoint) e agli applicativi;
- definire, monitorare e documentare *parametri quali-quantitativi*[22] per rilevare gli accessi non autorizzati o con *abuso dei privilegi concessi*[23].

2.3. Risposta

La fase di *risposta* – costituita dalle sotto-fasi di *segnalazione, investigazione*, *contenimento* ed *eradicazione* discusse nelle successive sezioni del presente paragrafo – inizia nel momento in cui è stato dichiarato l'incidente e rappresenta la fase centrale del processo di gestione degli incidenti.

Con riferimento alle varie sotto-fasi, si osserva che le stesse non seguono generalmente un ordine lineare ma tendono piuttosto a essere realizzate in parallelo, in modo strettamente interlacciato. Inoltre, non tutte devono essere necessariamente implementante per ogni tipo di evento: potrebbero esserci infatti eventi che non

[21] I livelli di servizio attesi, indicati con l'acronimo SL, sono definiti in autonomia dal soggetto e rappresentano gli obiettivi, indicati in termini misurabili, che definiscono le prestazioni attese dei servizi e delle attività del soggetto. Non necessariamente coincidono con i livelli di servizio definiti nei contratti denominati generalmente *SLA* o *Service Level Agreement*.

[22] Insieme di indicatori di tipo qualitativo e quantitativo: un esempio di indicatore di tipo quantitativo è il superamento di una soglia per le interrogazioni di una banca dati da parte di un singolo utente, un esempio di indicatore di tipo qualitativo è l'accesso di un amministratore di sistema al di fuori dell'orario di servizio.

[23] Fattispecie in cui l'utente di un sistema informativo e di rete abbia l'autorizzazione tecnica (disponibilità di credenziali che sono configurate per accedere ai dati) per accedere a determinati dati ma tale acceso sia effettivamente illecito in quanto, ad esempio, effettuato in violazione delle politiche del soggetto o risulti strumentale al perseguimento di scopi estranei alle necessità funzionali di accesso.

richiedono attività di *contenimento* e/o *eradicazione*, come, ad esempio, nel caso di eventi per i quali non c'è stato alcun impatto[24].

2.3.1. Segnalazione

In questa sotto-fase si procede a notificare l'incidente alle autorità competenti e a comunicarlo alle parti, interne ed esterne, interessate.

Sulla base di quanto previsto dal decreto NIS e dalla *determinazione obblighi di base*, i soggetti NIS sono tenuti a notificare le seguenti tipologie di incidente[25] al CSRIT Italia:

- **IS-1**: il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale;
- **IS-2**: il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
- **IS-3**: il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei *livelli di servizio atteso (SL)* definiti ai sensi della misura DE.CM-01.

I soggetti essenziali devono inoltre notificare la seguente tipologia di incidente:

- **IS-4**: il soggetto NIS ha evidenza, anche sulla base dei *parametri quali-quantitativi* definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con *abuso dei privilegi concessi*, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Evidenza dell'incidente

Come si evince dalla formulazione delle tipologie di incidente, ai fini dell'adempimento dell'obbligo di notifica degli incidenti ciò che rileva è che il soggetto *abbia evidenza dell'incidente*, ossia sia venuto a conoscenza del verificarsi di una delle tipologie di incidente previste.

Con la dicitura *avere evidenza dell'incidente* si intende che il soggetto dispone di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica.

L'acquisizione dell'evidenza è tipicamente successiva al verificarsi dell'incidente e definisce il momento dal quale decorre il termine per la trasmissione della pre-notifica (24 ore) e della notifica (72 ore).

L'evidenza di un incidente viene generalmente acquisita tramite:

- analisi di segnalazioni fatte da attori esterni al soggetto, come ad esempio quelle effettuate dal CSIRT Italia;
- analisi di segnalazioni fatte da attori interni al soggetto, come ad esempio quelle di un utente che riporta un malfunzionamento al servizio di help desk;
- analisi degli eventi di sicurezza rilevati dai sistemi di monitoraggio.

[24] Rientrano, ad esempio, in tali fattispecie, i quasi-incidenti che, ai sensi dell'articolo 2, comma 1, lettera u), del decreto, sono definiti come eventi che avrebbero potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato.

[25] Per una trattazione di sintesi si faccia riferimento all'Appendice A.

Ai fini dell'obbligo di notifica non è necessario valutare o risalire alla causa iniziale dell'incidente. Ciò che rileva, infatti, è che i suoi effetti siano riconducibili ad una delle tipologie di incidente sopraelencate, che possono essere dovute ad eventi sia di natura intenzionale, che accidentale come, ad esempio, il guasto o il malfunzionamento dei sistemi, anche generati a causa di un errore umano.

Acquisita l'evidenza del verificarsi di una delle tipologie di incidente sottoposte all'obbligo di notifica – ai sensi di quanto previsto dall'articolo 5, comma 1, del decreto – i soggetti trasmettono al CSIRT Italia:

a) senza ingiustificato ritardo, e comunque entro **24 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;
b) senza ingiustificato ritardo, e comunque entro **72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **notifica** dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;
d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:
   - una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
   - il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;
   - le misure di attenuazione adottate e in corso;
   - ove noto, l'impatto transfrontaliero dell'incidente;
e) in caso di incidente in corso al momento della trasmissione della relazione finale, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

Come osservato in Ruoli e responsabilità per la gestione degli incidenti, la figura del soggetto deputata alle interlocuzioni con lo CSIRT Italia e ad effettuare le notifiche obbligatorie degli incidenti significativi (e quelle volontarie) è il *Referente CSIRT* (e gli eventuali sostituti).

Nell'ambito delle interlocuzioni con lo CSIRT Italia potrebbe tuttavia rendersi necessario adottare decisioni che non rientrano nelle competenze del Referente CSIRT.

Per garantire che le informazioni siano trasmesse con tempestività alle strutture e figure competenti, devono essere pertanto definiti ruoli, responsabilità, fasi e procedure per l'assunzione di tali decisioni, che nei casi più rilevanti spettano agli organi di amministrazione e direttivi.

Tali elementi devono essere riportati nel *piano per la gestione degli incidenti* previsto dalla misura **RS.MA-01** che indica – per l'appunto – le fasi e le procedure di gestione e notifica degli incidenti, con l'indicazione dei relativi ruoli e delle responsabilità, tra gli elementi minimi che devono essere ricompresi nel piano.

Nel caso in cui il soggetto non sia tenuto a notificare l'incidente allo CSIRT Italia, è comunque possibile procedere alla notifica volontaria di informazioni pertinenti – come, ad esempio, quelle relative a minacce informatiche e ai *quasi-incidenti* – sulla base di quanto previsto dall'articolo 26, comma 1, del decreto.

Per ulteriori chiarimenti e indicazioni sulla notifica degli incidenti significativi si può fare riferimento alle FAQ pubblicate sul sito dell'Agenzia all'indirizzo https://www.acn.gov.it/portale/faq/nis/misure-notifiche-base.

La trasmissione delle notifiche al CSIRT Italia, ivi incluse quelle ai fini dell'obbligo di notifica, è effettuata tramite il portale pubblicato all'indirizzo https://segnalazioni.acn.gov.it/.

Al riguardo, si osserva che nelle fasi iniziali di risposta all'incidente potrebbero non essere immediatamente disponibili tutte le informazioni richieste (ad esempio i servizi e gli utenti impattati o le vulnerabilità sfruttate), che sono generalmente acquisite a valle di un esame approfondito dell'incidente.

Tipicamente, si procederà pertanto alla trasmissione della pre-notifica (entro 24 ore dall'evidenza dell'incidente) con le informazioni effettivamente disponibili, per poi effettuare le attività di investigazione e tornare[26] quindi alla sotto-fase di *segnalazione* per trasmettere la notifica (entro 72 ore dall'evidenza dell'incidente).

Per maggiori approfondimenti sulla procedura di notifica verso l'Agenzia per la cybersicurezza nazionale si può far riferimento alla *guida alla notifica degli incidenti al CSIRT Italia*[27].

Nella sotto-fase di *segnalazione*, si procede inoltre a comunicare l'incidente alle parti interne (come, ad esempio, i vertici del soggetto o l'ufficio legale) ed esterne (come, ad esempio, utenti impattati, fornitori o altri soggetti coinvolti) interessate.

Ai sensi di quanto previsto dal punto **1** della misura **RS.CO-02**, qualora intimato dall'Agenzia per la cybersicurezza nazionale 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 è necessario comunicare ai destinatari dei propri servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi e 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.

Il **punto 2** della medesima misura prevede inoltre di 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.

Ai sensi di quanto previsto dall'articolo 33 del Regolamento (UE) 2016/679 (GDPR), qualora l'incidente di sicurezza comporti una **violazione di dati personali**, è inoltre necessario effettuare la notifica al *Garante per la protezione dei dati personali*, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

2.3.2. Investigazione

In questa sotto-fase viene esaminato in modo approfondito l'incidente. L'obiettivo è ricostruire possibilmente l'intera sequenza degli eventi occorsi (cosiddetta *cyber kill chain*), individuare la causa dell'incidente e valutare l'estensione della compromissione.

[26] Come osservato in precedenza, le varie sotto-fasi di risposta non seguono un ordine lineare e sono strettamente interlacciate tra loro.

[27] La guida è pubblicata all'indirizzo https://www.acn.gov.it/portale/w/guida-alla-notifica-degli-incidenti-informatici.

Considerato che le successive attività potrebbero far emergere nuovi elementi informativi tali da richiedere lo svolgimento di ulteriori attività di analisi e approfondimento per ricostruire la dinamica dell'incidente, potrebbe essere necessario tornare nuovamente alla sotto-fase di investigazione nel corso delle attività di risposta. Ad esempio, a seguito della notifica di incidente allo CSIRT Italia, questo potrebbe fornire nuovi elementi, quali indicatori di compromissione, per proseguire le attività di investigazione, o, ancora, durante la fase di eradicazione potrebbe essere rilevato un nuovo artefatto malevolo, che potrebbe richiedere di svolgere ulteriori approfondimenti sulla causa o sull'estensione dell'incidente.

Le attività di investigazione riguardano, ad esempio:

- l'acquisizione delle evidenze forensi;
- la valutazione del perimetro compromesso in termini di comprensione del contesto e dell'estensione dell'incidente;
- la caratterizzazione dell'incidente almeno in termini di categoria (ad esempio, *ransomware* oppure *DDOS*), gravità e impatto;
- l'esame dell'incidente tramite acquisizione di *log* dei sistemi, artefatti ed evidenze rilevati, correlazione di eventi e attività dell'attaccante, predisposizione della *timeline* degli eventi occorsi, identificazione del vettore di attacco e della possibile causa dell'incidente, individuazione e documentazione degli IOC;
- la definizione delle prime attività di risposta dell'incidente come, ad esempio, eventuali azioni di contenimento preventivo (e.g. disabilitazione delle utenze compromesse, isolamento dei sistemi compromessi dalla rete, blocco dei flussi di comunicazione da e verso gli indicatori di compromissione);
- la valutazione del supporto di terze parti per la gestione dell'incidente (ad esempio supporto per le indagini forensi);
- la valutazione della presenza di ulteriori vettori di attacco e meccanismi di persistenza multipli.

Con riferimento alla caratterizzazione dell'incidente, al fine di disporre di un *linguaggio comune* si può far riferimento alla tassonomia cyber dell'Agenzia per la cybersicurezza nazionale[28].

2.3.3. Contenimento

In questa sotto-fase viene circoscritto il perimetro dell'attacco in modo da limitare l'impatto dell'incidente ed evitarne l'estensione ad altri sistemi informativi e di rete. Se al termine della sotto-fase si rilevano ancora evidenze di compromissione, sarà necessario tornare alla sotto-fase di *investigazione*.

Le attività di contenimento riguardano, ad esempio:

- la definizione della strategia di contenimento tenendo conto almeno dell'esigenza di preservare le evidenze, dei requisiti di disponibilità dei servizi (livelli di servizio attesi), delle risorse umane e finanziarie disponibili, delle tempistiche;

[28] La tassonomia è pubblicata all'indirizzo https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn.

- l'isolamento dei sistemi e i segmenti di rete coinvolti nell'incidente prevedendo almeno di: implementare regole sui sistemi perimetrali in base agli indicatori di compromissione individuati, bloccare gli accessi non autorizzati e le sorgenti dei malware, disabilitare account compromessi;
- il monitoraggio delle eventuali attività malevole a seguito delle azioni di contenimento;
- la verifica della presenza di ulteriori possibili meccanismi di persistenza;
- l'aggiornamento della *timeline* dell'attacco con le evidenze rilevate in questa fase.

Al fine di garantire tracciabilità e coerenza delle azioni intraprese, è opportuno tracciare le attività di contenimento documentando almeno le seguenti informazioni:

- sistemi informativi e di rete impattati dalle attività;
- obiettivi delle attività di contenimento;
- attività di contenimento individuate e loro motivazioni;
- strutture tecniche e organizzative coinvolte nelle attività di contenimento;
- impatto stimato sull'operatività delle attività di contenimento;
- modalità di verifica dell'efficacia delle attività di contenimento;
- esiti attesi delle attività di contenimento.

2.3.4. Eradicazione

In questa sotto-fase viene rimossa ogni capacità di controllo e persistenza nella rete da parte dell'attaccante. Se al termine della sotto-fase sono rilevate ancora attività malevole, sarà necessario tornare alla sotto-fase di *Investigazione*.

Le attività di eradicazione riguardano, ad esempio:

- la bonifica delle credenziali utilizzate dall'attaccante;
- la rimozione degli artefatti malevoli dai sistemi e dalle reti interessate;
- la bonifica dei sistemi compromessi;
- la risoluzione o mitigazione delle vulnerabilità sfruttate dall'attaccante;
- l'installazione degli aggiornamenti, in particolare quelli di sicurezza;
- il monitoraggio delle eventuali reazioni dell'attaccante alle attività di eradicazione;
- l'aggiornamento della timeline dell'attacco con le evidenze rilevate in questa fase;
- l'esecuzione di ulteriori scansioni per verificare la presenza di malware.

Al fine di garantire tracciabilità e coerenza delle azioni intraprese, è opportuno tracciare le attività di eradicamento documentando almeno le seguenti informazioni:

- sistemi informativi e di rete impattati dalle attività;
- obiettivi delle attività di eradicazione;
- attività di eradicazione individuate e loro motivazioni;
- strutture tecniche e organizzative coinvolte nelle attività di eradicazione;
- modalità di verifica dell'efficacia delle attività di eradicazione;

- esiti attesi delle attività di eradicazione.

2.4. Ripristino

La fase di *ripristino* è finalizzata a riportare i sistemi informativi allo stato antecedente all'incidente, assicurandosi che tutto funzioni regolarmente.

Le attività di questa fase riguardano, ad esempio:

- la creazione di *golden/clean image*[29];
- la reinstallazione dei i sistemi a partire dalle *golden/clean image*;
- il ricollegamento in rete dei sistemi informativi e di rete bonificati;
- il monitoraggio dei sistemi per verificare l'efficacia delle attività.

Al fine di garantire tracciabilità e coerenza delle azioni intraprese, è opportuno tracciare le attività di ripristino documentando almeno le seguenti informazioni:

- sistemi informativi e di rete impattati;
- obiettivi delle attività di ripristino;
- attività di ripristino individuate e loro motivazioni;
- strutture tecniche e organizzative coinvolte nelle attività di ripristino;
- modalità di verifica dell'efficacia delle attività di ripristino;
- esiti attesi delle attività di ripristino.

Con riferimento alle attività di ripristino, il **punto 1** della misura **RC.RP-01** richiede – nell'ambito del piano per la gestione degli incidenti – di adottare e documentare 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 gli incidenti significativi oggetto di obbligo di notifica.

Per i *soggetti essenziali*, ai sensi del **punto 1** della misura **RC.CO-03**, è inoltre richiesto di adottare e documentare procedure per comunicare alle parti interne interessate, ivi incluse le articolazioni competenti del soggetto NIS, le attività di ripristino a seguito di un incidente.

2.5. Miglioramento

La fase di *miglioramento* si estende per l'intero ciclo di vita del processo ed è finalizzata a potenziare la capacità di gestione degli incidenti.

Riguarda principalmente attività come l'analisi post-incidente al fine di individuare eventuali carenze e valutare l'efficacia della risposta.

[29] Per immagine *golden* o *clean* si intende la copia originale e ben configurata di un sistema informativo che può essere utilizzata per ripristinare il sistema ad uno stato consistente, funzionante e non compromesso dal punto di vista della sicurezza.

A tal fine sono organizzate le cosiddette riunioni di *lesson learned* in cui si ha l'opportunità di trarre insegnamenti, alla luce di quanto emerso durante la gestione dell'incidente, dalle azioni intraprese e dalla loro efficacia e di individuare gli interventi correttivi e di potenziamento.

Nell'ambito di tali riunioni sono generalmente affrontate tematiche quali, ad esempio:

- la valutazione sulla corretta esecuzione delle procedure previste e della loro adeguatezza;
- le criticità emerse durante l'esecuzione del processo di risposta;
- l'identificazione di ruoli, responsabilità, interlocutori e autorità non chiari o non definiti;
- le proposte migliorative per la condivisione delle informazioni;
- la necessità di ulteriori strumenti o risorse per migliorare il rilevamento e il processo di gestione e risposta agli incidenti;
- le attività da realizzare per prevenire il ripetersi di incidenti simili;
- gli indicatori di compromissione (IOC) rilevati da monitorare;
- la valutazione dell'adeguatezza delle misure di sicurezza esistenti;
- l'identificazione delle politiche e delle procedure da modificare per evitare il ripetersi di incidenti simili.

Gli esiti di tali riunioni sono la base per definire gli interventi di miglioramento necessari per risolvere le questioni emerse durante la gestione dell'incidente e possono comprendere, ad esempio, l'aggiornamento delle politiche e delle procedure, l'implementazione di nuove logiche di rilevamento e la previsione di specifiche attività di formazione.

Con riferimento agli interventi di miglioramento, il **punto 1** della misura **ID.IM-01** richiede di definire, attuare e documentare un *piano di adeguamento*, approvato dagli organi di amministrazione e direttivi, che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza.

Questa sotto-fase comprende anche la valutazione periodica (tramite, ad esempio, autovalutazioni o valutazioni di terzi) delle prestazioni – anche attraverso l'utilizzo di indicatori e metriche (*Key Performance Indicator – KPI*[30]) – della gestione degli incidenti.

A tale riguardo, il **punto 3** della misura **ID.IM-01** richiede ai soggetti essenziali di definire, attuare, aggiornare e documentare 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.

Sulla base delle lezioni apprese durante la gestione degli incidenti, in questa sotto-fase sono anche aggiornati i piani dedicati alla *continuità operativa*, al *ripristino in caso di disastro* e alla *gestione delle crisi*, al fine di tenere in considerazione gli insegnamenti maturati e correggere le eventuali criticità riscontrate.

La definizione dei suddetti piani è richiesta dalla misura **ID.IM-04,** che indica gli elementi minimi che i piani devono comprendere:

[30] Esempi di KPI sono il *Mean Time to Detect (MTTD)* definito come il tempo medio impiegato per rilevare un incidente e il *Mean Time to Resolution/Repair (MTTR)* definito come il tempo medio necessario per risolvere un incidente.

- **piano di continuità operativa:** le finalità e l'ambito di applicazione, i ruoli e le responsabilità, i contatti principali e i canali di comunicazione (interni ed esterni), le condizioni per l'attivazione e la disattivazione del piano, le risorse necessarie, ivi compresi i backup e le ridondanze;
- **piano di ripristino in caso di disastro**: le finalità e l'ambito di applicazione, i ruoli e le responsabilità, i contatti principali e i canali di comunicazione (interni ed esterni), le condizioni per l'attivazione e la disattivazione del piano, le risorse necessarie, ivi compresi i backup e le ridondanze, l'ordine di ripristino delle operazioni, le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino;
- **piano di gestione delle crisi**: i ruoli e le responsabilità del personale e, se opportuno, dei fornitori, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le procedure specifiche da seguire, le modalità di comunicazione tra i soggetti e le autorità competenti.

I suddetti piani devono essere approvati dagli organi di amministrazione e direttivi, 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.

Appendice A – introduzione alle specifiche di base

Nell'ambito degli adempimenti del decreto NIS, sono previsti obblighi per gli organi di amministrazione e direttivi (articolo 23 del decreto), la gestione dei rischi per la sicurezza informatica (articolo 24 del decreto) e le notifiche di incidente (articolo 25 del decreto).

Ai sensi dell'articolo 42, comma 1, lettera c) del decreto NIS, l'Agenzia per la cybersicurezza nazionale, in qualità di Autorità nazionale competente NIS, può stabilire, in fase di prima applicazione, *modalità e specifiche di base* per assicurare la conformità dei soggetti NIS all'adempimento di tali obblighi.

Le modalità e le specifiche di base sono state stabilite dalla *determinazione obblighi di base*[31] che riporta i seguenti allegati tecnici**:**

- **Allegato 1**: misure di sicurezza di base per i soggetti importanti.
- **Allegato 2**: misure di sicurezza di base per i soggetti essenziali.
- **Allegato 3**: incidenti significativi di base per i soggetti importanti.
- **Allegato 4**: incidenti significativi di base per i soggetti essenziali.

Gli allegati tecnici costituiscono le cosiddette **specifiche di base**, ossia:

- le **misure di sicurezza di base** (indicate anche come **misure di sicurezza**) che i soggetti sono tenuti ad adottare per l'assolvimento degli obblighi di cui agli articoli 23 e 24 del decreto;
- le tipologie di **incidenti significativi di base** (indicati anche come **incidenti significativi**) che i soggetti sono tenuti a notificare al CSRIT Italia per l'assolvimento degli obblighi di cui all'articolo 25 del decreto.

Sistemi informativi e di rete

Oggetto delle misure di sicurezza e delle notifiche di incidente sono i **sistemi informativi e di rete** del soggetto. L'articolo 2, comma 1, lettera p), del decreto NIS definisce un *sistema informativo e di rete* come:

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

Il termine per l'adozione delle misure di sicurezza di base è fissato in **diciotto mesi** dalla ricezione, da parte del soggetto NIS della comunicazione di inserimento nell'elenco dei soggetti NIS[32] mentre quello per

[31] Determinazione di cui all'articolo 31, commi 1 e 2, del decreto NIS, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

[32] A partire dal 12 aprile 2025, l'Agenzia per la cybersicurezza nazionale ha provveduto a comunicare ai soggetti interessati il loro inserimento nell'elenco dei soggetti NIS.

l'adempimento dell'obbligo di notifica degli incidenti significativi di base è fissato in **nove mesi** dalla ricezione, da parte del soggetto NIS, della medesima comunicazione.

A seguire sono introdotti le misure di sicurezza e gli incidenti significativi di base. Per maggiori approfondimenti si può far riferimento alla **guida alla lettura delle specifiche di base** pubblicata dall'Agenzia per la cybersicurezza nazionale[33] di cui questa appendice è un compendio.

Misure di sicurezza di base

Le *misure di sicurezza*, definite al fine di ricomprendere i dieci elementi[34] indicati dall'articolo 24, comma 2, del decreto, sono state sviluppate in accordo al **Framework nazionale**[35] e sono organizzate in funzioni, categorie, sottocategorie e requisiti: ogni misura è costituita da un **codice identificativo**[36], una **descrizione** e uno o più **requisiti**: il *codice identificativo* e la *descrizione* fanno riferimento alle sottocategorie del Framework nazionale, i *requisiti* indicano ciò che è richiesto ai fini dell'implementazione della misura.

Nel complesso sono state definite **37** misure di sicurezza con **87** requisiti per i soggetti importanti e **43** misure di sicurezza con **116** requisiti per i soggetti essenziali.

Sono stati, infatti, definiti requisiti e misure di sicurezza aggiuntivi per i soggetti essenziali rispetto ai soggetti importanti, in considerazione di quanto indicato dall'*articolo 31* del decreto NIS che prevede di tener conto – nello stabilire gli obblighi – del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

L'articolo 31 è stato inoltre considerato anche ai fini della formulazione dei requisiti, prevedendo le seguenti clausole in specifici casi:

- **per almeno i sistemi informativi e di rete rilevanti**: il soggetto ha la facoltà di *limitare l'ambito di applicazione* delle relative disposizioni ai sistemi *informativi e di rete rilevanti*[37], definiti – ai sensi dell'articolo 1 della determinazione obblighi di base – come i *sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi per i quali il soggetto rientra nell'ambito di applicazione del decreto NIS*;
- **in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05**: il soggetto ha la facoltà di definire le modalità di attuazione del requisito (*come* è applicato) e l'ambito di attuazione del requisito (*dove* è applicato) in funzione dei risultati della valutazione del rischio fatta dal soggetto ai sensi della misura *ID.RA-05*;

---

[33] https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base.

[34] Come osservato in Premessa uno degli elementi indicati è la gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26.

[35] Il Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) è uno strumento di supporto alle organizzazioni che necessitano di strategie e processi volti alla protezione dei dati personali e alla sicurezza cyber. L'elemento principale è il cosiddetto Framework Core strutturato in funzioni, categorie e sottocategorie. Le misure di sicurezza di base fanno uso della versione 2025 del framework (https://www.cybersecurityframework.it/).

[36] Il codice identificativo è del tipo **XX**.**YY**-**NN**, dove **XX** rappresenta la funzione, **YY** la categoria ed **NN** la sottocategoria del Framework nazionale.

[37] La misura **GV.OC-04** richiede di mantenere un elenco dei sistemi informativi e di rete rilevanti.

- **fatte salve motivate e documentate ragioni normative o tecniche**: il soggetto ha la facoltà di derogare dall'applicazione del requisito se sussistono vincoli normativi (ad esempio, leggi o regolamenti) o tecnici (ad esempio, limiti tecnologici o operativi) che non ne permettano l'implementazione[38];
- **forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete**: il soggetto ha la facoltà di limitare l'*ambito di attuazione* delle relative disposizioni alle forniture la cui eventuale compromissione può determinare effetti sulla *sicurezza dei sistemi informativi e di rete* [39];.

Incidenti significativi di base

Le tipologie di *incidenti significativi* sono costituite da un codice identificativo e da una descrizione relativa alla fattispecie di incidente soggetto a notifica.

Nel complesso sono state definite 3 tipologie di incidenti significativi per i soggetti importanti e 4 tipologie di incidenti significativi per i soggetti essenziali[40].

Ogni tipologia di incidente può essere logicamente descritta da un modello costituito dai seguenti elementi:

- **condizione**: circostanza che determina l'obbligo di notifica;
- **compromissione**: evento di sicurezza per il quale si configura l'incidente significativo;
- **oggetto compromissione**: risorsa sul quale l'evento di sicurezza ha impatto.

Sulla base di tale modello, le tipologie di incidente possono essere rappresentate nella seguente tabella[41].

CODICE	CONDIZIONE	COMPROMISSIONE	OGGETTO COMPROMISSIONE
IS-1	Il soggetto ha evidenza	Perdita di riservatezza, verso l'esterno.	Dati digitali
IS-2		Perdita di integrità, con impatto verso l'esterno.	Dati digitali
IS-3		Violazione dei livelli di servizio attesi.	Servizi e/o attività
IS-4		Accesso non autorizzato o con abuso dei privilegi concessi	Dati digitali

[38] Qualora per motivate e documentate ragioni normative o tecniche non siano attuati i requisiti per i quali è prevista tale facoltà (requisiti indicati nella tabella 2 in appendice all'allegato delle misure di sicurezza), il soggetto dovrà motivare e documentare tali ragioni e, ai sensi del **punto 2** della misura **ID.RA-06**, dovrà adottare, ove applicabile, misure di mitigazione compensative e includere nel piano di trattamento del rischio (richiesto ai sensi del **punto 1** della misura **ID.RA-06**) la descrizione delle misure e dell'eventuale rischio residuo.

[39] L'articolo 2, comma 1, lettera q), del decreto definisce la sicurezza dei sistemi informativi e di rete come "*la capacità di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi*".

[40] In ragione delle medesime considerazioni fatte nello sviluppo delle misure di sicurezza, è stata infatti definita una tipologia di incidente significativo aggiuntiva per i soggetti essenziali.

[41] Per semplificazione non è riportata la dicitura completa delle varie tipologie di incidenti significativi.

Con riferimento alla **condizione**, si osserva che la circostanza che determina l'obbligo di notifica è che il soggetto abbia **evidenza** dell'incidente, ossia dispone di elementi oggettivi dai quali si evince che è occorso un incidente di sicurezza informatica.

Con riferimento alla **compromissione**:

- la *perdita di riservatezza verso l'esterno* si configura quando dati digitali, che dovrebbero essere accessibili solo a utenti o sistemi autorizzati, sono divulgati o esposti, in modo intenzionale o accidentale, a utenti o sistemi esterni al soggetto, configurando così una compromissione che comporta la fuoriuscita dei dati verso l'esterno. Esempi di tale fattispecie sono l'esfiltrazione di documenti dagli archivi dell'organizzazione o l'esposizione sulla rete *Internet* di credenziali degli utenti;
- la *perdita di integrità con impatto verso l'esterno* si configura quando dati digitali sono modificati senza autorizzazione determinando impatti verso utenti o sistemi esterni al soggetto. Esempi di tale fattispecie sono il *defacement* del sito web dell'organizzazione, la corruzione o l'alterazione di un database che rende disponibili all'esterno dati inconsistenti o errati;
- la *violazione dei livelli di servizio attesi* si configura quando i livelli di servizio attesi – definiti dal soggetto ai sensi di quanto previsto dalla misura DE.CM-01 – non sono rispettati. Esempi di tale fattispecie sono l'indisponibilità del sito *web* per oltre 30 minuti consecutivi o la limitata disponibilità di un servizio *online* per oltre il 5% degli utenti[42];
- l'*accesso non autorizzato o con abuso dei privilegi concessi* si configura quando un utente o un sistema ottiene accesso a dati digitali senza avere i permessi o i diritti per farlo. L'uso della dicitura *con abuso dei privilegi concessi* ricomprende quelle fattispecie in cui un utente, ivi inclusi quelli con privilegi amministrativi, ha l'*autorizzazione tecnica*[43] per accedere a determinati dati ma utilizza tale accesso in modo illecito, ad esempio in violazione delle politiche dell'organizzazione o per perseguire scopi estranei alle necessità funzionali per le quali gli è stato attribuito l'accesso. Esempi di tali fattispecie sono l'uso di credenziali rubate per accedere a specifici *account* di posta elettronica o la consultazione di banche dati da parte di personale che ha l'autorizzazione tecnica ad accedervi, ma in violazione delle politiche.

Con riferimento all'**oggetto della compromissione**:

- per *dati digitali di proprietà del soggetto* si intendono i dati creati dall'organizzazione o dei quali ne assume la titolarità, mentre per i *dati digitali sui quali esercita il controllo anche parziale* si intendono i dati per i quali non si detiene la proprietà, ma si dispone di una responsabilità, anche parziale, per il loro trattamento, in forza di contratti, accordi o della normativa vigente, come ad esempio nel caso di un fornitore di servizi *cloud* che gestisce, tramite i propri sistemi informativi e di rete, i dati di un cliente;
- per *servizi e attività* si intende tutto quello che *fa* un'organizzazione per il perseguimento dei propri obiettivi, come, ad esempio, la produzione, la logistica o la gestione del personale[44].

[42] Nel primo caso sarà stato definito, come livello di servizio atteso, che il sito web non deve essere indisponibile per più di 30 minuti consecutivi, nel secondo che il servizio *online* deve essere disponibile per almeno il 95% degli utenti.

[43] Per autorizzazione tecnica si intende la disponibilità di credenziali che sono configurate per accedere ai dati.

[44] Nelle attività e servizi sono ricompresi anche le attività e i servizi di supporto.

Appendice B – misure di sicurezza gestione incidenti

Sono di seguito elencate le misure di sicurezza, e i relativi requisiti in forma tabellare[45], relative alle varie fasi del processo di gestione degli incidenti[46].

Preparazione – Governo

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.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
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.	●	●
3	Le politiche di cui al punto 1 sono approvate dagli organi di amministrazione e direttivi e rese note alle articolazioni competenti del soggetto NIS tenuto anche conto della necessità di conoscere (need to know).	●	●

[45] Il cerchio pieno di colore blu nella colona S_I indica che il corrispondente requisito si applica ai soggetti importanti e Il cerchio pieno di colore verde nella colona S_E indica che il corrispondente requisito si applica ai soggetti essenziali.

[46] La misura RS.MA-01 riguarda il piano di gestione degli incidenti ed è qui riportata nella fase di risposta, deve tuttavia considerarsi estesa a tutte le fasi del processo.

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.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
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.	●	●
3	È mantenuto un registro aggiornato contenente gli esiti del riesame di cui al punto 1.		●

GV.RR-02: I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
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.	●	●
3	All'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, sono inclusi il punto di contatto e il suo sostituto, il referente CSIRT e gli eventuali suoi sostituti, di cui alla determinazione adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.	●	●
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.	●	●

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.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
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.	●	●

Preparazione – Identificazione

ID.AM-01: Sono mantenuti gli inventari dell'hardware gestito dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
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.	●	●

ID.AM-02: Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
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 accessibili tramite API, approvati da attori interni al soggetto NIS.	●	●

ID.AM-03: Sono mantenute le rappresentazioni delle comunicazioni di rete e dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione.

PUNTO	REQUISITO	S_I	S_E
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.		●

ID.AM-04: È mantenuto un inventario aggiornato dei servizi informatici erogati dai fornitori, ivi inclusi i servizi *cloud*.

PUNTO	REQUISITO	S_I	S_E
1	È mantenuto un inventario aggiornato dei servizi informatici erogati dai fornitori, ivi inclusi i servizi *cloud*.	●	●

ID.RA-01: Le vulnerabilità negli asset sono identificate, confermate e registrate.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
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*.		●
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.		

Preparazione – Protezione

PR.DS-11: I backup dei dati sono creati, protetti, mantenuti e verificati.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
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.		●
4	Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
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.		●

PR.PS-04: I registri di *log* sono generati e resi disponibili per il monitoraggio continuo.

PUNTO	REQUISITO	S_I	S_E
1	Tutti gli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi sono registrati.	●	●
2	Per almeno i sistemi informativi e di rete rilevanti, sono acquisiti e, in modo sicuro e possibilmente centralizzato, conservati almeno i *log* necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto 1.	●	●
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.	●	●
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.	●	●

PR.IR-01: Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.

PUNTO	REQUISITO	S_I	S_E
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.	●	●

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.	●	●
3	Sono presenti, aggiornati, mantenuti e configurati in modo adeguato i sistemi perimetrali, quali firewall.	●	●
4	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 2 e 3.	●	●

PR-IR-03: Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.

PUNTO	REQUISITO	S_I	S_E
1	In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono utilizzati sistemi di comunicazione di emergenza protetti.		●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.		●

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.

PUNTO	REQUISITO	S_I	S_E
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: c) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita; d) le eventuali modalità di verifica dell'acquisizione dei contenuti.	●	●
2	Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.	●	●
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.	●	●

PR-AT-02: 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.

PUNTO	REQUISITO	S_I	S_E
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: e) le istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete; f) le informazioni sulle minacce informatiche note;		●

	g) le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.		
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.		●

Rilevamento

DE.CM-01: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
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.	●	●
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.	●	●
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).		●
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, ai punti terminali (endpoint) e agli applicativi al fine di rilevare gli eventi di sicurezza informatica.		●
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.		●
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.		●

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.

PUNTO	REQUISITO	S_I	S_E
1	Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione dei punti terminali (endpoint) per il rilevamento del codice malevolo.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●

Risposta

RS.MA-01: Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

PUNTO	REQUISITO	S_I	S_E
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: h) le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità; i) 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; j) le informazioni di contatto per la segnalazione degli incidenti; k) le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna; l) la reportistica da utilizzare per la documentazione dell'incidente.	●	●
2	Il piano di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.	●	●
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.	●	●

RS.CO-02: Gli stakeholder interni ed esterni sono informati degli incidenti.

PUNTO	REQUISITO	S_I	S_E
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 propri servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi; b) ai destinatari dei propri 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.	●	●
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.	●	●

Ripristino

RC.RP-01: La parte del piano di risposta agli incidenti relativa al ripristino viene eseguita una volta avviata dal processo di risposta agli incidenti.

PUNTO	REQUISITO	S_I	S_E
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.	●	●

RC.CO-03: Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati.

PUNTO	REQUISITO	S_I	S_E
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.		●

Miglioramento

ID.IM-01: Sono identificati miglioramenti in esito alle valutazioni.

PUNTO	REQUISITO	S_I	S_E
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.	●	●
2	Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sugli esiti dei piani di cui al punto 1.	●	●
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.		●
4	Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sul piano di valutazione dell'efficacia di cui al punto 3.		●

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.

PUNTO	REQUISITO	S_I	S_E
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, ivi incluse le esigenze di continuità operativa, 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.		
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, ivi incluse le esigenze di ripristino in caso di disastro, 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.	●	●
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 le 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.	●	●
4	I piani di cui ai punti 1, 2 e 3 sono approvati dagli organi di amministrazione e direttivi.	●	●
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.	●	●