ISTITUTO NAZIONALE DI FISICA NUCLEARE

CONSIGLIO DIRETTIVO

DELIBERAZIONE n. 17602

Oggetto: Approvazione del Piano di Risposta agli Incidenti Informatici nell'INFN

Il Consiglio Direttivo dell'Istituto Nazionale di Fisica Nucleare, riunito in Roma in data 19/12/2025 alla presenza di n. 34 suoi componenti su un totale di n. 34

Visti

- il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR);
- il Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche e integrazioni, recante il "Codice in materia di protezione dei dati personali";
- il Decreto Legislativo 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679;
- il provvedimento n. 9126951 del 30 luglio 2019 del Garante per la Protezione dei Dati Personali sulla notifica delle violazioni dei dati personali (data breach);
- la legge 28 maggio 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici;
- la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (di seguito: direttiva NIS2);
- il decreto legislativo 4 settembre 2024, n. 138 (di seguito: decreto NIS), con cui l'Italia ha recepito la direttiva (UE) 2022/2555;
- la determinazione ACN n. 164179 del 14 aprile 2025 e suoi allegati, recante le "Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS";
- la determinazione del Direttore Generale ACN n. 136430 del 12 aprile 2025, con cui l'INFN è stato individuato come soggetto importante ai sensi del decreto NIS;
- la deliberazione di questo Consiglio n. 14844 del 27 luglio 2018, che ha definito l'organizzazione del trattamento dei dati personali all'interno dell'INFN;
- la lettera di trasmissione del Direttore Generale del 23 luglio 2019, relativa alla procedura di gestione data breach;
- l'articolo 12, comma 4, lettera i) dello Statuto dell'Istituto Nazionale di Fisica Nucleare in materia di attribuzioni del Consiglio Direttivo;
- la proposta del presidente di Commissione Calcolo e Reti di adottare per l'INFN il piano di risposta agli incidenti informatici sviluppato ed approvato dalla stessa Commissione di concerto con il RTD.

Considerato

- prioritario definire le procedure per ottemperare agli obblighi di notifica degli incidenti informatici, conformandosi alle prescrizioni del decreto NIS;
- altresì prioritario dotare l'Ente di un Piano di Risposta agli Incidenti Informatici sulle infrastrutture informatiche dell'Ente che includa tali procedure;
- che l'esecuzione della presente deliberazione non comporta oneri aggiuntivi di bilancio.

Direzione Sistemi Informativi
cd-A/02

Sentito

- il Data Protection Officer (DPO) dell'INFN.

Acquisito

- il parere della Giunta Esecutiva

Con n. 34 voti favorevoli

DELIBERA

1. di approvare il Piano di Risposta agli Incidenti Informatici per l'INFN, allegato alla presente deliberazione quale parte integrante e sostanziale.

Titolario	**Approvazione del Piano di Risposta agli Incidenti Informatici nell'INFN**		
Data GE		**Data CD**	
Componente di Giunta competente	**D. Bettoni**		
Persona Referente			
Struttura Proponenente	**CCR**		
Direzione AC che ha curato l'istruttoria	**DSI**		
Tipologia di Atto (breve descrizione)	Approvazione del Piano di Gestione degli Incidenti Informatici.		
costo complessivo	0,00		
copertura finanziaria anno	**progetto**	**capitolo di spesa**	**importo**
Allegato 1			
Allegato 2			
Allegato 3			
Note o riferimenti Atti precedenti	Adozione del piano di risposta agli incidenti in ottemperanza agli obblighi derivanti dal decreto NIS e dalle successive determinazioni di ACN. L'obbligo di segnalazione degli incidenti, che e' parte del piano, scatta a partire dal 1/1/2026.		

Piano di Risposta agli Incidenti Informatici

Doc. Id	*Vers.*	*Data*	*Stato*
INFN-PIA-IR	1.4	02/12/2025	Approvato

Obiettivi del piano

- Minimizzare l'impatto degli incidenti informatici sulle infrastrutture di calcolo dell'Ente e sui servizi da queste erogati.
- Salvaguardare **dati di ricerca, amministrativi e personali** in conformità alle prescrizioni della normativa vigente.
- Garantire la continuità operativa e la resilienza informatica dell'Ente.

Ambito di Applicazione

Il presente piano è valido per:

- Infrastrutture fisiche e virtuali di calcolo scientifico dell'Ente (es. TIER, cluster HPC, infrastrutture CLOUD, cluster per la virtualizzazione/containerizzazione...)
- Sistemi infrastrutturali centrali e locali che erogano servizi al personale e/o a terzi (Servizi Nazionali, DNS, infrastrutture di gestione della posta elettronica, infrastruttura AAI, applicativi amministrativi, server web centrali/di struttura/di esperimento, ...)
- Risorse di calcolo personale utilizzate da dipendenti, associati, ospiti o visitatori
- Risorse di rete fisiche e logiche

Definizione di Incidente Informatico

Qualsiasi evento non autorizzato che minacci di mettere o metta significativamente a repentaglio integrità riservatezza o disponibilità dei sistemi informativi o dei dati da essi trattati, o che minacci di costituire o costituisca una violazione della legge, delle politiche e procedure di sicurezza o delle

politiche di utilizzo accettabile dell'Ente (si veda anche l'Allegato 3 alla determinazione ACN 164179 del 14/4/2025)

Ruoli e Responsabilità

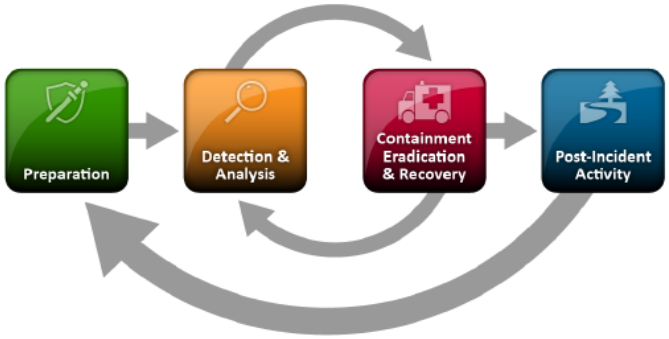
Ruolo	**Responsabilità**
CSIRT INFN (*incident manager*)	Attivazione, coordinamento e gestione IRP; supporto nella gestione degli incidenti (preparazione, analisi, mitigazione, ripristino), reportistica, rapporti con CSIRT terzi, coordinamento comunicazioni con CSIRT Italia/ACN e organismi investigativi
CSIRT manager	Coordinatore CSIRT INFN o suo vice
Referente Security locale (*incident handler*)	Identificazione, comunicazione a CSIRT INFN, contenimento, analisi degli incidenti, raccolta dati, aggiornamento registro locale degli incidenti; comunicazione a DPO eventuale data breach
APM	Contatto tecnico verso GARR anche per eventi di sicurezza informatica. Inoltra le segnalazioni di GARR-CERT al Referente Security Locale e risponde alle relative segnalazioni
Amministratore di sistema (AdS)/utente privilegiato/proprietario degli asset coinvolti	Segnalazione degli incidenti al team responsabile delle risorse informatiche; collaborazione nella raccolta delle informazioni sull'asset e sull'incidente; eventuale assistenza sistemistica
Team responsabile delle risorse informatiche coinvolte	Supporto sistemistico in tutte le fasi di gestione dell'incidente.
NUCS INFN	Elaborazione e aggiornamento politiche di sicurezza in collaborazione con la Struttura di Coordinamento della Sicurezza informatica dell'Ente ex lege 90
Punto di Contatto ACN e suo sostituto (NIS2)	Comunicazioni con ACN
Referente CSIRT e suoi sostituti	Segnalazione incidenti significativi a CSIRT Italia
DPO	Rapporti con il Garante Privacy, compliance con GDPR
Ufficio Comunicazione	Gestione comunicazioni esterne (ove necessarie)
Dirigenza Ente (Management)	Organo amministrativo/direttivo centrale con responsabilità di approvazione delle politiche di sicurezza
Unità di crisi	Organo di gestione delle crisi nell'INFN con responsabilità di gestire eventi con impatto critico per l'INFN

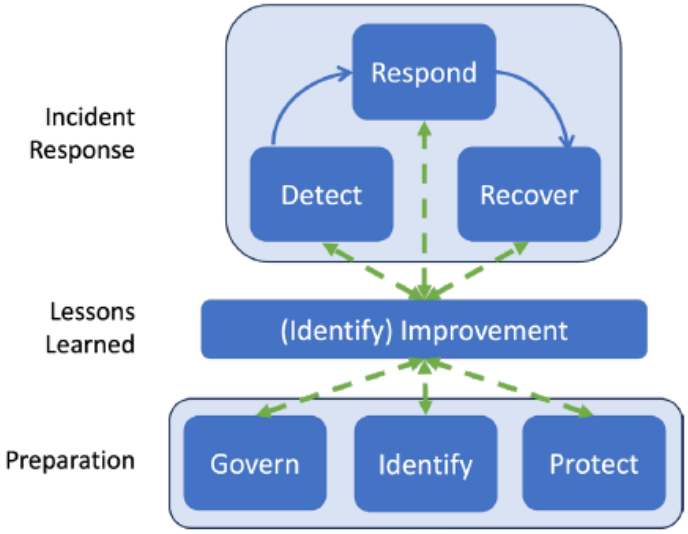
Ruolo	Responsabilità
Direttore di riferimento (Management)	Organo amministrativo/direttivo della struttura a cui appartengono gli asset coinvolti
CCR	Struttura di Coordinamento della Sicurezza Informatica dell'Ente ex lege 90, elaborazione e aggiornamento politiche e procedure di sicurezza in collaborazione con l'RTD ed il NUCS.
RTD	Coordinamento Sicurezza Informatica dell'Ente, elaborazione delle politiche di sicurezza in collaborazione con CCR e NUCS

Contatti con le Autorità - matrice dei contatti

Autorità	Quando contattare	Referente interno	Canale ufficiale
Garante Privacy	Entro 72 ore in caso di violazione dati personali (GDPR)	Direttore di riferimento, DPO	PEC istituzionale/portale segnalazione data breach
CSIRT Italia	Entro 24/72 ore in caso di incidente significativo ai sensi della NIS2	Referente CSIRT, CSIRT INFN	Portale ACN / PEC istituzionale/ canale dedicato referente
ACN	Registrazione, comunicazioni su organizzazione e adempimenti	Punto di contatto ACN e suo sostituto	Portale ACN
Polizia Postale e delle Comunicazioni	Attacchi gravi con implicazioni legali (es. ransomware, frodi, furti dati)	CSIRT Manager, Management, Direttore di riferimento	PEC istituzionale

Fasi della Risposta e relazioni con le funzioni fondamentali del CSF





La fase di preparazione è comune a tutti gli incidenti informatici, a prescindere dalla loro tipologia e gravità; la successiva fase di Risposta varia in relazione agli obblighi di segnalazione pertinenti alla significatività dell'incidente e alla natura dei dati su cui questo ha avuto impatto.

Preparazione

A cura della CCR, RTD, NUCS, con la consulenza dell'Ufficio Legale:

- Predisposizione politiche e procedure di sicurezza
- Individuazione strumenti di gestione degli eventi di sicurezza
- Predisposizione di PlayBook per casi di particolare rilevanza/criticità.

A cura del team responsabile delle risorse di calcolo, degli AdS o dei proprietari degli asset:

- Verifica periodica aderenza a politiche di sicurezza adottate dall'INFN;
- Predisposizione, gestione e controllo backup
- Predisposizione e aggiornamento continuo Inventario asset
- Valutazione periodica del rischio informatico e gestione delle vulnerabilità
- Predisposizione e gestione strumenti di rilevazione/identificazione/analisi eventi di sicurezza (SIEM, EDR, IDS, IPS, log sistemi e firewall, ...)

Risposta: rilevamento, identificazione e classificazione preliminare

Amministratori di sistema, asset owner o utenti che dovessero rilevare un potenziale incidente di sicurezza devono informare appena possibile il team responsabile delle risorse informatiche di riferimento, che a sua volta informa immediatamente l'Incident Handler.

Qualora la segnalazione venisse riportata dall'esterno su una casella PEC istituzionale, l'informazione deve essere inoltrata immediatamente allo CSIRT INFN, via mail (csirt@infn.it) o PEC (csirt@pec.infn.it), che a sua volta informa immediatamente l'incident handler della struttura interessata.

Segalazioni provenienti da GARR-CERT ed indirizzate all'APM locale devono essere immediatamente inoltrate all'Incident Handler della struttura interessata.

L'incident handler, una volta rilevato un evento di sicurezza attraverso qualsiasi fonte, ad esempio:

- Compromissione palese di riservatezza, integrità o disponibilità di dati o servizi (DDOS, invio massivo di messaggi di SPAM, violazione account, ...)
- Sistemi di logging e allarmistica in produzione;
- Segnalazione da AdS, da asset owner o da utenti
- Segnalazione da CSIRT INFN
- Segnalazione da CSIRT/CERT terzi
- Segnalazione della Polizia Postale e delle Comunicazioni

si fa carico della prima analisi dello stesso, ne dà tempestiva comunicazione a CSIRT INFN e collabora con quest'ultimo a una sua classificazione preliminare che tenga conto:

1. della gravità dell'incidente, e se questo si configuri come significativo ai sensi del Decreto NIS2 (cioè, se ha 'causato una significativa interruzione dei servizi o una perdita finanziaria rilevante per l'entità interessata', o se ha 'interessato altre persone fisiche o giuridiche causando danni materiali o immateriali considerevoli' – si vedano le Appendici per la definizione puntuale);
2. della natura dei dati eventualmente compromessi dall'incidente, ovvero se questo abbia avuto o meno impatto su dati personali

Incidente non significativo ai sensi del Decreto NIS2

L'incident handler ne dà formale comunicazione, tempestivamente e comunque non oltre 2 ore, a:

- Direttore di Riferimento;
- Team responsabile delle risorse di calcolo;
- AdS/Asset owner (se del caso);
- utenti eventualmente impattati dall'evento (se del caso).

e collabora con lo CSIRT INFN:

- all'analisi dell'evento;

- all'assegnazione di un livello di gravità e alla classificazione dell'evento ai sensi della Tassonomia Cyber di ACN (vedi Appendice) e alla conseguente assegnazione di una priorità alle operazioni di gestione;
- alla raccolta delle informazioni essenziali necessarie alla descrizione puntuale dell'evento, con particolare riferimento a:
    - data e ora di rilevamento dell'incidente;
    - asset impattati;
    - vettori d'attacco;
    - eventuali indicatori di compromissione (IOC);
    - eventuali evidenze rilevanti (log, script, ...);
    - misure di mitigazione immediata intraprese e/o pianificate.
- al salvataggio in un'area ad accesso limitato del sistema documentale dell'Ente di tutte le informazioni di cui sopra nonché di una descrizione di tutte le azioni di gestione dello stesso (analisi, mitigazione, contenimento, ...)
- all'aggiornamento del Registro degli Incidenti locale, copia del quale verrà trasmessa a CSIRT INFN

Incidente significativo

L'incident handler segue la procedura per la gestione di un incidente non significativo e provvede inoltre:

- a trasmettere entro 4 ore a CSIRT INFN tutta le informazioni necessarie alla redazione della segnalazione preliminare da inviare a CSIRT Italia entro 24 ore dal rilevamento dell'incidente, che includano almeno, se possibile:
    - tipologia dell'incidente significativo (vedi appendice)
    - se l'incidente possa ritenersi il risultato di atti illegittimi o malevoli
    - se possa avere impatto transfrontaliero
- alla stesura, in collaborazione con CSIRT INFN e gli eventuali altri attori coinvolti nella gestione dell'incidente, del rapporto dettagliato da inviare a CSIRT Italia entro 72 ore dal rilevamento dell'incidente, che includa almeno, se possibile:
    - un aggiornamento delle informazioni relative alla segnalazione preliminare
    - una valutazione di gravità e impatto
    - eventuali indicatori di compromissione
- alla redazione, in collaborazione con CSIRT INFN e gli eventuali altri attori coinvolti nella gestione dell'incidente, di una relazione finale da inviare a CSIRT Italia entro 1 mese, se l'incidente è stato chiuso, o di un aggiornamento intermedio in caso contrario, contenente almeno:
    - la tipologia dell'incidente significativo (vedi appendice)
    - la descrizione completa dell'incidente, della gravità del suo impatto
    - le cause principali, ed il tipo di minaccia
    - le misure adottate per contenerne gli effetti e prevenirne il ripetersi

È responsabilità del referente CSIRT l'interazione con CSIRT Italia in relazione all'incidente: invio di segnalazioni, relazioni intermedie e conclusiva, risposte a eventuali richieste di informazioni.

È responsabilità' del referente CSIRT e del Punto di Contatto ACN inoltrare al Management l'eventuale richiesta di ACN di dare avviso pubblico dell'incidente. L'avviso sarà pubblicato sul sito web istituzionale dell'INFN o della struttura coinvolta, a seconda del perimetro impattato.

Il coordinamento di altre comunicazioni di natura tecnica con strutture INFN terze o CSIRT di organizzazioni esterne eventualmente impattate o genericamente coinvolte nell'incidente sarà responsabilità dello CSIRT INFN nella sua qualità di Incident Manager.

I rapporti con ulteriori entità esterne non tecniche direttamente o indirettamente coinvolte saranno curati dalla Dirigenza dell'INFN, eventualmente attraverso l'Ufficio di Comunicazione, in collaborazione con CSIRT INFN e se opportuno con la consulenza dell'Ufficio Legale, che deve essere obbligatoriamente coinvolto nella gestione dell'incidente nel caso questo minacci di avere conseguenze giuridicamente rilevanti.

Incidente con impatto su dati personali (perdita di riservatezza, integrità o disponibilità)

A prescindere dalla significatività dell'incidente, in caso di violazione accertata di dati personali (data breach: compromissione credenziali, diffusione non autorizzata di dati etc.), l'incident handler:

- notifica la violazione al Direttore di Riferimento e agli utenti interessati;
- collabora con il Direttore di Riferimento e col referente locale del DPO alla stesura di una segnalazione da inviare al DPO INFN e, ove necessario e sentito il DPO INFN, al GPDP attraverso il portale https://servizi.gpdp.it/databreach/s/, rispettando il limite di 72 ore.

Coinvolgimento dell'Unità di Crisi dell'INFN

Qualora l'incidente abbia un potenziale impatto che minacci gli obiettivi strategici, la reputazione o la sopravvivenza dell'INFN, il Direttore di riferimento attiva la procedura di gestione delle crisi nell'INFN, informando immediatamente l'Unità di Crisi dell'INFN, ed informa della decisione lo CSIRT INFN.

Tutte le successive azioni di gestione dell'incidente saranno portate avanti in stretta collaborazione con l'Unità di Crisi.

Contenimento

Le operazioni di contenimento a breve e lungo termine sono coordinate dall'Incident Handler con la collaborazione di CSIRT INFN, sono a cura del team responsabile delle risorse di calcolo e dell'AdS/asset owner, devono essere effettuate con priorità proporzionale alle gravità dell'incidente e in ogni caso **senza precludere la possibilità di portare a termine l'analisi di cui al punto precedente** (avendo, cioè, cura di preservare tutte le evidenze rilevanti senza cancellare dati, reinstallare sistemi, effettuare upgrade):

Gravità incidente	**Priorità di gestione - tempo di risposta**
Alta	Immediato – meno di 1 ora dalla rilevazione
Media	2 ore
Bassa	8 ore

Operazioni di contenimento a breve termine:

- Isolamento nodi compromessi
    - disconnessione fisica/logica interfacce di rete
    - spostamento su rete privata dedicata
- Disabilitazione servizi/processi coinvolti
- Disabilitazione account sospetti/coinvolti
- Altre azioni finalizzate alla limitazione del perimetro colpito dall'incidente ed al contenimento degli effetti sui sistemi e servizi informatici dell'INFN

Operazioni di contenimento a lungo termine:

- Aggiornamento S/W, Installazione patch, applicazione mitigazioni
- Aggiornamento regole firewall, riconfigurazione rete (segmentazione)
- Aggiornamento backup policy
- Aggiornamento policy EDR/SIEM
- Disattivazione selettiva accessi remoti
- Modifica credenziali
- ...

Eradicazione e ripristino

Le operazioni di eradicazione e ripristino sono coordinate dall'Incident Handler con la collaborazione di CSIRT INFN, sono a cura del team responsabile delle risorse di calcolo e dell'AdS/asset owner e devono essere effettuate **solo dopo avere raccolto e salvato in un'apposita area ad accesso limitato del sistema documentale dell'Ente tutte le evidenze digitali relative all'incidente e ai sistemi coinvolti** utili per l'analisi post mortem o per una successiva analisi forense (ove necessaria).

La decisione ultima sul ritorno in produzione di sistemi coinvolti in incidenti, ovvero la riabilitazione di account violati, è responsabilità di CSIRT INFN sentiti il Direttore di riferimento e il team responsabile delle risorse di calcolo, e può avvenire solo dopo avere verificato il loro corretto funzionamento per un periodo di tempo adeguato (normalmente proporzionale all'entità dell'incidente e degli interventi di eradicazione e ripristino).

Attività di eradicazione

- Rimozione software malevolo
- Rimozione accessi illeciti
- Validazione dell'integrità dei software
- Analisi forense

Attività di ripristino

- Reinstallazione sistema/ripristino da backup validati

- Applicazione di tutti gli eventuali aggiornamenti di sicurezza pubblicati dopo la data di esecuzione del backup
- Riammissione controllata in rete
- Verifica della funzionalità e monitoraggio dedicato
- Ripristino account
- Ripristino servizi esposti

Attività post incidente: post mortem e lezioni apprese

Tutti gli incidenti di sicurezza devono essere documentati nel Registro degli incidenti della struttura interessata a cura dell'Incident Handler e nel Registro degli incidenti centrale a cura di CISRT INFN (vedi Appendice); i citati registri devono contenere, per ogni incidente, una descrizione sommaria dello stesso e delle attività svolte per la sua gestione

Per ogni incidente dovrà essere inoltre redatto entro un mese dalla chiusura dell'incidente, un report dettagliato conclusivo, che verrà archiviato - unitamente a tutte le relative evidenze digitali – in un'apposita area ad accesso controllato del sistema documentale dell'ente. Il report conterrà anche le risultanze dell'attività di analisi post mortem che impegnerà tutti i soggetti coinvolti nella gestione dello stesso e sarà funzionale a individuare:

- Eventuali criticità:
    - mancanza/carenza di
        - competenze
        - strumenti di prevenzione
        - strumenti di rilevamento o analisi
        - aderenza alle politiche di sicurezza;
        - documentazione sugli asset
    - difetti di
        - configurazione sistemi
        - comunicazione;
        - collaborazione
- Eventuali aggiornamenti/migliorie a procedure e strumenti utilizzati.

Lo CSIRT INFN si farà carico di valutare le azioni proposte per avviare, ove necessario, un processo di revisione di politiche, procedure o misure tecniche nelle sedi opportune (CCR, NUCS).

I dati relativi alle evidenze forensi (log, tracce su disco) devono essere salvati in formato criptato.

Riesame periodico e aggiornamento del Piano

Il presente piano è aggiornato a cura della CCR e del RTD almeno una volta ogni due anni, o se necessario in caso di incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.

Le modifiche al piano sono approvate dal Consiglio Direttivo dell'INFN, sentito il parere della Giunta Esecutiva, su proposta della CCR di concerto con il RTD.

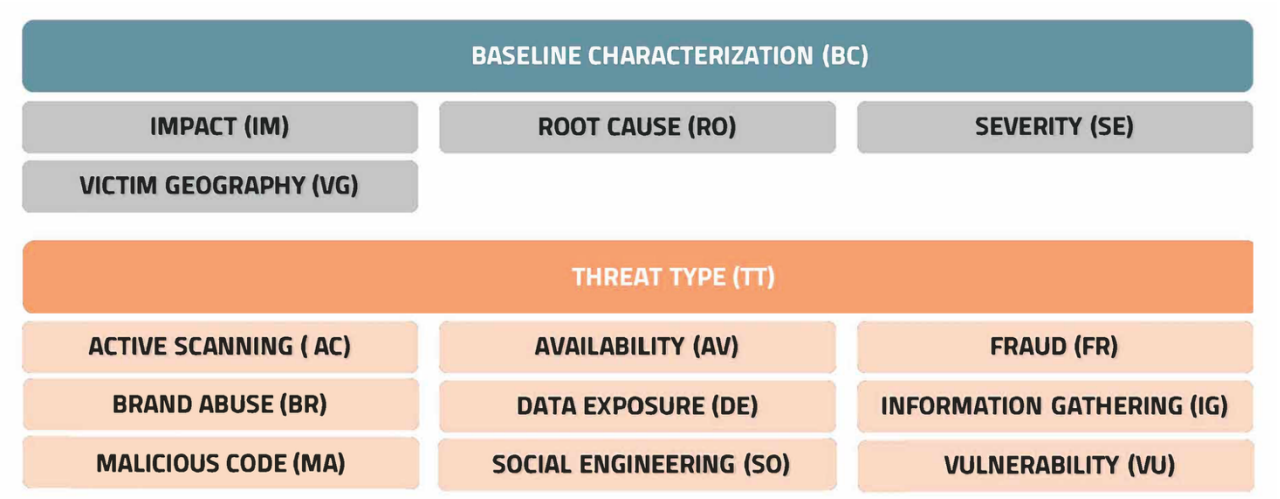
Appendice

Incidenti significativi di base per soggetti importanti

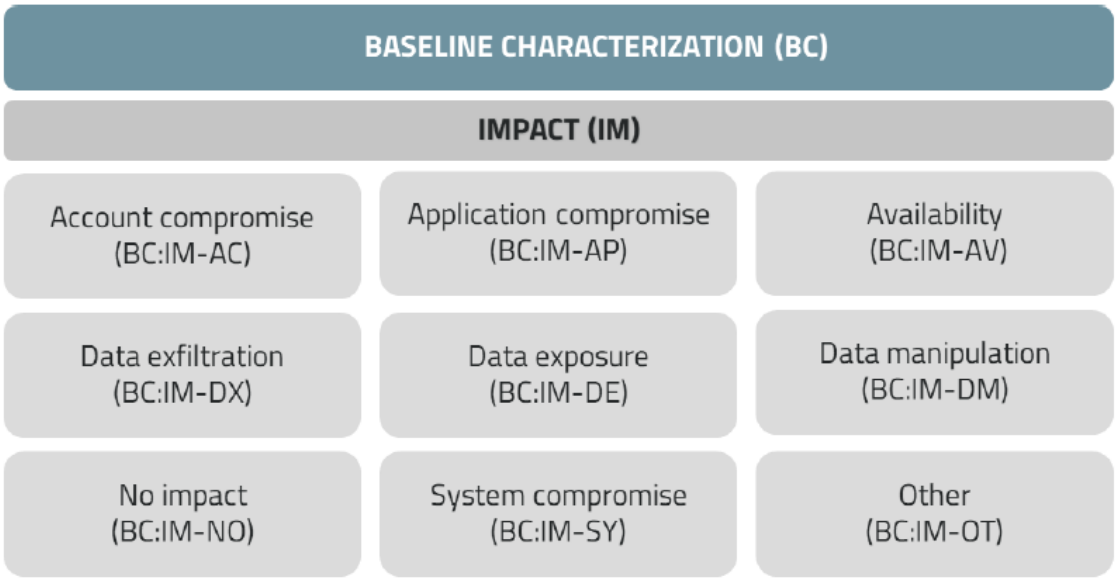
Codice	Descrizione
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o 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) stabiliti ai sensi della misura DE.CM-01.

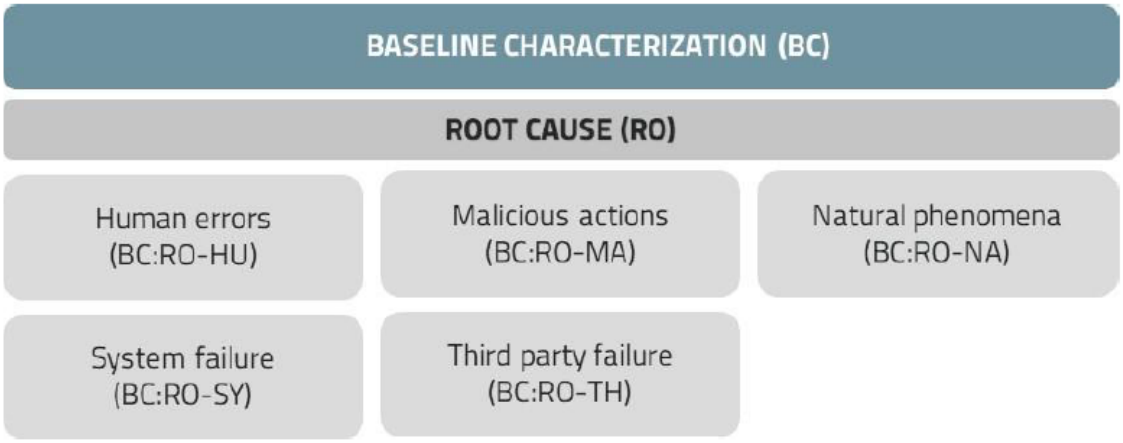
Tassonomia Cyber ACN

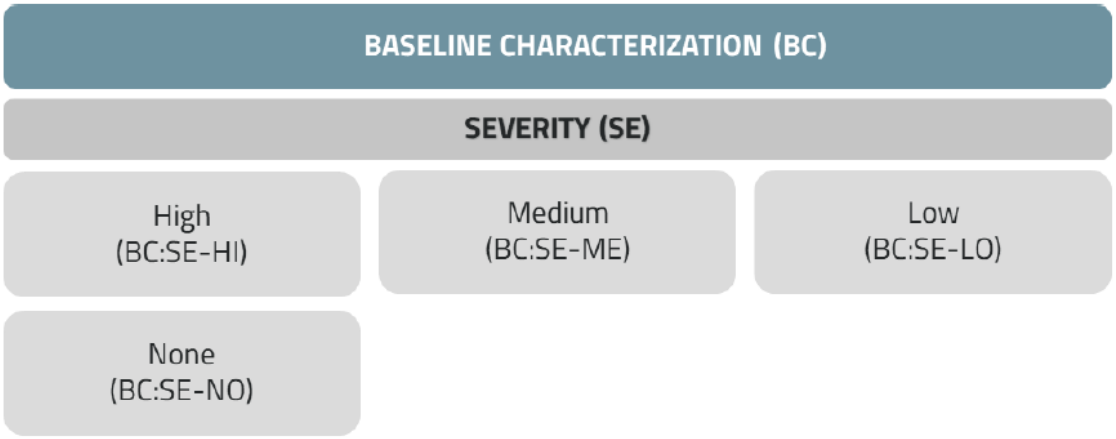
Si raccomanda di utilizzare la Tassonomia cyber di ACN (TC-ACN)[1] almeno per quanto riguarda le macrocategorie BASELINE CHARACTERIZATION e il THREAT TYPE e i relativi predicati – se ne riportano qui solo alcuni estratti:



[1] https://www.acn.gov.it/portale/documents/20119/552690/ACN_Tassonomia_Cyber_CLEAR.pdf/9595cc35-1c0b-4007-07b2-8f0468e5b82e?t=1731598519616







Registro degli incidenti

Template del documento descrittivo dell'incidente:

ID	MIB-20250912-01 (SEDE-YYYYMMDD-NN)
Data rilevamento	
Modalità rilevamento	

Classificazione da tassonomia ACN Baseline Characterization	Impact (BC:IM)	
	Root Cause (BC:RO)	
	Severity (BC:SE)	
Incidente significativo		
Tipologia dati coinvolti		
Impatto su RID		
Data presunta evento		
Asset coinvolti		
Descrizione		
Cause		
Stato iniziale		
Misure di contenimento e mitigazione		
Misure di eradicazione e ripristino		
Stato finale		
Data chiusura incidente		
Post mortem		
Soggetti coinvolti nella gestione		
Comunicazioni		
Documentazione		

Nome file: <***ID***>**.[pdf|docx|xlsx|csv]**, da salvare nel registro incidenti locale. La versione in formato CSV è obbligatoria.

Registro incidenti locale: sistema documentale Alfresco dell'INFN, sito CCR, cartella:

Sicurezza Informatica e GDPR->Documenti strutture->*struttura*->Incidenti->Registro Incidenti

Documentazione incidente (descrizione, evidenze forensi, verbale post mortem e da qualunque altro documento pertinente): sistema documentale Alfresco dell'INFN, sito CCR, cartella:

Sicurezza Informatica e GDPR->Documenti strutture->*struttura*->Incidenti->*identificativo incidente*.

Protezione di registro locale e documentazione incidenti:

- read/write: Incident Handler, Team responsabile delle risorse di calcolo
- read: Direttore di riferimento, CSIRT INFN, RTD

Registro centrale degli incidenti (aggregato di tutti i registri locali): sistema documentale Alfresco dell'INFN, sito CCR, cartella:

Sicurezza Informatica e GDPR->CSIRT->Incidenti->Registro Incidenti.

Protezione del registro centrale degli incidenti:

- read/write: CSIRT INFN
- read: RTD

Ulteriori accessi ai registri locale e centrale possono essere consentiti a discrezione della CCR e dell'RTD, in accordo con lo CSIRT INFN.

Canali di comunicazione interni/esterni

Destinatiario	**Canali di comunicazione**
CSIRT INFN	mail: csirt@infn.it (comunicazioni interne, segnalazione incidenti) portale web: https://csirt.infn.it/si.html (segnalazione incidenti) pec: csirt@pec.infn.it (comunicazioni esterne)
CSIRT manager	mail: csirt@infn.it (comunicazioni interne, segnalazione incidenti) pec: csirt@pec.infn.it (comunicazioni esterne) cell: +39 340 968 0316
Referente Security locale (*incident handler*)	mail: indirizzo di posta elettronica INFN individuale telefono: recapito telefonico individuale
APM	mail: apm@<*struttura*>.infn.it
Team responsabile delle risorse informatiche coinvolte	mail: calcolo@<*struttura*>.infn.it telefono: recapito telefonico del servizio
NUCS INFN	mail: nucs@infn.it
Punto di Contatto ACN	mail: enrico.pasqualucci@infn.it pec: enrico.pasqualucci@pec.infn.it cell: +39 320 923 2335
Sostituto del Punto di Contatto ACN	mail: luca.carbone@mib.infn.it pec: luca.carbone@pec.infn.it cell: +39 340 968 0316
Referente CSIRT e suoi sostituti	mail: luca.carbone@mib.infn.it pec: luca.carbone@pec.infn.it cell: +39 340 968 0316
Ufficio Legale	mail: legale@lnf.infn.it

Destinatiario	**Canali di comunicazione**
DPO	mail: dpo@infn.it
Ufficio comunicazione	mail: uffcom@lists.infn.it
Dirigenza Ente (Management)	Presidente - mail: presidenza@infn.it Consiglio Direttivo - mail: cd@lists.infn.it
Direttore di riferimento (Management)	mail: indirizzo individuale INFN
Unità di crisi	Tramite il direttore di riferimento
CCR	Presidente – mail: alessandro.brunengo@infn.it
RTD	mail: enrico.pasqualucci@infn.it pec: enrico.pasqualucci@pec.infn.it