Linee Guida per la redazione della documentazione contrattuale afferente le forniture di sistemi IT[1] e OT[2] destinati a bordo delle UU.NN. che prevedono requisiti di sicurezza cibernetica

Edizione gennaio 2019

[1] *Information Technology*.
[2] *Operations Technology*.

Ministero della Difesa

Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti
Direzione degli Armamenti Navali

NAV-50-4217-0010-13-00B000

ATTO DI APPROVAZIONE

Approvo la seguente Pubblicazione:

- LINEE GUIDA PER LA REDAZIONE DELLA DOCUMENTAZIONE CONTRATTUALE AFFERENTE LE FORNITURE DI SISTEMI IT E OT DESTINATI A BORDO DELLE UU.NN. CHE PREVEDONO REQUISITI DI SICUREZZA CIBERNETICA

Roma, lì 17 GEN. 2019

IL DIRETTORE
Amm. Isp. Capo Matteo BISCEGLIA

Sommario

1 Definizioni e note di linguaggio 5

2 Normativa di riferimento 7

2.1 Direttive nazionali 7

2.2 Direttive Difesa 8

2.3 Normativa NATO 8

2.4 Normativa Internazionale 9

3 Finalità del documento 10

4 Applicabilità 11

5 Processo di acquisizione e valutazione della Sicurezza Cibernetica per sistemi "*Secure by Design*" 12

6 Iter di omologazione per i sistemi ICT militari che gestiscono informazioni classificate 18

7 Norme per la definizione dei requisiti di un sistema CIS di tipo industriale (OT e IOT) 19

8 Requisiti Funzionali per la Sicurezza Cibernetica. 19

9 Ridondanza e continuità operativa *(ICT readiness for business continuity)* 20

10 Valutazione del rischio cibernetico 20

10.1 Applicazione della ISO 27005 20

10.2 La redazione della Relazione Tecnica di Valutazione del Rischio (RTVR) o *Technical Risk Assessment Report.* 22

Annesso 1 – Selezione dei requisiti di Sicurezza Cibernetica per la scrittura della Specifica Tecnica 23

1 Introduzione 23

2 Requisiti funzionali per la sicurezza cibernetica 23

2.1 Politiche di sicurezza 23

2.2 Organizzazione della sicurezza delle informazioni 23

2.2.1 Ruoli e responsabilità per la sicurezza delle informazioni 23

2.2.2 Separazione dei compiti 24

2.2.3 Contatti con i CERT di FA, della DIFESA o di organizzazione Internazionali 24

2.3 Gestione dei componenti/*asset* dei sistemi (ISO27002 cap.8) 24

2.3.1 Classificazione degli asset e delle informazioni 24

2.4 Requisiti per il controllo degli accessi ai sistemi 25

2.4.1 Politiche di controllo degli accessi 25

2.4.2 Sistemi di Gestione degli accessi 26

2.4.3 Gestione degli accessi di tipo privilegiato 26

2.4.4 Responsabilità degli utenti e gestione dell'accounting 27

2.4.5 Procedure di log-on sicure 27

2.4.6 Sistemi di gestione delle password 28

2.4.7 Autenticazione per l'uso di moduli software di utilità con alti privilegi 29

2.4.8 Controllo degli accessi al codice sorgente dei programmi 30

2.5 Crittografie e chiavi crittografiche. 31
2.5.1 Politiche sull'uso dei controlli crittografici 31
2.5.2 Gestione delle chiavi 31
2.6 Sicurezza Fisica ed Ambientale 32
2.6.1 Perimetro di sicurezza e protezione degli asset critici. 32
2.6.2 Fattori ambientali 32
2.6.3 Fattori ambientali e ridondanza fisica dei componenti 33
2.6.4 Sicurezza dei sistemi all'esterno delle aree sicure o accessibili da personale esterno. 33
2.6.5 Manutenzioni presso strutture esterne all'organizzazione 34
2.7 Operatività dei sistemi 34
2.7.1 Meccanismi di controllo e gestione dei sistemi complessi 34
2.7.2 Gestione dei cambiamenti 34
2.7.3 Controllo e gestione della capacità di un sistema 35
2.7.4 Configurazione del software e protezioni *anti-malware (end point protection)* 35
2.7.5 Backup dei sistemi 35
2.8 Raccolta dei log e monitoraggio dei sistemi 36
2.8.1 Registrazione log di allarmi ed eventi 36
2.8.2 Protezione delle registrazioni e dei file di log 37
2.8.3 Attività di amministratori e manutentori dei sistemi IT/OT 38
2.8.4 Sincronizzazione degli orologi 38
2.9 Ciclo di vita del software - aggiornamenti ed installazione nuovo software 39
2.10 Ciclo di vita del software - Gestione delle vulnerabilità tecniche 39
2.11 Limitazioni all'installazione del software 40
2.12 Sicurezza delle comunicazioni – Reti 40
2.12.1 Controlli di rete 40
2.12.2 Segregazione delle reti 41
2.12.3 Segregazione delle reti - reti wireless 42
2.12.4 Protezione delle transazioni dei servizi applicativi 42
Annesso 2 – *Common Criteria Evaluation Assurance Level* 43
1 Introduzione 43
2 *Evaluation Assurance Level* (EALs) 43
2.1 EAL 1 *(Functionally Tested)* 43
2.2 EAL 2 *(Structurally Tested)* 43
2.3 EAL 3 (*Methodically Tested & Checked*) 43
2.4 EAL 4 (*Methodically Designed, Tested & Reviewed*) 43
2.5 EAL 5 (*Semi-formally Designed & Tested*) 44
2.6 EAL 6 *(Semi-formally Verified Designed & Tested)* 44

2.7 EAL 7 (*Formally Verified Designed & Tested*) 44
3 *Composed Assurance Packages* (CAPs) 44
3.1 CAP- A *(Structurally composed)* 44
3.2 CAP- B *(Methodically composed)* 44
3.3 CAP- C *(Methodically composed, tested and reviewed)* 44
Annesso 3 – *Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks* 45

1 Definizioni e note di linguaggio

Per una comprensione esaustiva del presente documento e allo scopo di chiarirne l'ambito di applicabilità, è necessario allineare il linguaggio utilizzato nell'ambito del *procurement* navale al contesto della Difesa cibernetica, focalizzando l'attenzione sui seguenti concetti e definizioni[3]:

- **sistema complesso:** si intende una unità fisica o funzionale, costituita da più parti o sottosistemi, interagenti (od in relazione funzionale) tra loro che formano un tutt'uno ed in cui ogni parte da il proprio contributo per una finalità comune. In tale accezione si può considerare come "sistema complesso" l'intera Unità navale militare in relazione ad una specifica missione o, nell'uso comune, un sottosistema, ossia un elemento fisico e/o funzionale costituito da componenti che interagiscono tra loro per una finalità comune[4].

- **sistema CIS**[5]: si intende l'insieme di sottosistemi/componenti *hardware*, *software* e dei loro collegamenti fisici e logici interni ed esterni, che operano direttamente o indirettamente nello spazio cibernetico[6]. Il sistema CIS può essere anche caratterizzato mediante la sua infostruttura[7] e la sua infrastruttura[8];

- **sistema IT**[9]: sistema CIS principalmente destinato all'elaborazione, trattamento e presentazione delle informazioni;

- **sistema OT**[10]: sistema CIS principalmente destinato al controllo e all'automazione di macchinari, impianti o sistemi complessi;

sistema ICT[11]: sistema IT: sistema CIS principalmente destinato all'elaborazione, trattamento e presentazione delle informazioni; in generale, può essere inteso come l'insieme dei sistemi che rappresentano il mondo IT e OT;

- **spazio cibernetico**: dominio creato dall'uomo in cui operano comunicazioni e sistemi informatizzati interconnessi;

- **difesa cibernetica (*cyber defence*):** Il complesso di predisposizioni, misure, procedure e attività volte a proteggere i sistemi informativi e le infostrutture CIS, nello specifico, del Comparto Difesa dalle azioni cibernetiche ostili nella massima accezione possibile;

- **sicurezza cibernetica**: condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebito di dati, nella

---

[3] Alcune definizioni sono mutuate dalla normativa di riferimento, in particolare dalla pubblicazione di SMD denominata *Joint Integrating Concept* (JIC) 012 edizione 2014 inerente "Le attività militari nello spazio cibernetico (La *Cyber-Warfare*)" che definisce il quadro concettuale ed organizzativo di riferimento della Difesa nel settore cyber.

[4] In tale accezione, il *Combat Management System* e lo *Ship Management System* (SMS) delle UU.NN. della Marina Militare sono sistemi complessi rispettivamente in relazione alle funzioni combattimento e condotta della piattaforma.

[5] *Communication Information System*.

[6] Vedasi definizione all'alinea 4.

[7] Ossia l'insieme delle regole con il quale il sistema gestisce le informazioni, opera sui dati ed interagisce a livello logico con gli altri sistemi.

[8] Ossia l'insieme dell'hardware che consente il funzionamento del sistema e consente di interagire a livello fisico con gli altri sistemi.

[9] *Information Technology*.

[10] *Operational Technology*.

[11] Information and Communication Technology.

loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

- **vulnerabilità cibernetica:** debolezza nella configurazione della porzione del proprio spazio cibernetico o più in generale nel sistema delle proprie infostrutture che potrebbe essere sfruttata da un potenziale avversario in possesso delle capacità sufficienti ad infliggere danni cibernetici tramite la pianificazione e la condotta di azioni cibernetiche offensive e/o informative;

virus: Un software appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da fare copie di sé stesso, generalmente senza farsi rilevare dall'utente e può arrecare danni al sistema informatico rallentandolo o rendendolo inutilizzabile;

***malware*:** Abbreviazione di un generico MALicious softWARE, una tipologia di software creati per finalità malevole, quali l'accesso illecito al sistema informatico, il furto di informazioni o la sottrazione (da cui derivano anche esempi più specifici come i *ransomware* che effettuano la criptazione di dati tipicamente a fini di estorsione) della loro disponibilità al possessore, l'esecuzione di processi estranei al sistema informatico o l'alterazione di quelli che il sistema esegue (es: sabotaggio dei sistemi di controllo industriali);

***zero day*:** Vulnerabilità di sicurezza non pubblicamente note;

***exploit*:** Vulnerabilità di sicurezza insite nel codice di un sistema operativo o di un *software* applicativo;

- ***penetration testing (PT)***: processo operativo di valutazione della sicurezza di un sistema o di una rete;
- **effetto cibernetico**: mutamento permanente o temporaneo della funzionalità di un sistema informatico, telematico e/o informativo;
- **danno cibernetico:** cancellazione, manipolazione e/o sottrazione non autorizzata di dati contenuti in una infostruttura o comunque in una porzione di proprietà all'interno del dominio cibernetico.

2 Normativa di riferimento

Di seguito sono riportate i principali riferimenti normativi applicabili che afferiscono il settore della protezione dei dati e della difesa cibernetica:

2.1 Direttive nazionali

Rif.[]	Sigla	Titolo	Ente	Ediz.	Contenuto
Rif.[N1]	PCM-ANS TI-001	Procedura nazionale per l'omologazione di sistemi/reti EAD militari	PCM-ANS	1995	
	PCM ANS TI-002	Standard di Sicurezza per Sistemi/reti EAD militari	PCM-ANS		Standard minimi di sicurezza per garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite dai sistemi EAD.
Rif.[N2]	DPCM 1°agosto 2015	Direttiva "Misure minime di sicurezza ICT per le PP.AA."	AgID	2016	Documento che contiene le Misure minime di sicurezza ICT per le PA in attuazione della Direttiva DPCM del 1° agosto 2015al fine di fornire un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura che risponde alle esigenze operative ed individuando anche gli interventi idonei per il suo adeguamento
Rif.[N3]	DPCM, 17 febbraio 2017	DPCM del 17 febbraio 2017, recante i "nuovi indirizzi per la protezione cibernetica e la sicurezza informatica nazionali"	PCM	2017	
Rif.[N4]		Quadro strategico nazionale per la sicurezza dello spazio cibernetico del 2013	PCM	2013	
Rif.[N5]		Piano nazionale per la protezione cibernetica e la sicurezza informatica del 2017 della PCM	PCM	2017	
Rif.[N6]		PCM ANS/1 (R)	PCM	2006	
Rif.[N7]		PCM ANS/2 (R)	PCM	2006	
Rif.[N8]	Agid 2/2017	CIRCOLARE 18 aprile 2017, n. 2/2017 Misure minime di sicurezza ICT per le pubbliche amministrazioni.	Agid	2017	Misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono oggetti i sistemi informativi della p.a..

2.2 Direttive Difesa

Rif.[]	Sigla	Titolo	Ente	Ediz.	Contenuto
Rif.[D1]	SMD-G-032	Direttiva Interforze di *Policy* sull'Ambiente Cibernetico" (SMD-G-032) ed.2012	SMD	2012	
Rif.[D2]	SMD-I-003	Disciplinare interno all'A.D. su l'utilizzo dei servizi informatici NC erogati in ambito difesa, quali i servizi di posta elettronica, *instant messaging* ed accesso ad internet	SMD VI Reparto	2017	La Direttiva vale sia come disciplinare sull'impiego dei servizi informatici (posta elettronica, Internet, etc) sia come informativa sulle finalità e modalità del trattamento delle informazioni personali nelle attività di controllo tecnico svolte dall'A.D., ai sensi dell'art. 13 della Legge 196/2003.
Rif.[D3]	SMD-I-019	Politica di Sicurezza per i Sistemi di Telecomunicazione e Informatici non classificati della Difesa (Politica di Sicurezza per l'*Information & Communication Technology*)	SMD VI Reparto	2009	indica le misure che "l'Ente fornitore dei servizi connessi ad Internet" deve adottare al fine di ridurre i rischi correlati ad azioni, ovvero ad usi impropri
Rif.[D4]	SMD-I-024	Procedure sulla gestione in sicurezza dei servizi informatici non-classificati dell'AD	SMD VI Reparto	2017	Direttiva che delinea i criteri organizzativi, procedurali e tecnici fondamentali da porre in essere, al fine di conseguire un livello di sicurezza adeguato all'attuale minaccia cibernetica dell'A.D..
Rif.[D5]	SMD-I-013	Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa	SMD VI Reparto	2008	

2.3 Normativa NATO

Rif.[]	Sigla	Titolo	Ente	Ediz.	Contenuto
Rif.[NATO1]		NATO Cyber Defence Policy del 7 giugno 2011	NATO	2011	
Rif.[NATO2]		Minimum requirements of CIS security (including Cyber Defence) for national CIS critical for NATO Core Tasks	NATO	2014	
Rif.[NATO3]		CIS security technical and implementation guidance on protecting authentication credentials (NATO Restricted)	NATO	2015	

Rif.[]	Sigla	Titolo	Ente	Ediz.	Contenuto
Rif.[NATO4]		NATO Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks	NATO	2017	

2.4 Normativa Internazionale

Rif.[]	Sigla	Titolo	Ente	Ediz.	Contenuto
Rif.[I1]		NIST 800-30 Rev.1	*National Institute of Standards and Technology - U.S. Department of Commerce*	2012	INFORMATION SECURITY - Guide for Conducting Risk Assessments
Rif.[I2]		IEC 62443-3-3	*International Electrotechnical Commission*	2014	Dettaglia I requisiti tecnici per i sistemi di controllo (*System Requirements*, SRs) associate con i requisiti fondamentali (*Foundational Requirements*, FRs) derivanti dalla Norma IEC 62443-1-1, includendo anche i requisiti dei i livelli di sicurezza per un sistema di controllo (*Security Levels*, SL-C, *control system*).
Rif.[I3]		IEC/EN 61508	*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*	2010	
Rif.[I4]		ISO 27001	*Information technology — Security techniques — Information security management systems — Requirements*	2005	
Rif.[I5]		ISO 27002	*Information technology – Security techniques – Code of practice for information security controls*	2013	
Rif.[I6]		ISO 27005	*Information technology — Security techniques — Information security risk management*	2018	
Rif.[I7]		ISO 27031	*Information technology -- Security techniques -- Guidelines for cybersecurity*	2012	
Rif.[I8]		Mil-Std-498	*Software Development and Documentation*	1994	

3 Finalità del documento

In considerazione del complesso quadro normativo di riferimento nel settore della sicurezza delle informazioni nel campo ICT[12] e, più in particolare, nell'ambito della sicurezza cibernetica, si è avvertita l'esigenza di redigere delle Linee Guida per indirizzare le attività ed i processi di *procurement* della Direzione per gli Armamenti Navali (NAVARM) in accordo a detta normativa ed in linea con i requisiti dettati dal Committente.

In particolare, la norma è finalizzata principalmente alle forniture di sistemi Non Classificati, dal momento che per i sistemi Classificati le procedure e le attività connesse sono specificatamente normate e richiedono l'implementazione di processi di omologazione dei sistemi e la definizione di specifici requisiti di sicurezza dettagliati nella normativa di riferimento Nazionale (serie Rif.[Nx]).

La NAV, in altri termini, ha come obiettivi principali quelli di supportare le Divisioni Tecniche nella:

identificazione e selezione dei requisiti di qualità e sicurezza funzionali dei sistemi ICT;

introduzione di clausole di sicurezza specifiche nei contratti e dalle quali partire per la progettazione di sistemi informatici che possano essere impiegati in modo sicuro;

previsione di specifici processi di valutazione e controllo dell'implementazione della sicurezza cibernetica all'interno delle attività di *procurement* di sistemi ICT.

La norma NON affronta questioni inerenti la definizione di *policy* di Sicurezza in quanto esplicitamente compito di altri Organismi o Enti di Forza Armate e della Difesa. La norma fornirà le indicazioni per la definizione di prassi consolidate laddove per la gestione dei sistemi IT/OT non vi siano espresse indicazioni su specifiche normative applicabili o particolari *policy* di sicurezza da implementare.

Il rischio di incidenti informatici, siano essi accidentali od intenzionali, può essere minimizzato attraverso l'applicazione di processi di gestione e controllo dei sistemi derivanti da "buone prassi" tecniche (*best practices*) e corrette procedure di gestione.

In particolare, i requisiti di sicurezza derivano da quelli riportati nella SMD-I-019 e, laddove non specificati nelle Direttive Difesa, sono stati derivati dalla ISO 27001 per l'implementazione di un "sistema di gestione della sicurezza delle informazioni" e dalla ISO 27002 per quanto concerne le modalità di controllo. Le citate normative costituiscono una base di processi, largamente riconosciuta, volta ad assicurare una corretta condotta dei sistemi informatici e una corretta gestione delle informazioni in essi contenute. I sistemi realizzati secondo tali linee guida dovranno essere **abilitanti** per le suddette funzioni, ovvero permetteranno l'implementazione di un sistema di gestione della sicurezza delle informazioni. Questo insieme di funzionalità è deducibile:

- ⇨ dagli **Obbiettivi di Controllo** definiti in **Annesso A** alla ISO 27001 e
- ⇨ implementabile mediante le indicazioni pratiche di **modalità di controllo** definite dalla ISO 27002;

le modalità di implementazione potranno essere, quindi, prese a riferimento per la scrittura di Capitolati Tecnici, indicando dove necessario anche **differenti o ulteriori** controlli di processo da implementare in soddisfacimento di specifici requisiti operativi, o per l'implementazione delle specifiche *policy* di sicurezza definite dagli Enti preposti.

[12] *Information and Communication Technology*.

Se è vero che "la sicurezza che può essere ottenuta attraverso mezzi tecnici è limitata e dovrebbe essere supportata da una gestione e da procedure appropriate"[13], è anche vero che una non corretta progettazione dei sistemi informatici può rendere molto difficile, se non addirittura inefficace, l'attuazione di procedure di controllo per la sicurezza cibernetica. Per questo, è necessario esplicitare nei requisiti tecnici dei sistemi in acquisizione le modalità di gestione della sicurezza che si vorranno implementare. In tal modo sarà possibile guidare i progettisti nel processo di sviluppo (*Secure by Design*) fino a verificare quanto eseguito in fase di qualifica o quanto collaudato mediante specifiche metodologie di analisi (implementazione del concetto di *Secure by Design*).

Da quanto sopra esposto ne deriva che per la gestione di sistemi complessi sarà sempre indispensabile valutare i rischi connessi alla sicurezza cibernetica in fase di progettazione. Per questo sarà necessario eseguire delle valutazioni prima tecniche e poi procedurali per consentire agli utilizzatori finali dei sistemi di decidere se applicare azioni mitigatrici aggiuntive o accettare il rischio residuo. A similitudine di quanto avviene per la sicurezza sui luoghi di lavoro, si prevedere di ricevere assieme alla consegna del sistema, o in una fase subito successiva, una Relazione Tecnica di Valutazione del Rischio Cyber, come base di partenza per la pianificazione dei processi e delle procedure d'impiego dei sistemi acquisiti, coerentemente al contesto operativo applicabile.

La parte dedicata al *Risk Management* si focalizza proprio sulle modalità di stesura di tale Relazione Tecnica, basandosi sulla norma ISO 27005 come base di partenza per lo sviluppo dei documenti di valutazione del rischio. In tale fase viene lasciata comunque la libertà di procedere operativamente anche secondo altri standard o procedure, applicando norme come, ad esempio, la NIST 800-30r1 (**Rif.[I1]**) o la metodologia FAIR[14].

Si sottolinea, infine, come le presenti Linee Guida siano state concepite come un "*living document*" nel quale introdurre prontamente gli elementi di sviluppo nel settore ICT e le modifiche discendenti dal quadro normativo di riferimento in continuo aggiornamento.

4 Applicabilità

Le presenti Linee Guida discendono dalle normative in vigore nel settore della sicurezza delle informazioni e possono essere applicate, in tutto o in parte, alle forniture di sistemi informatici non classificati nel campo IT e OT qualora richiamate espressamente nelle specifiche tecniche dei contratti o dei bandi di gara.

In altri termini, i requisiti funzionali riportati nelle Linee Guida possono essere utilizzati qualora il Requisito Tecnico-Operativo dell'oggetto di fornitura richiedesse l'implementazione di requisiti minimi di sicurezza cibernetica senza richiamare una specifica normativa di settore o prevedere specifici requisiti di sicurezza. Ad esempio, la fornitura di sistemi classificati spesso richiede l'implementazione di opportuni requisiti per raggiungere uno specifico livello di sicurezza (EAL - *Evaluation Assurance Level*) basato sui *Common Criteria*[15], come verrà accennato successivamente.

Vista la rapida evoluzione tecnologica nel settore ICT, non è consigliabile identificare e selezionare in modo specifico strumenti e soluzioni tecnologiche a difesa delle infrastrutture, in quanto **le azioni di**

[13] cit. Introduzione ISO 27002.

[14] *Factor Analysis of Information Risk*; è una tassonomia di fattori che contribuisce alla valutazione del rischio e a cercare di mettere in evidenza come tali fattori si influenzano l'uno con l'altro; FAIR cerca di fornire i fondamenti e un framework per eseguire la *risk analysis*; essa viene spesso impiegata per comprovare, più che sostituire, le attuali metodologie di *risk analysis*. Maggiori informazioni sono disponibili al seguente url: https://www.fairinstitute.org .

[15] I *Common Criteria for Information Technology Security Evaluation* è uno standard internazionale (ISO/IEC 15408) per la certificazione di sicurezza di PC.

controllo e mitigazione del rischio cibernetico potrebbero subire cambiamenti troppo rapidi per essere recepiti in un processo di acquisizione di uno o più sistemi complessi. Per tale ragione, i requisiti definiti in queste linee guida sono da intendersi come **requisiti prettamente funzionali**. In fase successiva, dopo aver individuato tali requisiti funzionali, le diverse tecnologie saranno selezionate in ragione delle funzionalità che queste "abiliteranno" all'interno del Sistema Complesso di riferimento, lasciando ai progettisti la possibilità di selezionare la migliore tecnologia o prassi operativa disponibile al momento, aggiornata al più recente stato dell'arte.

Allo scopo di utilizzare modelli e definizioni accessibili a tutti gli operatori economici sul mercato Europeo ed Extra-Europeo, la presente NAV si basa su standard internazionali di larga diffusione come le norme della serie ISO 27000, con particolare riferimento alla ISO 27001 e 27002. Queste due norme definiscono dei requisiti minimi e delle prassi comuni per l'implementazione di un Sistema di Gestione della Sicurezza, ovvero l'implementazione di processi di controllo e gestione delle informazioni che risultano applicabili **in generale e trasversalmente a tutti i sistemi CIS** per garantirne adeguati livelli di sicurezza cibernetica.

Per quanto concerne l'ambito OT, saranno specificate funzionalità e requisiti tecnico-funzionali in modo da declinare in maniera più peculiare i requisiti generali di sicurezza e le modalità di gestione del rischio cibernetico per sistemi industriali e, più in particolare, per l'automazione navale.

Allo scopo di porre in evidenza la maggiore distinzione tra il mondo It e quello OT, si può affermare che la più grande distinzione tra i due consiste nella loro *mission*: mentre i sistemi IT trattano i dati e in caso di attacco cyber tendono ad disconnettersi per proteggere le informazioni stesse (ad esempio, la protezione di dati su uno specifico canale di telecomunicazioni), i sistemi OT sono progettati per funzionare sempre e in caso di attacco, essi devono consentire una *graceful degradation* delle prestazioni per garantire fino alla fine il servizio che erano preposti ad erogare (ad esempio, l'erogazione dell'energia elettrica ad una Unità navale).

I requisiti tecnico-funzionali minimi indicati nella presente norma sono coerenti con la norma IEC 62443-3-3 (**Rif.[I2]**), con riferimento ai livelli di sicurezza SL3 e SL4.

Nello specifico, i sistemi ICT dovranno seguire le indicazioni riportate:

- ⇨ nella normativa di cui alla serie Rif.[Nx] per i sistemi IT classificati;
- ⇨ nella normativa serie Rif.[Dx] e in Annesso 1, per sistemi OT in generale;
- ⇨ nella normativa serie Rif.[Dx], nell'Annesso 1 e nell'Annesso 2 per i sistemi OT e relativo software;
- ⇨ nella normativa serie Rif.[Dx], in Annesso 2, per i sistemi IT e relativo software;
- ⇨ nella normativa serie Rif.[Dx] e serie Rif.[NATOx] se i sistemi in fase di acquisizioni dovranno essere interfacciati anche con sistemi NATO;
- ⇨ per quanto concerne lo sviluppo e la documentazione del software, la normativa di cui al Rif.[I8].

5 Processo di acquisizione e valutazione della Sicurezza Cibernetica per sistemi "*Secure by Design*"

In linea generale, le attività contrattuali che prevedono l'acquisizione di un sistema possono variare sensibilmente a seconda di vari fattori: *in primis* le classiche variabili del *Project Management* (obiettivi, tempi e costi), eventuali vincoli costruttivi o la maturità tecnologica del sistema, non ultimo la cornice normativa di riferimento per lo svolgimento delle attività tecnico-amministrative. Ad esempio, l'acquisizione di una nuova Unità navale richiede attività estremamente lunghe e articolate

che prevedono lo svolgimento di più fasi volte ad assicurare il corretto sviluppo del progetto e la sua rispondenza al requisito operativo della F.A.

Per semplicità ed ai soli fini di evidenziare le attività tecnico-contrattuali che richiedono delle valutazioni sotto il profilo della Difesa cibernetica, è stato schematizzato l'intero processo di acquisizione di un sistema complesso[16], in 3 fasi principali[17]:

Fase di analisi dei requisiti del sistema (***System Requirement Review***): è la fase che generalmente intercorre dalla ricezione del Mandato contenente il Requisito Operativo (o il Requisito Tecnico-Operativo) e la definizione della Specifica Tecnica (ST) contrattuale che definisce le caratteristiche del sistema e le modalità di svolgimento delle fasi successive.

Fase di progetto del sistema (***System Design***): è la fase che parte dalla progettazione preliminare del sistema e si completa con la fase di revisione ed accettazione del progetto definitivo.

Normalmente viene suddivisa in due sotto-fasi:

a. ***System Design Review*** **(SDR)**: è la fase che valuta, per ciascun sottosistema, l'ottimizzazione, la tracciabilità, la correlazione, la completezza dei requisiti tecnici allocati ed i rischi associati. Il *deliverable* contrattuale più importante relativo a questa fase è la produzione del documento *System Subsystem Specification* (SSS) per ciascun sistema CIS in fornitura. Tale fase si conclude con la revisione (*review*) formale di tutta la documentazione prodotta e con la sua accettazione.

b. ***Critical Design Review (CDR)****:* è la fase che dimostra se la maturità del progetto è appropriata per supportare i processi di fabbricazione, assemblaggio, integrazione e test nella successiva fase di sviluppo del sistema. Il *deliverable* contrattuale più significativo relativo a tale fase è la produzione del documento *System Subsystem Design Description* (SSDD) per ciascun sistema CIS in fornitura. La fase in parola si conclude con la *review* formale di tutta la documentazione prodotta e con la sua accettazione.

Fase di sviluppo/realizzazione/test del sistema (***System Development***): è la fase che parte dalla progettazione esecutiva e si conclude con la realizzazione e consegna del prototipo del sistema da qualificare (*First of Class*) o del sistema finale da collaudare.

L'acquisizione di un singolo sistema/sottosistema[18] CIS può essere impostata e finalizzata prevedendo una semplificazione/compressione delle fasi e dei processi precedentemente indicati.

Con riferimento alla Figura 1, l'attività di *procurement* di un sistema complesso parte con l'analisi del Requisito Operativo Definitivo (ROD)[19] ricevuto dal Committente mediante una Lettera di Mandato con l'indicazione di un *budget* per realizzare la commessa.

In tale fase, la Divisione Tecnica imposta l'attività tecnico-amministrativa e procede alla redazione di una Specifica Tecnica che consente agli operatori economici interessati di valutare meglio il requisito del cliente e di identificare le principali caratteristiche tecniche del sistema richiesto. Qualora nel documento di mandato fossero espressi specifici requisiti connessi alla sicurezza cibernetica o riferimenti a specifica normativa del settore da applicare, la Divisione Tecnica ha il compito di

[16] Nel caso in cui sia costituito da sottosistemi CIS che necessitano di una valutazione nel dominio della sicurezza cibernetica.

[17] La descrizione è fatta dall'ottica della Direzione Tecnica incaricata dell'attività tecnico-amministrativa e fa riferimento alle fasi previste dalla MIL-STD 498 "*Software Development and Documentation Standard*".

[18] Si pensi, ad esempio, all'ammodernamento dell'infrastruttura della rete informatica di bordo basata su tecnologia COTS.

[19] In molti casi è sufficiente un Requisito Tecnico-Operativo.

riportare/declinare tali requisiti nella ST integrandoli, laddove necessario ed applicabile, con i requisiti tecnico-funzionali definiti con le presenti Linee Guida.

Completata la fase di affidamento della commessa che termina con la stipula del contratto, qualora prevista e con le modalità stabilite nel contratto stesso, inizia la fase di progetto del sistema (*System Design*).

Nella fase di SDR è fondamentale assicurarsi che i requisiti di sicurezza riportati nella ST contrattuale siano mappati e tracciati correttamente nei documenti consegnati[20]. A tale scopo può essere utile richiedere all'industria di "identificare" il sottoinsieme di requisiti funzionali e fisici per ciascun sistema CIS che possono avere un impatto sotto il profilo della sicurezza cibernetica[21]. Tuttavia, questa fase risulta uno stadio a carattere marcatamente preliminare e non ancora idoneo per condurre una valutazione puntuale del rischio cibernetico che, invece, verrà svolta nella fase successiva.

Completata la fase SDR, si procederà con la CDR che prevede la progettazione funzionale del sistema con l'identificazione dei sottosistemi/componenti che lo costituiscono, nonché con la descrizione delle interazioni tra questi ed altri sistemi/componenti. Tale fase è caratterizzata dalla consegna del documento di SSDD. Una volta acquisito tale documento, se il contratto lo prevede, può essere richiesto un *Technical Risk Assessment* (TRA) con la consegna di un *deliverable* contenente gli elementi utili all'A.D. per valutare la bontà della progettazione sotto il profilo della sicurezza cibernetica. Sulla base della minaccia cibernetica, nota o ipotizzata, dal confronto con il documento di SSDD e dalla verifica dei requisiti espressi nei documenti di ST e di SSS, l'A.D. potrà valutare il livello di rischio di sicurezza associato al sistema e le implicazioni di carattere progettuale che possono avere impatti su tempi e costi del progetto.

In questa fase, specie se in presenza di sistemi basati su prodotti COTS[22], il documento potrà contenere una prima Analisi delle Vulnerabilità (*Vulnerability Assessment* – VA) basata sulla conoscenza dei componenti e delle architetture prescelte.

A questo punto, nel caso siano verificate entrambe le seguenti condizioni ovvero se i requisiti di progetto sono soddisfatti ed il livello di rischio è considerato accettabile, si procederà con l'approvazione formale dell'eventuale documento di TRA e con l'accettazione del documento di SSDD nella CDR formale. In caso contrario, occorrerà procedere con l'emissione di una richiesta di modifica (*Engineering Change Request* – ECR) volta ad individuare, tramite la correlata proposta di modifica (*Engineering Change Proposal* – ECP), la soluzione più idonea per consentire di ricondurre il rischio di sicurezza a livelli accettabili o comunque coerenti con i requisiti contrattuali.

Al termine della CDR si apre la fase di sviluppo che prevedrà la progettazione esecutiva[23] del sistema e la realizzazione di un *test bed* (o del prototipo) sul quale condurre i test di qualifica. Se previsto contrattualmente, verranno eseguiti anche dei test per la parte Sicurezza Cibernetica volti a verificare la corretta implementazione dei requisiti di sicurezza da parte degli implementatori/esecutori

[20] Ad esempio, il requisito di ST "il sistema dovrà prevedere un sistema di autenticazione", può declinarsi nel requisito di SSS "il sistema dovrà prevedere un sistema di autenticazione SW basato su *login* e *pwd*" oppure declinarsi nel requisito "il sistema dovrà prevedere un sistema di autenticazione multilivello basato sull'acquisizione di dati biometrici".

[21] Ad esempio, al requisito funzionale di SSS "il sistema dovrà consentire l'aggiornamento del SW mediante connessione remota" può essere inserito un "*tag*" cyber perché il requisito ha o può avere un impatto sotto il profilo sicurezza cibernetica.

[22] *Commercial Off The Shelf*.

[23] Documento interno alla industria.

contrattuali[24]. Queste prove costituiscono un *Security Assessment* (SA) che bisogna prevedere contrattualmente che sia condotto da un Ente o Organizzazione diverso da quello che ha realizzato il sistema. Le verifiche prevedranno un nuovo VA sul sistema reale e, per i sistemi ritenuti più critici, una fase di *Penetration Test* (PT).

Le attività di VA e PT consentiranno di analizzare, secondo modalità concordate, l'effettiva capacità di impiegare le vulnerabilità note del sistema per causare danni, identificando anche eventuali vulnerabilità non note (i c.d. "*0 o Zero Days*") e valutare la resilienza del sistema ad un possibile attacco cibernetico. L'insieme di tali attività di verifica permetteranno di generare un *Test Report* che conterrà:

- ⇨ un aggiornamento della Relazione Tecnica di Valutazione Rischio Cibernetico (il *Techinical Risk Assessment*), completo delle
- ⇨ azioni mitigatrici HW e SW eventualmente implementate per ridurre il rischio a livelli accettabili.

Tenuto conto dell'evoluzione costante della minaccia cibernetica, dal confronto tra il suddetto report e i documenti di progetto, l'A.D. sarà in grado di valutare il livello di rischio di sicurezza residuo intrinseco nel sistema. In base al livello di rischio calcolato, l'A.D. potrà stabilire se minimizzarlo ulteriormente con una modifica progettuale (tramite emissione di ECR), mediante accorgimenti procedurali (che agiscono sulle persone che impiegano il sistema) o fisici (che agiscono su elementi esterni al sistema)[25].

Nel caso in cui il rischio residuo sia ritenuto accettabile, l'A.D. procederà all'accettazione del documento ed alla qualifica del sistema sotto il profilo della Sicurezza Cibernetica.

Allo scopo di conseguire il desiderato livello di sicurezza, alle sopra citate attività ne potranno essere affiancate anche altre di controllo se contrattualmente previste, come l'esecuzione di *Code Analysis* sul *software* sviluppato o di *Cyber Threat Intelligence* (CTI).

Quest'ultima eventuale azione di identificazione ed analisi delle minacce dovrà essere considerata come trasversale a tutto il processo di acquisizione e programmata in ognuna delle sue tre principali fasi (Valutazione requisito & ST, Progettazione e Sviluppo – vds Figg. 1 e 2). In particolare, a seconda della desiderato livello di approfondimento della ricerca di possibili minacce, la CTI si tradurrà in operazioni di *Open Source Intelligence* (OSINT) modulata su diversi livelli di complessità. In maniera similare al presente documento, è auspicabile che l'attività di CTI sia continua ed integrata con l'evoluzione del sistema in fase di progettazione poiché le minacce che insistono su di esso si evolveranno in maniera similare.

Al termine del processo, la Relazione Tecnica di Valutazione del Rischio Cibernetico (RTVR–C) sarà consegnata alla A.D. per essere estesa agli Enti competenti (es. CERT e SOC di Forza Armata) e ai diretti responsabili dell'impiego dei sistemi acquisiti.

[24] Per "implementatori" si intendono tutti coloro i quali hanno partecipato allo sviluppo esecutivo del progetto, sviluppando *software* e/o configurando i componenti *software* e *hardware* COTS impiegati nel sistema CIS.

[25] Ad esempio l'inserimento di un *firewall*.

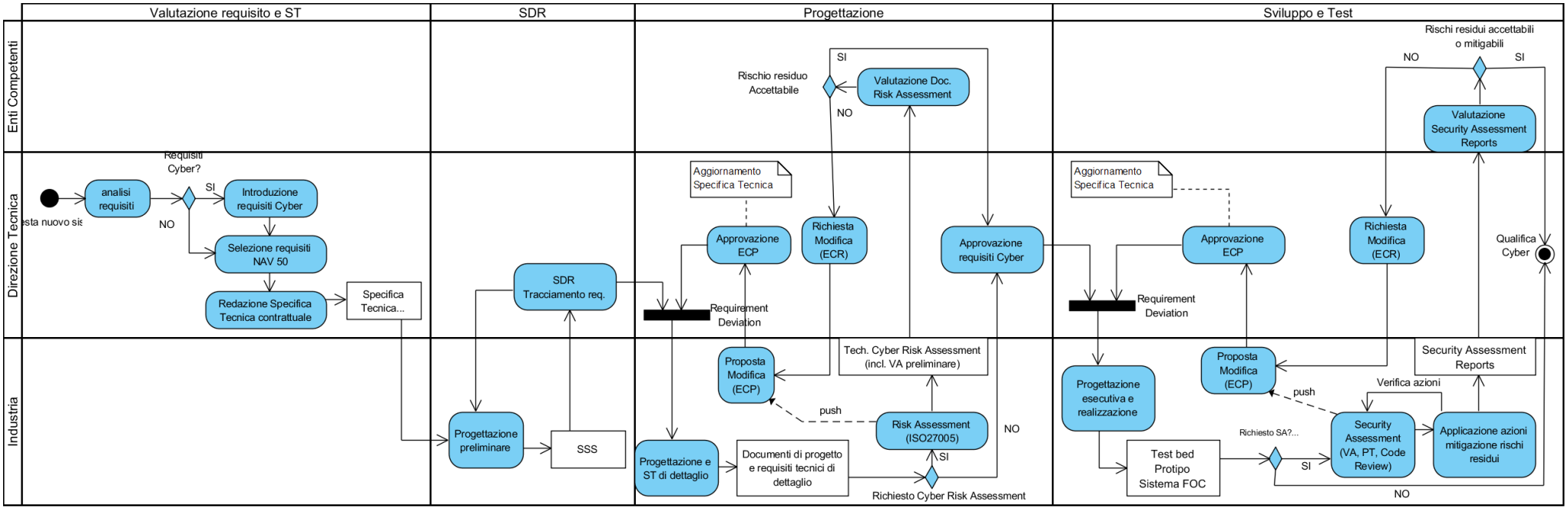

Figura 1 Processo di acquisizione sistema CIS complesso (IT/OT)

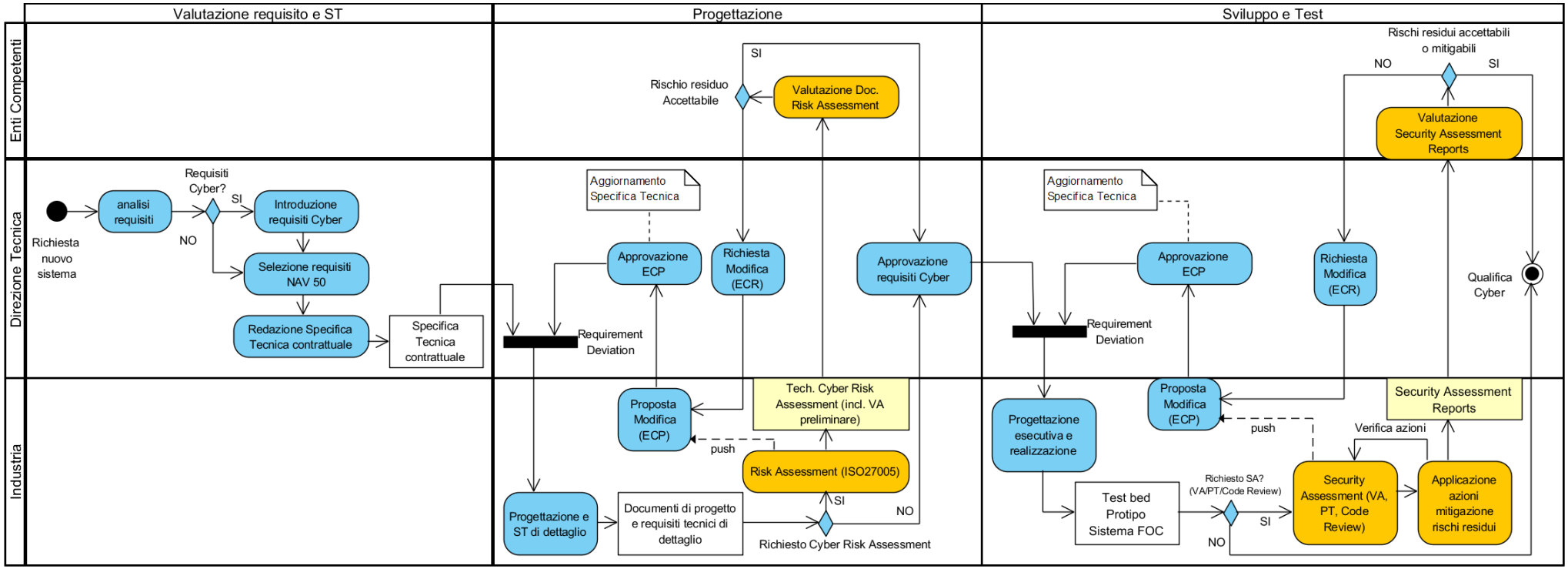

Figura 2 -Processo di acquisizione semplificato

6 Iter di omologazione per i sistemi ICT militari che gestiscono informazioni classificate

Come accennato in precedenza, nel tempo l'Autorità Nazionale di Sicurezza (ANS) ha emanato Direttive precise in merito alla sicurezza informatica ed ha definito uno "schema nazionale" per la certificazione di prodotti classificati nel settore ICT che è obbligatorio seguire.

Nello specifico, la pubblicazione [Rif.N1] PCM ANS TI-001[26] definisce la procedura nazionale per l'omologazione di sistemi e reti EAD militari ai fini della sicurezza nel campo delle tecnologie dell'informazione (INFOSEC) e fornisce le linee guida generali per la elaborazione degli stessi requisiti di sicurezza**. Tale procedura è principalmente orientata verso quei sistemi ICT destinati a gestire dati/informazioni coperti dal segreto di stato o di vietata divulgazione.**

La PCM ANS TI-002 stabilisce gli standard minimi di sicurezza per garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite dai predetti sistemi.

Le citate direttive tecniche fanno riferimento ai criteri di valutazione contenuti nella normativa europea ITSEC[27] o nello standard ISO/IEC 15408 (*Common Criteria for Information Technology Security Evaluation*), quest'ultimo meglio conosciuto semplicemente come *Common Criteria* (CC).

In particolare, allo standard CC è associata una metodologia per la valutazione, *la Common Criteria Evaluation Methodology (CEM)*, anch'essa standardizzata dall'ISO (ISO/IEC 18405:2005).

Per certificare un prodotto, denominato *Target of Evaluation (ToE)*, con il processo descritto nei CC vanno preliminarmente identificati e specificati i seguenti elementi:

- **obiettivi di sicurezza**: rappresentano gli obiettivi che il Committente si pone con l'intenzione di contrastare una minaccia o di rispettare leggi e direttive di sicurezza vigenti. Il raggiungimento degli obiettivi si concretizza attraverso l'adozione di misure di sicurezza tecniche (funzioni di sicurezza) e non tecniche (fisiche o procedurali).
- **ambiente di sicurezza**: tiene conto principalmente dell'uso del sistema da certificare, dell'ambiente in cui viene ad operare, delle minacce da contrastare e delle politiche di sicurezza dell'organizzazione che lo impiega.
- **requisiti di garanzia (*assurance)***: tali requisiti consentono di identificare il livello di sicurezza che si vuole raggiungere e di conseguenza verificarlo attraverso un processo di valutazione del prodotto o del sistema. I CC definiscono una scala di 7 livelli di valutazione (da EAL 1 a EAL 7[28]) identificando, per ogni livello, un set di requisiti di sicurezza funzionali (mandatori o opzionali). In annesso 2 sono meglio specificati gli obiettivi e le componenti di *assurance* per ciascuno dei predetti livelli.

L'adozione della metodologia descritta nei CC assicura un metodo analitico di identificazione degli obiettivi di sicurezza di un sistema, dei relativi requisiti funzionali e di *assurance* utilizzando i cataloghi dei CC[29], e di un processo rigoroso di verifica del soddisfacimento di detti requisiti.

[26] T.I. sta per Tecnologia dell'Informazione.
[27] *Information Technology Security Evaluation Criteria.*
[28] *Evaluation Assurance Level.*
[29] Il catalogo delle componenti funzionali è contenuto nella parte 2 dei CC; quello delle componenti di *assurance* nella parte 3 dei CC.

Per i sistemi che rientrano in tale ambito, dunque, si applica la normativa citata e le disposizioni che l'organizzazione per la sicurezza nazionale nel tempo ha emanato.

I requisiti e i livelli di sicurezza definiti nei CC potranno comunque essere richiamati anche in modo parziale nelle Specifiche Tecniche contrattuali anche per applicazione non classificate laddove questo sia ritenuto utile al raggiungimento di specifiche prestazioni di sicurezza richieste espressamente dal Committente nel requisito tecnico-operativo.

7 Norme per la definizione dei requisiti di un sistema CIS di tipo industriale (OT e IOT[30])

Per la progettazione dei sistemi industriali sono disponibili norme tecniche di riferimento che forniscono indicazioni specifiche per l'implementazione soluzioni tecniche volte a garantire la sicurezza cibernetica dei sistemi di controllo e automazione. Per i sistemi OT potrà essere richiamata la norma IEC 62443 ed in particolare i requisiti tecnici definiti nella IEC 62443-3-3. I requisiti definiti in questa norma internazionale costituiscono un riferimento utile alla definizione di ST contrattuali. I livelli di sicurezza applicabili ai sistemi operativi della FA sono di massima SL3 e SL4. Anche in tale caso, l'applicazione parziale dei requisiti è possibile se adeguatamente giustificata da motivazioni tecniche di applicabilità o di costo/efficacia.

I requisiti descritti nella IEC 62443-3-3 sono direttamente compatibili con quelli definiti nelle presenti linee guida e riportati in dettaglio nel capitolo 8 e in annesso 1.

8 Requisiti Funzionali per la Sicurezza Cibernetica.

Come richiamato nel Cap 14.1.1 della ISO 27002*,*

"I requisiti relativi alla sicurezza delle informazioni dovrebbero essere inclusi all'interno dei requisiti per i nuovi sistemi informativi o per l'aggiornamento di quelli esistenti."

[…]

"I requisiti per la sicurezza delle informazioni dovrebbero anche prendere in considerazione i seguenti punti:

a) il livello di fiducia richiesto in ogni dichiarazione di identità degli utenti, al fine di dedurre i requisiti per la loro autenticazione;

b) il *provisioning* degli accessi e i processi di autorizzazione per utenti di *business* e per utenti privilegiati o tecnici;

c) la comunicazione, a utenti e operatori, dei loro compiti e delle loro responsabilità;

d) le necessità di protezione degli *asset* coinvolti, con particolare riguardo per la disponibilità, per la riservatezza e per l'integrità;

e) i requisiti derivanti da processi di business quali il monitoraggio e la raccolta di *log* delle transazioni nonché i requisiti per il non ripudio;

f) i requisiti richiesti da altri controlli di sicurezza, per esempio interfacce per la raccolta di *log* e il monitoraggio o sistemi di individuazione di fughe di informazioni."

[30] *Internet Of Things*.

Su tali fondamenti sono riportati i requisiti funzionali da integrare nelle ST di acquisizione di sistemi IT/OT riportati in **Annesso 1**. Come già descritto negli obiettivi della normativa (rif. §7), i requisiti funzionali descritti dovranno essere abilitanti per l'implementazione di un corretto sistema di gestione della sicurezza. È bene sottolineare che **non in tutti i casi** sarà necessario garantire l'applicabilità di tutti i requisiti funzionali descritti. La maggiore complessità derivante da tecniche di protezione sofisticate potrebbe non essere proporzionata al rischio mitigato e risultare sovradimensionata dal punto di vista del rapporto costi/benefici. D'altra parte, l'impossibilità di implementare adeguate soluzioni tecniche per la mitigazione dei rischi dovrà essere sempre documentata per permettere all'utente finale di gestire il rischio residuo, ad esempio, mediante apposite prescrizioni procedurali.

I requisiti funzionali potranno essere integrati nelle specifiche tecniche anche in modo parziale ed in combinazione a specifici requisiti di sicurezza richiesti dal committente come i *Common Criteria* o le norme ISO e IEC.

Per i sistemi OT, l'applicazione dei requisiti di sicurezza descritti in **Annesso 1** potranno essere integrati o riferiti esplicitamente ai requisiti definiti nel Rif.[I2] (IEC 62443-3-3).

9 Ridondanza e continuità operativa *(ICT readiness for business continuity)*

Per i sistemi IT/OT *mission critical*, ed in particolare per i sistemi che assolvono funzioni di sicurezza per uomini e mezzi, dovranno essere implementati meccanismi di controllo e ridondanza (evitando quindi, per quanto possibile, casi di *single point of failure*) in grado di garantire la disponibilità dei servizi di rete e dei sistemi ad essa collegati in caso di incidente.

Per alcuni dei componenti critici, al fine di garantire e dimostrare il livello di affidabilità di un dispositivo, potrà essere richiesto la conformità agli standard *Safety Integrity Level* (SIL) secondo la norma IEC/EN 61508, legati a fattori sicurezza funzionale. Conseguentemente, a seconda dello specifico livello di certificazione, la Relazione Tecnica di Valutazione del Rischio Cyber dovrà evidenziare eventuali criticità sui sistemi associati e specificare i requisiti SIL richiesti.

Si evidenzia che, secondo le indicazioni della ISO 27031, l'interruzione delle funzioni di un sistema critico dovrà essere valutata all'interno del Risk Assessment.

Inoltre, nell'ambito della definizione delle procedure/piani di emergenza dovranno essere valutate le interazioni con i CERT di livello superiore, in modo da permettere il coordinamento delle attività di fail-over da parte degli Enti preposti.

A garanzia della corretta progettazione dei sistemi potranno essere richiamati i requisiti della IEC 62443-3-3, ed in particolare quelli della sezione FR7 (Rif.[I2] §11).

10 Valutazione del rischio cibernetico

10.1 Applicazione della ISO 27005

La valutazione del rischio cibernetico costituisce un elemento essenziale per le analisi progettuali e per la valutazione finale di un sistema ICT/CIS. Il riferimento scelto su cui basare tale analisi è la norma ISO 27005.

La valutazione del rischio si inserisce un contesto di analisi continua tipo PDCA (Plan-Do-Check-Act) e riferita a scenari di minaccia applicati al sistema di riferimento. Il processo proposto dalla norma è riassunto nel seguente schema.

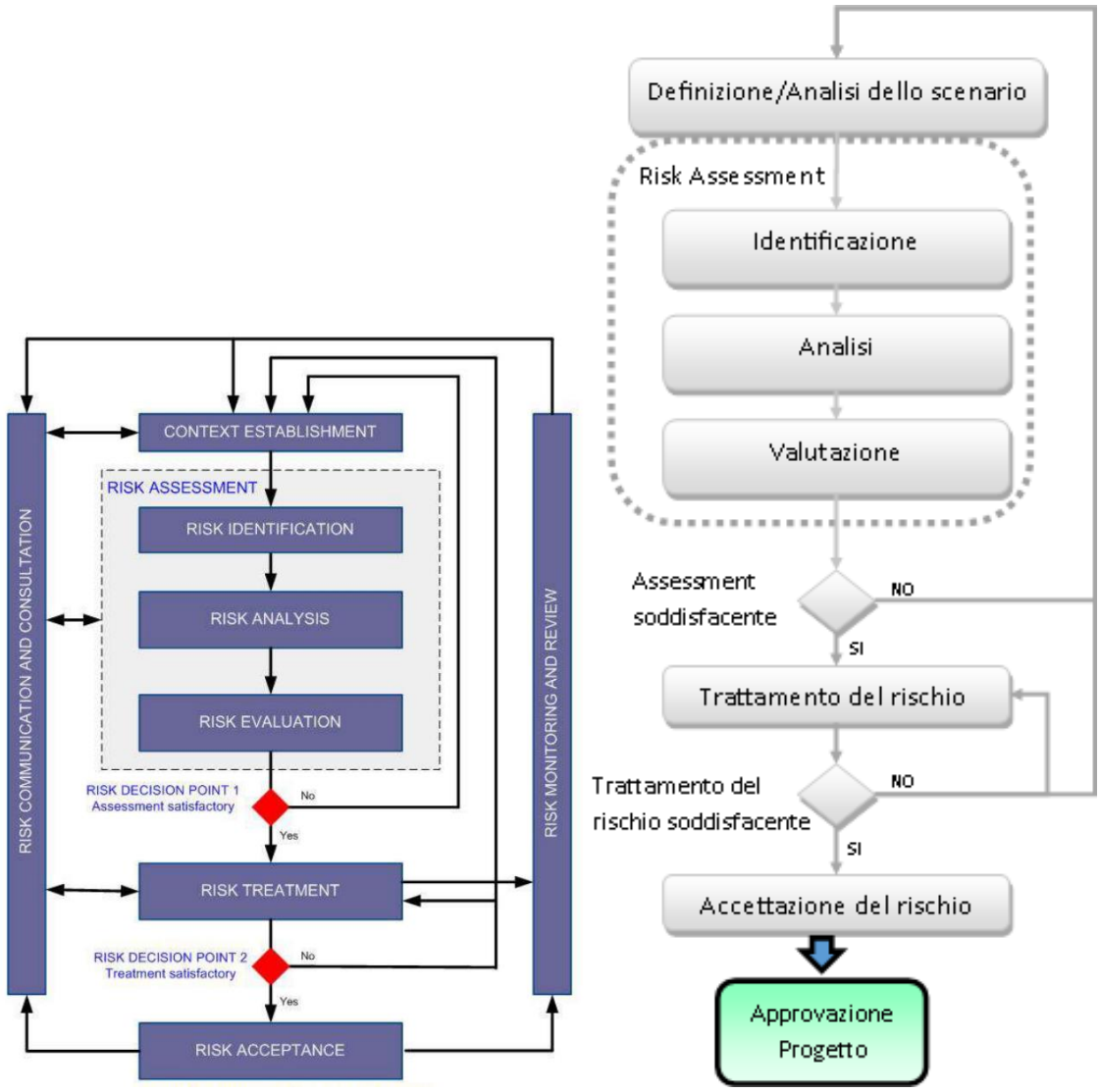

Figura 3 – ISO 27005: Risk Management Process (a) ed applicazione al processo di acquisizione (b).

Come descritto in Figura 3, il *Risk Assessment* è una delle fasi centrali del processo e lo strumento per valutare il sistema (vedasi *Risk Decision Point* 1).

Per poter ottenere un sistema "*Secure by Design"* diventa necessario avviare il processo di *Risk Management* fin dalle fasi di progettazione. Il *Risk Assessment* diventa quindi un documento di progetto che dovrà essere valutato **prima dell'avvio** della fase di sviluppo. Infatti, il progetto potrà subire delle modifiche proprio in ragione della necessità di mitigazione del rischio cibernetico.

Nelle fasi di sviluppo potranno inoltre essere individuate anche ulteriori vulnerabilità dei sistemi, cosa che richiederà un aggiornamento del *Risk Assessment* e l'introduzione di eventuali ulteriori modifiche al progetto.

L'accettazione finale del rischio residuo dovrà essere effettuata dagli Enti competenti in coordinamento con l'Ente preposto al collaudo ed accettazione del sistema.

Con l'intento di permettere l'implementazione del modello di "gestione continua" del rischio indicato dalla ISO 27005, la Relazione Tecnica di Valutazione del Rischio Cibernetico sarà consegnata assieme al sistema collaudato a chi ne gestirà la conduzione. In analogia a quanto avviene per il Documento di

Valutazione del Rischio per la sicurezza sul lavoro, la valutazione del rischio cibernetico necessiterà di aggiornamenti periodici per tutto il ciclo di vita del Sistema.

10.2 La redazione della Relazione Tecnica di Valutazione del Rischio (RTVR) o *Technical Risk Assessment Report.*

A partire da quanto definito nella ISO 27005 per il processo di valutazione del rischio cibernetico, la redazione della Relazione Tecnica di Valutazione del Rischio potrà essere effettuata anche mediante l'applicazione di altri standard. La norma ISO 27005 rimane piuttosto generica nelle modalità operative di valutazione quantitativa dei rischi. Per questo è naturale attendersi l'applicazione di metodologie operative differenti a seconda delle aziende o delle organizzazioni che effettueranno tali stime. Ad esempio, potranno essere impiegate le modalità definite nella norma NIST 800-30 o potranno essere applicati *framework open source*, come la metodologia FAIR e, in particolare, la sua tassonomia del rischio per la valutazione della magnitudo e della probabilità. La metodologia FAIR risulta particolarmente indicata in conforto ad una valutazione del rischio derivata da altra metodologia in quanto consente di riverberare i potenziali rischi individuati nei discendenti impatti economici, per i quali corrispondono azioni di mitigazione spesso molto onerose. In tali casi, il rapporto costi/benefici diventa facilmente esprimibile attraverso una misura economica del rischio, il cui valore risulta direttamente confrontabile con gli investimenti economici richiesti per la mitigazione.

Annesso 1 – Selezione dei requisiti di Sicurezza Cibernetica per la scrittura della Specifica Tecnica

1 Introduzione

I Requisiti funzionali richiamati sono funzione dei concetti generali di sicurezza cibernetica e sono applicabili a tutti i sistemi, classificati e non, IT e OT. Tuttavia, come descritto nel corpo della NAV, i sistemi classificati possiedono un preciso percorso dettagliato nelle pubblicazioni di cui alla serie Rif.[Nx]. Pertanto, obiettivo del presente Annesso 1 sono i sistemi IT Non Classificati e i sistemi OT.

Gli elementi fondanti sono richiamati nel capitolo 8.

2 Requisiti funzionali per la sicurezza cibernetica

2.1 Politiche di sicurezza

minimale

I sistemi IT/OT della Difesa dovranno essere inquadrati uno specifico contesto di applicazione. In base al contesto applicativo dovranno essere richiamate a riferimento le pertinenti politiche di sicurezza, o documenti di policy, definiti dagli Enti preposti. Il riferimento esplicito a documenti di policy della Difesa permetterà ai progettisti di verificare l'applicabilità delle politiche di sicurezza al sistema complesso da progettare, costituendo una guida imprescindibile per la corretta implementazione all'interno del progetto.

Le politiche di sicurezza sono soggette a revisione continua specie nelle parti più strettamente legate ai dettagli implementativi e tecnologici[31]. Per questo

minimale

L'implementazione tecnica delle politiche di sicurezza dovrà prevedere una certa flessibilità e lasciare la libertà ai responsabili della sicurezza dei sistemi di adeguare i provvedimenti implementativi alle nuove esigenze, limitando al massimo le esigenze di modifica radicale di hardware e software applicativo.

Esempio: Regole per la composizione delle password flessibili e configurabili.

Esempio: Profili utente e stratificazione delle gerarchie dei ruoli operatore personalizzabili/configurabili.

Alle politiche di sicurezza discendenti da norme o disposizioni emanate dagli Enti competenti saranno necessariamente aggiunte quelle derivanti dall'analisi del rischio cibernetico (rif. §10). Oltre alle azioni puntuali o alle soluzioni tecniche attuabili per la mitigazione del rischio potranno essere definite anche specifiche policy d'impiego dei sistemi.

2.2 Organizzazione della sicurezza delle informazioni

I sistemi sviluppati secondo le presenti linee guida dovranno rispondere alle policy di sicurezza definite dagli Enti preposti di FA e della Difesa. In ogni caso dovranno essere garantiti i seguenti requisiti funzionali per una corretta gestione ed implementazione delle policy.

2.2.1 Ruoli e responsabilità per la sicurezza delle informazioni

Tutte le responsabilità relative alla sicurezza delle informazioni dovrebbero essere definite e assegnate (ISO27002).

minimale

Questo requisito funzionale implica che il sistema informatico dovrà essere progettato prevedendo al minimo la definizione di ruoli distinti fra utente e amministratore.

[31] *ISO27002 §5 Riesame delle politiche per la sicurezza delle informazioni*

avanzato

Laddove le policy di sicurezza applicabili prevedano ruoli specifici questi dovranno corrispondere a modalità di autenticazione/ profilazione adeguati alla loro corretta implementazione nel sistema.

2.2.2 Separazione dei compiti

I compiti e le aree di responsabilità in conflitto tra loro dovrebbero essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset(risorse) dell'organizzazione.

In relazione alla complessità del sistema e alla complessità dell'organizzazione del *sistema di gestione* implementabile, dovrà essere implementata una corretta separazione dei compiti da assegnare a ciascun ruolo definito all'interno del sistema informatico. Dovrà essere implementato un sistema di autenticazione e/o di controllo di accesso al sistema in grado di replicare fedelmente i ruoli organizzativi previsti dalle policy di sicurezza e/o dal modello organizzativo operativo come indicato al para 2.1.

minimale

Nessun individuo dovrebbe poter accedere o modificare un *asset* del sistema senza che vi sia la segnalazione o la registrazione dell'evento. Per quanto possibile la modifica ad un componente (*asset*) del sistema dovrebbe poter essere eseguita da un individuo ed autorizzata/controllata da un terzo indipendente.

La possibilità di collusione dovrebbe essere tenuta in considerazione nella progettazione dei controlli.

2.2.3 Contatti con i CERT di FA, della DIFESA o di organizzazione Internazionali

minimale

Coerentemente con le politiche di sicurezza applicabili al progetto, i sistemi dovranno poter essere inseriti in sistema di gestione della sicurezza di livello superiore. Per questo potranno essere richiesti livelli di autenticazione e accesso ai sistemi che permettano agli organismi preposti alla gestione delle Emergenze Cyber come i CERT di Forza Armata di poter intervenire sui sistemi in modo rapido e efficace. Questo potrebbe richiedere anche l'accesso remoto ai sistemi per la gestione delle emergenze o per il controllo ispettivo della corretta applicazione delle politiche di sicurezza vigenti.

2.3 Gestione dei componenti/*asset* dei sistemi (ISO27002 cap.8)

Tutti i componenti hardware e software che compongono un sistema IT/OT dovranno essere gestiti "in configurazione". L'insieme dei componenti hardware e software potranno essere analizzati per la definizione corretta del Risk Assessment Cyber (rif. §Valutazione del rischio cibernetico10). Dovendo garantire una corretta gestione del sistema complesso, per ciascun *asset* dovrà essere possibile individuare ruoli e responsabilità in modo chiaro nel sistema di gestione della sicurezza.

Come sarà chiarito nei paragrafi successivi, la corretta verifica della configurazione hardware e software è alla base delle attività di controllo di ***integrità*** dei sistemi IT e OT.

La gestione in configurazione nel ciclo di vita di un sistema IT/OT è necessaria sia per il corretto supporto logistico sia per la corretta gestione della sicurezza cibernetica.

Ciascun sottosistema o componente del sistema IT/OT sarà inserito nel Risk Assessment per una corretta valutazione del Rischio Cibernetico.

2.3.1 Classificazione degli asset e delle informazioni

Le informazioni dovrebbero essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate (ISO27002 §8.2)

Come risultato del *Risk Assessment Cyber* per il sistema IT/OT, dovranno essere indicate le risorse di maggior valore. Come sarà chiarito nel capitolo 10 dedicato al *Risk Assessment*, con la fornitura di

un nuovo sistema potrà essere richiesto un primo *Risk Assessment* tecnico/funzionale per il quale potrà essere valutato il valore di ciascun asset in base all'impatto funzionale sulle capacità del sistema IT/OT rispetto ad un set di minacce cibernetiche standard (ad esempio rif. NIST 800-30). Un *Risk Assessment* completo richiede la partecipazione attiva dell'organizzazione di riferimento e un'analisi delle minacce di competenza degli Enti preposti.

minimale

- (requisito minimo) Per la fornitura di un sistema IT/OT potrà essere richiesta una valutazione qualitativa della criticità dei componenti hardware e software del sistema.

avanzato

- (requisito ideale) Per la fornitura di un sistema IT/OT Potrà essere richiesto un'analisi del Rischio Cibernetico di tipo tecnico/funzionale su tutti gli asset del sistema.

Definito il valore degli asset e l'eventuale classifica dei sistemi, dovrebbero essere definite delle procedure per trattare, elaborare, archiviare e comunicare le informazioni in modo coerente con la loro classificazione (IT), o alla rilevanza funzionale per il sistema complesso di appartenenza (OT).

Potrà essere richiesto:

a) la limitazione degli accesi, anche fisici, a sostegno dei requisiti di protezione per ciascun livello di classificazione o livello di criticità dei componenti per prevenire accessi da parte di personale non autorizzato (es. chiusura con chiave, combinazione o lucchetto di armadi e rack; predisposizione segnalazioni di allarme);

b) il mantenimento di registrazioni formali degli accessi agli asset critici (es. registrazione allarmi e aperture armadi e/o rack);

c) la protezione di copie temporanee o permanenti delle informazioni ad un livello coerente con la protezione delle informazioni originarie;

d) l'archiviazione degli asset IT in conformità con le specifiche dei produttori;

e) la chiara marcatura di tutte le copie dei supporti all'attenzione dei destinatari autorizzati

Per i sistemi ad alta classifica saranno implementate le norme specifiche di cui alla documentazione Rif.[Nx] e di cui al paragrafo 6.

2.4 Requisiti per il controllo degli accessi ai sistemi

2.4.1 Politiche di controllo degli accessi

minimale

Saranno applicate le politiche di controllo degli accessi definite dagli Enti competente ove applicabile. In tutti i casi dovranno essere applicati i seguenti principi di progettazione per i sistemi di autenticazione.

a) la **necessità di conoscere** (***need-to-know***): si è autorizzati ad accedere solo alle informazioni di cui si ha bisogno per eseguire i propri compiti; differenti compiti/ruoli implicano necessità differenti di conoscenza e quindi differenti profili di accesso.
b) la **necessità d'uso** (***need-to-use***): si è autorizzati ad accedere solo alle strutture di elaborazione delle informazioni (apparecchiature IT/OT, applicazioni, procedure, locali) di cui si ha necessità per eseguire il proprio compito/lavoro/ruolo.

Dovranno quindi essere applicate regole basate sul presupposto "**Tutto è generalmente <u>vietato</u> se non espressamente permesso**" invece del più debole *"Tutto è generalmente permesso se non espressamente vietato".*

minimale

La definizione dei ruoli è e dei permessi di accesso dovrà anche rispecchiare l'effettiva organizzazione funzionale degli utenti finali.
Sarà inoltre necessario verificare la presenza di specifici ruoli previsti dal **quadro normativo applicabile**, specie per i controllori, i manutentori o i **responsabili della sicurezza**.

avanzato

Allo scopo di poter agevolare le attività di controllo o le attività forensi per i sistemi critici o ad alta classifica sarà necessario effettuare l'archiviazione delle registrazioni di tutti gli eventi significativi concernenti l'uso e la gestione delle identità degli utenti e delle informazioni segrete (es. password) di autenticazione; l'archiviazione potrà essere **parziale**, ovvero registrando solo le ultime modifiche al profilo.

stringente

Per i sistemi critici l'archiviazione dovrà essere **completa** di tutte le variazioni ai profili (storico completo delle modifiche con *timestamp* e utente che ha eseguito l'operazione).

avanzato

Per i sistemi complessi può essere richiesta la segregazione dei ruoli di controllo degli accessi, distinguendo ad esempio fra richieste di accesso, autorizzazioni di accesso, amministrazione dell'accesso.

2.4.2 Sistemi di Gestione degli accessi

Per una corretta gestione degli accessi ad un sistema IT e OT dovrebbe essere attuato un processo formale di registrazione e de-registrazione degli utenti per abilitare e disabilitate l'assegnazione dei diritti di accesso.

minimale

Dal punto di vista implementativo per i sistemi complessi è importante l'utilizzo di **user ID univoche** per consentire il collegamento tra gli utenti e le loro azioni, in modo da garantire la corretta corrispondenza fra operazioni effettuate e responsabile dell'attività (***accountability***); l'uso di indentificativi condivisi, come ad esempio password di amministrazione o accesso a sistemi distribuiti (IOT), è permesso solo quando per ragioni tecniche od operative non sia altrimenti possibile, o quando il rischio derivante sia ritenuto comunque accettabile. In questi casi potranno essere previste procedure di controllo aggiuntive e/o procedure di aggiornamento delle credenziali (es. cambio password periodico e condizionato all'avvicendamento del personale responsabile) specifiche per il modello di impiego previsto per il sistema/sottosistema.

minimale

In caso di avvicendamento del personale o di modifica delle attribuzioni gli account nominativi dovranno essere disabilitati. Questo non implica la rimozione dei dati personale. Dove possibile è preferibile la disabilitazione degli account e/o il cambio delle password, invece della loro cancellazione per evitare di perdere dati storici sulle operazioni effettuate sugli asset software e hardware del sistema da parte degli *operatori protempore* (esigenze forensi/ gestione in configurazione del sistema).

avanzato

Nei sistemi complessi e ove ritenuto necessario, per gli utenti con alti privilegi sarà richiesta la registrazione di tutte le modifiche dei privilegi stessi, in modo da permettere la ricostruzione delle autorizzazioni protempore e il possibile riconoscimento di ***privilege escalation*** non autorizzate.

minimale

La strutturazione dei ruoli deve rispecchiare quanto più possibile l'organizzazione funzionale corrispondente agli incarichi assegnati al personale che impiegherà i sistemi. Questo potrà rendere più semplice la gestione delle autorizzazioni all'accesso ai sistemi in fase di cambio incarico, in caso di sostituzione temporanea o di ristrutturazione gerarchica dell'organizzazione.

2.4.3 Gestione degli accessi di tipo privilegiato

Per accessi di tipo privilegiato si intendono i profili in grado di apportare modifiche significative al funzionamento dei sistemi. Fra questi rientrano ovviamente i profili di amministrazione e/o manutenzione.

L'assegnazione e l'uso di diritti di accesso privilegiato dovrebbero essere limitati e controllati.

minimale

Dovranno essere identificati i diritti di accesso privilegiato relativi a ciascun sistema o processo (per esempio per i sistemi operativi, i sistemi di gestione di database, ciascuna applicazione, sottosistema e servizio software) e gli utenti a cui è necessario assegnarli.

avanzato

Quando possibile, i diritti di accesso privilegiato dovrebbero essere assegnati a user ID differenti da quelle usate nelle attività di business quotidiane. L'attività quotidiana di un utente non dovrebbe essere eseguita tramite un account privilegiato.

minimale

E' infatti necessario introdurre un consenso esplicito all'attivazione di un profilo amministrativo applicando in ogni caso il principio di minimo privilegio (*need to use - need to know)*

minimale

Per le ***user ID*** amministrative generiche, ovvero non nominative, dovrebbe essere mantenuta la riservatezza delle informazioni segrete di autenticazione quando questa è condivisa. Sarà quindi necessario cambiare password periodicamente e/o in occasione di avvicendamento, sospensione o eliminazione dei relativi ruoli organizzativi.

2.4.4 Responsabilità degli utenti e gestione dell'accounting

Gli utenti di un sistema IT e OT sono responsabili della salvaguardia delle loro informazioni di autenticazione. Le prassi di gestione di queste informazioni sono particolarmente critiche per la corretta gestione degli accessi al sistema. La complessità delle modalità di autenticazione è da ridurre al minimo in ragione della corretta usabilità del sistema, allo scopo cioè di non indurre gli utenti finali ad aggirare le difficoltà di accesso mediante pratiche non sicure.

avanzato

Per questo è generalmente incentivato l'uso di strumenti di single sign-on o di altri strumenti per la gestione delle informazioni segrete di autenticazione, riducendo la quantità di informazioni che gli utenti hanno la necessità di proteggere, aumentando l'efficacia di questo controllo. Ciò nonostante questi strumenti possono anche amplificare l'impatto della divulgazione delle informazioni segrete di autenticazione. Per questo l'uso di strumenti di single sign-on deve corrispondere ad una maggiore e capillare applicazione dei requisiti di parcellizzazione/specializzazione delle utenze privilegiate, attuando politiche di accesso multilivello sui diversi asset hardware e software del sistema.

2.4.5 Procedure di log-on sicure

Quando richiesto dalle politiche di sicurezza, sia in applicazione di norme e disposizioni, sia in risposta alla necessità di mitigare i rischi residui individuati dal *risk assessment cyber* (rif §10), le procedure di log-on dovranno essere rinforzate.

avanzato

L'obbiettivo delle procedure di log-on è evidentemente dimostrare l'identità dichiarata di un utente. Quando sono richieste un'autenticazione forte ed una verifica d'identità, dovrebbero essere utilizzati metodi di autenticazione alternativi alle password quali mezzi crittografici, *smart card*, *token* o dispositivi biometrici.

avanzato

In questi casi l'autenticazione sarà eseguita in più fasi, combinando le predette metodologie fra loro in almeno 2 fasi.
Esempio di autenticazione in 2 fasi: Accesso con user e password (credenziali di accesso 1°fase) ed invio sms con *one time-token* (possesso SIM CARD per ricezione SMS 2°fase).

stringente

In questi casi l'autenticazione sarà eseguita in più fasi, combinando le predette metodologie fra loro in almeno 3 fasi.
Esempio di autenticazione in 3 fasi: Accesso con user e password (credenziali di accesso 1°fase), invio di token crittografico su dispositivo o account proprietario (2°fase), sblocco *token* crittografico mediante chiave privata su sistema biometrico o SMART CARD. (3°fase).

minimale

La procedura per l'accesso ad un sistema o ad un'applicazione dovrebbe essere progettata per minimizzare le opportunità di accessi non autorizzati. La procedura di log-on dovrebbe quindi rivelare il minimo di informazioni circa il sistema o l'applicazione, al fine di evitare di fornire ad un utente non autorizzato ogni assistenza non necessaria.

minimale

Per la realizzazione di una procedura di log-on vi sono delle buone prassi da seguire valide indipendentemente dal contesto di applicazione. La procedura di log-on deve:

a. mostrare un messaggio di avviso generale che il sistema dovrebbe essere acceduto solo da utenti autorizzati;

b. non mostrare identificativi di sistemi o applicazioni fino a quando il processo di log-on sia stato completato con successo;

c. non fornire messaggi di aiuto durante la procedura di log-on che potrebbero facilitare un utente non autorizzato;

d. validare le informazioni di log-on solo al completamento dell'inserimento di tutti i dati. Nel caso in cui si verifichi una condizione di errore, il sistema non dovrebbe indicare quale parte dei dati è corretta o scorretta;

e. proteggere da tentativi di log-on a "forza bruta";

f. tracciare i tentativi riusciti e quelli falliti;

g. segnalare un evento di sicurezza nel caso in cui venga rilevata un potenziale violazione, tentata o riuscita, dei controlli di log-on;

h. visualizzare le seguenti informazioni al completamento con successo di un log-on:

   i. data e ora del precedente log-on effettuato con successo;

   ii. dettagli di ogni tentativo di log-on fallito dall'ultimo log-on effettuato con successo;

i. non mostrare la password inserita se non espressamente richiesto dall'utente. La visualizzazione della password deve essere possibile specie se in presenza di input touch, tipicamente impreciso;

j. non trasmettere la password in chiaro (al di fuori del processo attivo e dei suoi threads);

k. terminare le sessioni inattive dopo un determinato periodo di inattività, specialmente in luoghi ad alto rischio come aree pubbliche o aree esterne alla gestione della sicurezza dell'organizzazione o su dispositivi mobili;

limitare il tempo di connessione per fornire sicurezza aggiuntiva alle applicazioni ad alto rischio e ridurre la finestra di opportunità per accessi non autorizzati.

2.4.6 Sistemi di gestione delle password

Le password sono un modo comune per fornire identificazione ed autenticazione basata su un segreto che solo l'utente conosce. Lo stesso obiettivo può anche essere raggiunto con mezzi crittografici e con protocolli di autenticazione. La robustezza dell'autenticazione dell'utente dovrebbe essere appropriata per la classificazione delle informazioni accedute.

I sistemi di gestione delle password devo essere realizzati mediante interfacce interattive che guidino gli utenti alla scelta di combinazioni alfanumeriche sufficientemente robuste rispetto ad attacchi di tipo a **dizionario**.

Il sistema di gestione delle password deve:

minimale

a. forzare l'uso di identificativi utente e password individuali per mantenere la tracciabilità delle attività sui sistemi;
b. permettere agli utenti di selezionare e cambiare la propria password e includere una procedura di conferma per errori di input (se non assegnate da Enti terzi);
c. forzare la scelta di password di qualità, in base anche alle politiche vigenti;
d. forzare gli utenti a cambiare la loro password al primo log-on se provvisti di password di default note (se non assegnate da Enti terzi);
e. forzare un cambio periodico e quando necessario delle password;
f. mantenere una registrazione delle password precedentemente usate per prevenire il loro riuso;
g. non mostrare le password sullo schermo quando vengono inserite; La richiesta di visualizzazione, specie per password molto complesse, deve essere esplicita e solo temporanea;
h. memorizzare i file delle password (o il database) separatamente dai dati del sistema applicativo (dove applicabile);
i. memorizzare e trasmettere le password in modo protetto, mediante *hashing* o crittografia asimmetrica

Alcune applicazioni richiedono che le password degli utenti siano assegnate da parte di autorità indipendenti; in questi casi, i punti b), d) ed e) della guida precedente non si applicano. Nella maggior parte dei casi le password sono scelte e mantenute dagli utenti.

2.4.7 Autenticazione per l'uso di moduli software di utilità con alti privilegi

La presenza di moduli software di utilità in grado di aggirare in qualche modo i controlli dei moduli applicativi che gestiscono l'autenticazione degli utenti ai sistemi critici può costituire un mezzo per l'aggiramento delle protezioni messe in atto e la **scalata dei privilegi** nel sistema che li ospita. L'uso di Sistemi Operativi commerciali e in generale l'uso di piattaforme COTS porta con sé la presenza di applicativi dedicati alla gestione e manutenzione del sistema operativo non utili alle funzioni di business e causa di vulnerabilità indesiderate all'intero sistema IT/OT.

L'uso di questi strumenti software deve essere pertanto limitato e strettamente controllato. In particolare, devono essere applicati i seguenti principi di progettazione:

a) utilizzo di procedure di identificazione, autenticazione e autorizzazione per i programmi di utilità a similitudine di quanto fatto per gli account privilegiati;
b) separazione/segregazione dei programmi di utilità dai software applicativi;
c) limitazione dell'uso di programmi di utilità al minimo numero praticabile di utenti fidati e autorizzati;
d) autorizzazione ad hoc per l'uso dei programmi di utilità;

e) limitazione della disponibilità dei programmi di utilità, per esempio per la durata di un cambiamento autorizzato;

f) tracciamento di tutti gli utilizzi dei programmi di utilità;

g) definizione e documentazione dei livelli di autorizzazione per i programmi di utilità;

h) rimozione o disabilitazione di tutti i programmi di utilità non necessari;

i) non disponibilità di programmi di utilità a utenti che hanno accesso ad applicazioni su sistemi dove è richiesta una separazione dei compiti. L'accesso consentito corrisponderà ad esempio ai soli profili privilegiati.

È di massima preferibile, se non espressamente richiesto dalle politiche di sicurezza applicabili, l'impiego di Sistemi Operativi privi di tutti gli applicativi accessori non necessari al corretto funzionamento dei software di interesse primario. Saranno quindi richieste distribuzioni Linux minimali o versioni Windows dedicate (es. Windows LTSB).

2.4.8 Controllo degli accessi al codice sorgente dei programmi

minimale

È possibile che nei sistemi acquisiti siano disponibili anche i codici sorgente degli applicativi in uso, sia per motivi di manutenzione (es. PLC) sia di sviluppo continuo e/o personalizzazione delle funzioni. Alcuni applicativi potrebbero essere di natura Open Source, o comunque potrebbero richiedere una pubblicazione anche parziale su piattaforme pubbliche o accessibili anche da terze parti. Per questi devono essere considerati controlli aggiuntivi per aiutare ad ottenere **garanzie sulla loro integrità** (ad esempio firme digitali o controllo degli hash).
Gli accessi al codice sorgente dei programmi ed ai relativi elementi (come progetti, specifiche, piani di verifica e di validazione) devono essere strettamente controllati al fine di prevenire l'introduzione di funzionalità non autorizzate e di evitare cambiamenti non intenzionali, nonché per mantenere la riservatezza della proprietà intellettuale di valore.

Relativamente al codice sorgente dei programmi, questo può essere realizzato attraverso un archivio centrale controllato del codice, preferibilmente in librerie dei codici sorgente dei programmi. Le seguenti linee guida dovrebbero essere, quindi, considerate per controllare l'accesso a queste librerie dei codici sorgente dei programmi al fine di ridurre la possibilità di corruzione di un programma. In estrema sintesi:

a) dove possibile, le librerie dei codici sorgente dei programmi non dovrebbero essere mantenute sui sistemi di produzione; se parte del codice sorgente fosse funzionale alle attività manutentive questo dovrà essere accessibile solo ai relativi profili privilegiati.

b) il codice sorgente dei programmi e le librerie dei codici sorgente dei programmi devono essere gestiti secondo procedure applicabili per lo specifico contesto applicativo; se non imposto da norme specifiche, lo sviluppatore renderà noto lo standard scelto ed applicato per il controllo del codice sorgente; (*qualità del software*)

c) il personale di supporto non dove avere accesso illimitato alle librerie dei codici sorgente dei programmi; in particolare la modifica del codice sorgente non potrà essere eseguita da profili di manutenzione o supporto, ma solo da specifici profili privilegiati di amministrazione (a supporto del processo di autorizzazione delle modifiche);

d) l'aggiornamento delle librerie dei codici sorgente dei programmi e degli elementi associati e la pubblicazione dei codici sorgente dei programmi per i programmatori dovrebbero essere eseguiti solo dopo aver ricevuto appropriate autorizzazioni;

e) i listati dei programmi devono essere mantenuti in un ambiente sicuro;

f) In fase di produzione deve essere mantenuto un audit log di tutti gli accessi alle librerie dei codici sorgente dei programmi;

g) la manutenzione e la copia delle librerie dei codici sorgente dei programmi dovrebbero essere soggette a strette procedure di controllo.

2.5 Crittografie e chiavi crittografiche.

Allo scopo di assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni potranno essere applicate le policy di controllo delle informazioni classificate (ove applicabile) e le policy di controllo delle relative chiavi di cifratura applicabili tecnicamente per il sistema e previste dagli Enti preposti di FA e della Difesa, nonché in rispetto delle norme nazionali ed internazionali applicabili nel contesto d'impiego operativo del sistema IT/OT.

Il contesto applicativo non classificato può infatti beneficiare delle esperienze maturate nell'ambito della protezione delle informazioni per i sistemi classificati implementando, dove opportuno, processi e metodologie di protezione della **riservatezza** in uso nel mondo classificato per garantire **disponibilità** ed **integrità** dei servizi non classificati.

2.5.1 Politiche sull'uso dei controlli crittografici

Nell'attuazione della politica dell'organizzazione per la crittografia, si dovrebbero tenere in considerazione i regolamenti e le restrizioni nazionali che potrebbero essere applicati all'utilizzo di tecniche crittografiche in diverse parti del mondo e le questioni relative ai flussi transfrontalieri di informazioni crittografate (ove applicabile).

La crittografia potrà essere richiesta per i seguenti scenari applicativi:

a) **riservatezza**: utilizzando la crittografia delle informazioni per proteggere informazioni critiche, sia memorizzate sia trasmesse;

b) **integrità/autenticità**: utilizzando la firma elettronica oppure codici di autenticazione dei messaggi per verificare l'autenticità e l'integrità delle informazioni critiche, memorizzate o trasmesse;

c) **non ripudio**: utilizzando tecniche crittografiche per ottenere evidenze del verificarsi o del non verificarsi di un evento o azione;

d) **autenticazione**: utilizzando tecniche crittografiche per autenticare gli utenti e altre entità di sistema che richiedono l'accesso oppure effettuano transazioni con gli utenti del sistema, entità e risorse;

La valutazione dell'appropriatezza di un sistema di controllo crittografico o dell'adeguatezza degli algoritmi utilizzati per lo scenario di impiego ipotizzato per il sistema IT/OT dovrà essere rimandata agli Enti preposti, avvalendosi se necessario di consulenza specialistica.

2.5.2 Gestione delle chiavi

L'implementazione di sistemi crittografici implica anche la gestione delle relative chiavi di cifratura. Un sistema di gestione delle chiavi dovrebbe essere basato su un insieme concordato di norme, procedure e metodi sicuri per:

a) generare chiavi per sistemi crittografici e applicazioni differenti;

b) emettere e ottenere certificati a chiavi pubbliche;

c) distribuire chiavi alle entità previste, includendo le indicazioni su come dovrebbero essere attivate una volta ricevute;

d) memorizzare le chiavi, comprese le modalità affinché gli utenti autorizzati ottengano l'accesso alle chiavi;

e) modificare o aggiornare le chiavi, comprese le regole su quando le chiavi dovrebbero essere cambiate e su come questo è fatto;

f) come comportarsi in caso di chiavi compromesse;

g) revocare le chiavi, comprese le modalità con cui dovrebbero essere revocate o disattivate, per esempio quando le chiavi sono state compromesse o quando un utente lascia un'organizzazione (nel cui caso, le chiavi dovrebbero anche essere archiviate);

h) recuperare le chiavi smarrite o corrotte;

i) sottoporre a back-up o archiviare le chiavi;

j) distruggere le chiavi;

k) sottoporre a log e audit le attività relative alla gestione delle chiavi.

Attenzione. Le tecniche crittografiche possono anche essere usate per proteggere le stesse chiavi crittografiche. Potrebbe essere necessario prendere in considerazione delle procedure per la gestione di richieste di l'accesso alle chiavi crittografiche: potrebbe essere necessario rendere disponibili le informazioni crittografate in una forma *non crittografata* come **prova in un procedimento giudiziario**.

2.6 Sicurezza Fisica ed Ambientale

Allo scopo di prevenire l'accesso fisico non autorizzato, danni, manomissioni o limitazioni di accesso alle informazioni sensibili dell'organizzazione o alle funzionalità critiche di un sistema OT, è necessario proteggere anche fisicamente le strutture di elaborazione delle informazioni da accessi non autorizzati.

Saranno quindi implementate tutte le prescrizioni previste dalla normativa applicabile per i sistemi classificati e le policy di protezione previste dagli Enti Competenti per la segregazione fisica dei sistemi IT/OT.

2.6.1 Perimetro di sicurezza e protezione degli asset critici.

Gli elementi critici di un sistema IT/OT dovranno essere protetti da adeguate misure di segregazione fisica, in modo da limitarne l'accesso fisico da parte di soggetti non autorizzati e/o segnalarne l'accesso mediante meccanismi di log e/o di allarme.

L'accesso ai Server o alle componenti hardware principali di un sistema OT sarà limitato mediante l'uso di armadi provvisti di serrature e/o dotati di dispositivi di allarme. Le scelte tecniche adottate dovranno essere coerenti con il Risk Assessment prodotto in fase di progettazione preliminare (CDR[32]) o comunque a valle della definizione dell'architettura del sistema IT/OT (SDR[33]).

2.6.2 Fattori ambientali

Se non già specificatamente previsto dalle norme applicabili per gli ambienti di destinazione dei sistemi IT e OT, gli apparati dovranno essere dimensionati in modo da soddisfare i requisiti ambientali dei locali di destinazione. Dove questo non sia tecnicamente applicabile gli asset saranno dotati di sistemi di protezione (grado IP), supporti antivibranti e/o antishock o sistemi di

[32] CDR - *Critical Design Review*.
[33] SDR - *System Design Review*.

refrigerazione supplementari in grado di preservare il corretto funzionamento degli apparati e garantire la continuità operativa dei sistemi.

2.6.3 Fattori ambientali e ridondanza fisica dei componenti

Per i sistemi per i quali è prevista una ridondanza dei componenti, la dislocazione fisica di questi dovrà essere definita tenendo conto di fattori di rischio come l'incendio o l'allagamento dei locali che li conterranno.

Per sistemi destinati a unità combattenti la separazione fisica dovrà essere realizzata in armonizzazione con i piani di *difesa passiva* da eventi esterni.

Per sistemi critici distribuiti geograficamente sul territorio, la separazione fisica dei sistemi ridondanti dovrà essere studiata in modo da garantire continuità operativa in caso eventi naturali avversi (es. terremoti e alluvioni).

2.6.4 Sicurezza dei sistemi all'esterno delle aree sicure o accessibili da personale esterno.

I dispositivi dislocati in aree normalmente non presidiate, o esposte all'accesso fisico di personale esterno all'organizzazione di appartenenza, come ad esempio Corpi di Guardia, aree Controllo Accessi, sale riunioni e transiti negli edifici pubblici, ecc., dovranno essere messe in atto specifiche predisposizioni di protezione fisica dei sistemi (vedasi anche §2.6).

I sistemi dotati di autenticazione utente saranno dotati di meccanismi automatici di log-off per garantire la sicurezza degli account in caso di allontanamento anche momentaneo degli operatori o sottrazione del dispositivo (§2.6.4).

2.6.4.1 Dispositivi Mobili o Indossabili

I dispositivi mobili, ovvero tutti quei dispositivi che possono essere facilmente portati al di fuori delle aree di lavoro dell'organizzazione devono essere impiegati con estrema cautela, in quanto possibili vettori di esfiltrazione di dati sensibili o di trasmissione malware e virus.

Per questo è bene considerare:

- strumenti per la protezione fisica dei dispositivi, in particolar modo per garantirne la corretta custodia, sia in fase predisposizione all'utilizzo che in fase di manutenzione (es. fasi di ricarica o esecuzione backup);
- sistemi di protezione hardware e software da accessi indesiderati (es. blocco pin smartcard);
- policy di accesso restrittive con procedure di protezione a più livelli come descritto al para 2.4.5 (es. uso combinato di PIN, dati biometrici, custodia di smartcard o dispositivi equipollenti);
- limitazioni sull'istallazione di software e sul numero di servizi resi disponibili da questi device;
- impiego della crittografia per la protezione dei sistemi di storage locale e per le comunicazioni con i sistemi dell'Organizzazione;
- possibilità di controllo remoto per disabilitare, bloccare o cancellare servizi e dati sui dispositivi sensibili sui dispositivi (es. *smartphone*);
- di norma, non dovrà essere possibile collegare *smartphone* ai computer in dotazione di proprietà dell'Amministrazione o connessi alla rete dell'Amministrazione.

2.6.4.2 *Dispositivi per Corpi di Guardia e per punti di accesso alle infrastrutture*

Allo scopo di tutelare le informazioni gestite dai sistemi a supporto del personale di guardia presso i punti di accesso alle infrastrutture militari, i dispositivi dovranno essere progettati per limitare la visibilità da parte del personale esterno all'organizzazione dei display e degli altri dispositivi di *output* previsti.

2.6.4.3 *Stampanti condivise e stampanti non presidiate*

Le stampanti non presidiate, ovvero tutte le stampanti condivise all'interno di una rete dovranno essere dotate di un sistema di autenticazione in grado di limitare l'accesso agli stampati ai soli proprietari dei documenti.

2.6.5 Manutenzioni presso strutture esterne all'organizzazione

Per lo svolgimento delle attività manutentive sui componenti dei sistemi CIS devono essere applicate le stesse procedure previste per il loro sviluppo e configurazione. Nel corso delle attività manutentive sono infatti possibili alterazioni della configurazione hardware e software dei sottosistemi.

Per questo il fornitore del sistema CIS deve potersi far carico delle attività di controllo sull'operato delle eventuali terze parti coinvolte nel processo supporto in vita, con particolare riferimento alle attività manutentive in sede all'organizzazione o presso siti industriali.

Per i sistemi classificati la selezione di eventuali subfornitori per le attività manutentive seguirà gli stessi criteri applicabili alla fornitura del sistema stesso. In questo caso dovrà infatti essere verificata anche l'idoneità della parte terza a trattare i sistemi classificati.

2.7 Operatività dei sistemi

2.7.1 Meccanismi di controllo e gestione dei sistemi complessi

Per una corretta gestione dei sistemi complessi fortemente eterogenei nella loro composizione, ovvero composti di apparati di diversi produttori, le procedure di gestione dovrebbero essere il più possibile omogenee e quindi coerenti.

minimale

Dove applicabile, è richiesta la convergenza verso *tools* omogenei in grado di garantire l'operatività delle funzioni di gestione e/o di controllo, ovvero *tools* applicabili a tutti i componenti dei sistemi complessi mediante procedure comuni.

Differenti strumenti per l'esecuzione di attività come backup automatici, software anti-malware, audit software o controllo dei log di sistema, possono portare a procedure operative non condivisibili o addirittura non coerenti fra di loro. Questo può portare a inefficienze e *vulnerabilità* dei processi organizzativi.

2.7.2 Gestione dei cambiamenti

Il controllo non adeguato dei cambiamenti ai sistemi e alle strutture di elaborazione delle informazioni è una causa comune di malfunzionamenti dei sistemi o della sicurezza. I cambiamenti all'ambiente operativo, soprattutto quando si effettua un passaggio di un sistema dallo sviluppo alla produzione (es. nelle fasi di *setting to work*, ammodernamento progressivo o di correzione difetti) possono influenzare l'affidabilità dei sistemi e delle applicazioni.

Per le componenti critiche dei sistemi è richiesta un'attività di *de-risking* da effettuare mediante ambienti di prova che simulino il sistema in produzione. È quindi richiesto l'impiego di ambienti test (ambienti virtualizzati o *sandboxes*), che replichino fedelmente il sistema di produzione e che permettano di individuare in sicurezza eventuali problematiche sugli aggiornamenti ai sistemi IT/OT.

Per garantire la continuità operativa dei sistemi devono essere previste delle procedure di fall-back, in modo da poter ripristinare il sistema dai cambiamenti che non abbiano avuto successo o che possano causare problemi imprevisti (bug o nuove vulnerabilità).Tali procedure entreranno a far parte delle *procedure di emergenza* previste nei piani di gestione degli incidenti cyber.

2.7.3 Controllo e gestione della capacità di un sistema

L'uso delle risorse deve essere monitorato in modo da potere verificare costantemente i margini di crescita di un sistema in condizioni di operatività a fronte del loro possibile consumo progressivo. I controlli sulle risorse disponibili permettono di identificare eventuali criticità (colli di bottiglia) ed evitare l'insorgere di problematiche relative al consumo eccessivo di risorse da parte di un determinato processo o sottosistema.

minimale

Per i sistemi OT i tempi di latenza delle comunicazioni e la risposta dei controllori costituiscono un vincolo progettuale primario per il soddisfacimento di specifici requisiti di sicurezza per macchinari e operatori.

avanzato

Il monitoraggio delle risorse correlate agli *asset* critici per il sistema IT/OT sarà collegato a sistemi di allarme automatico che segnalino l'eventuale superamento di determinate soglie di guardia.

2.7.4 Configurazione del software e protezioni *anti-malware (end point protection)*

Fra le minacce tecniche più pericolose vi sono sicuramente i malware, ovvero software appositamente progettati per danneggiare un sistema IT/OT, sottraendo, alterando o neutralizzando risorse materiali e/o immateriali.

minimale

I sistemi saranno quindi dotati di sistemi di controllo anti-malware secondo quanto indicato dagli Enti governativi preposti. In alcuni sottosistemi potrebbe non essere tecnicamente possibile installare un software automatico di controllo dei malware

minimale

Per un corretto sistema di gestione della sicurezza cibernetica dovrà essere comunque possibile verificare l'eventuale alterazione della configurazione software dei sistemi.

minimale

Sarà necessario implementare un sistema di **controllo di configurazione del software**, con particolare riferimento ai software eseguiti all'interno dei sottosistemi critici. Dovrà essere verificata l'autenticità e la corrispondenza dei software eseguiti con quelli previsti dal piano di configurazione del software esteso a tutti i sottosistemi IT/OT.

minimale

Per la verifica di integrità potranno essere impiegate metodologie crittografiche quali firma digitale e/o *hasing* degli *eseguibili*.

avanzato

Per i sottosistemi critici sarà verificata la corretta esecuzione dei processi attivi implementando logiche di *white-list* per i processi attivi.

minimale

I sistemi automatici e/o manuali di protezione contro l'esecuzione di software non autorizzato non dovranno in alcun modo compromettere le attività operative del sistema IT/OT.

2.7.5 Backup dei sistemi

Allo scopo di proteggere i sistemi dalla perdita di dati o per attuare specifiche procedure di ripristino delle funzionalità dei sistemi a seguito di un incidente cibernetico (procedure di *failover*) dovrebbero essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi/sottosistemi secondo una periodicità concordata.

minimale

Ove applicabili dovranno essere implementate le politiche di backup definite dagli Enti competenti.

Le modalità di backup saranno costruite al preciso di scopo di ripristinare il funzionamento dei sistemi IT/OT minimizzando per quanto possibile la perdita di dati e le tempistiche di ripristino a seguito di un incidente.

La tipologia dei dispositivi di memorizzazione e le procedure di verifica periodica di funzionamento delle copie di backup sarà commisurato alle modalità e alla periodicità di effettuazione dei backup.

minimale

Ai backup dovrà essere assicurato il medesimo livello di protezione fisica dei sistemi protetti. Come per la ridondanza (rif. §2.6.3) la separazione fisica fra sistema e copia di backup è funzionale ad assicurare la possibilità di attuare un piano di ripristino delle funzionalità realmente efficace in caso di incidente.

minimale

Ai backup dovrà essere assicurato il medesimo livello di protezione crittografica applicata ai sistemi operanti. Anche le procedure di esecuzione, ripristino e verifica delle copie di backup dovranno essere sottoposte a valutazione di coerenza rispetto alle policy di protezione della confidenzialità dei dati stabilite per la risorsa di riferimento.

2.8 Raccolta dei log e monitoraggio dei sistemi

2.8.1 Registrazione log di allarmi ed eventi

La registrazione dei log contenenti allarmi ed eventi di sistema pone le basi per la realizzazione un sistema di monitoraggio automatizzato in grado di generare rapporti consolidati e allarmi sulla sicurezza dei sistemi controllati.

Con esplicito riferimento alla ISO 27002, i file di log dovranno includere tutti o parte dei seguenti elementi:

a. le user ID;
b. le attività di sistema;
c. la data, l'ora e i dettagli degli eventi principali, per esempio log-on e log-off;
d. l'identità del dispositivo o la sede, se possibile, e l'identificativo del sistema;
e. le registrazioni degli accessi riusciti e falliti al sistema;
f. le registrazioni degli accessi riusciti e falliti ai dati ed ad altre risorse;
g. i cambiamenti alla configurazione di sistema;
h. l'uso di privilegi;
i. l'uso di utilità di sistema e delle applicazioni;
j. i file acceduti e il tipo di accesso;
k. gli indirizzi di rete e i protocolli;
l. gli allarmi prodotti dal sistema di controllo degli accessi;
m. l'attivazione e la disattivazione dei sistemi di protezione, quali gli antivirus e i sistemi per l'individuazione delle intrusioni;
n. le registrazioni delle transazioni applicative effettuate dagli utenti.

Per le reti di comunicazione potranno essere registrati dati di log come indicato al para 2.7.1.

Per i sistemi OT è quasi sempre richiesta la registrazione dei dati di funzionamento dei macchinari controllati completi di eventi ed allarmi, spesso riferendosi ad essa come funzionalità "scatola nera".

Le registrazioni dei dati gestiti da un sistema OT dovranno essere gestite dal punto di vista della sicurezza cibernetica allo stesso modo dei file di log. Per i sistemi SCADA le registrazioni dovranno includere le seguenti funzioni:

a. le user ID degli utenti che operano sull'impianto;

b. eventi ed allarmi correlati alla diagnostica di sistema;

c. eventi ed allarmi correlati al funzionamento degli impianti e dei sottosistemi;

d. eventi di log-on e log-off dello SCADA (se distinto dall'autenticazione ai dispositivi);

e. le registrazioni degli accessi riusciti e falliti al sistema;

f. eventi e comandi inviati dagli utenti autorizzati.

Le informazioni di log (sistemi operativi, software, traffico di rete, ecc.) potranno essere raccolte ed aggregate da sistemi SIEM (*Security Information and Event Management*) in grado di supportare sistemi IDS (*Intrusion Detection Systems*). L'accesso ai dati aggregati dovrà essere soggetto alle stesse regole di accesso dei log e dei backup (para 2.7.5).

Nei casi in cui sarà previsto l'uso di sistemi di log delle comunicazioni di rete, i sistemi potranno essere configurati per la registrazione di:

- Session Data (session flow);
- Packet String Data;
- Full Packet String Data.

In relazione alle modalità di impiego dei sistemi IDS e/o SIEM, per ciascuna categoria di dati di log dovranno essere specificati i requisiti di *Data Retention* (conservazione dei dati) per le tre categorie di log del traffico di rete. Tali requisiti dovranno essere coerenti con quanto definito al para 2.7.5**Errore. L'origine riferimento non è stata trovata.** per le procedure di conservazione dei dati torici.

2.8.2 Protezione delle registrazioni e dei file di log

minimale

I log degli eventi, come pure le registrazioni dei dati per i sistemi OT possono contenere dati critici e personali. Devono quindi essere protetti da manomissioni ed accessi non autorizzati sia i file che gli eventuali database contenenti tali registrazioni. Le misure di protezione saranno applicate sia sui sistemi IT/OT in esercizio, sia sui supporti di memorizzazione impiegati per le funzioni di backup.

minimale

In relazione alla possibile necessità di raccolta e conservazione di evidenze relative ad eventi registrati dai sistemi IT/OT, dovranno essere impiegati meccanismi di verifica dell'integrità dei dati di backup di log e database.

I sistemi di registrazione dovranno essere protetti da:

minimale

a. alterazione delle tipologie di messaggi che vengono registrati;

minimale

b. modifica o la cancellazione dei file di log;

minimale

c. superamento della capacità di memorizzazione dei file di log che porti alla mancata registrazione degli eventi o alla sovrascrittura degli eventi passati.

E' necessario proteggere i log di sistema in quanto, se i dati al loro interno possono essere modificati o cancellati, la loro esistenza potrebbe creare un falso senso di sicurezza.

stringente

Allo scopo di evitare l'alterazione dei dati da parte degli stessi amministratori o attraverso i loro account, deve essere prevista una copia in tempo reale dei log su un sistema al di fuori del controllo degli stessi amministratori di sistema o dell'operatore ad elevati privilegi

2.8.3 Attività di amministratori e manutentori dei sistemi IT/OT

Le attività degli amministratori, dei manutentori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti come da §2.7.5.

I possessori di account privilegiati potrebbero manipolare i log delle strutture di elaborazione delle informazioni sotto il loro diretto controllo. È quindi necessario proteggere e riesaminare i log per mantenere la tracciabilità degli utenti privilegiati.

Parimenti quanto attiene la configurazione hardware e software dei sistemi e sottosistemi IT/OT, gli strumenti di rilevazione delle intrusioni (IDS) dovrebbero essere gestiti al di fuori del controllo diretto degli amministratori locali del sistema IT/OT.

minimale

Dove applicabile la configurazione dei sistemi IDS deve avvenire per tramite o su autorizzazione dei Comandi Sovraordinati, con particolare riferimento ai SOC di F.A. in accordo con le policy di sicurezza applicabili

2.8.4 Sincronizzazione degli orologi

minimale

Gli orologi di tutti i sistemi e sottosistemi di una rete o di un impianto di automazione che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto ad una singola sorgente temporale di riferimento.

Per i sistemi OT questo requisito è strettamente **mandatorio**.

La corretta impostazione degli orologi dei sistemi è importante per assicurare l'accuratezza dei log, delle registrazioni dei dati di funzionamento, che può essere richiesta nel corso di investigazioni o come evidenza in casi legali oppure in azioni disciplinari. Dei log inaccurati possono ostacolare tali investigazioni e danneggiare la credibilità dell'evidenza. Un orologio collegato ad una comunicazione via radio da un orologio atomico autorevole a livello nazionale può essere impiegato come orologio principale per i sistemi che raccolgono log. Un protocollo per la sincronizzazione temporale di rete può essere utilizzato per mantenere tutti i server in sincronia con l'orologio principale. (ISO 27002 §12.4.4).

2.9 Ciclo di vita del software - aggiornamenti ed installazione nuovo software

Per una corretta gestione della sicurezza delle applicazioni di sistema IT/OT è necessario utilizzare un sistema di **controllo delle configurazioni** per mantenere il controllo su tutto il software installato così come sulla documentazione di sistema.

Nel ciclo di vista di un software potranno essere individuate vulnerabilità o bug che potrebbero compromettere la sicurezza dei sistemi complessi in cui sono inseriti. Per questo il **controllo di configurazione del software** è necessario per pianificare l'eventuale intervento per mitigare o risolvere (patch) le vulnerabilità scoperte.

Il software impiegato sui sistemi di produzione dovrebbe essere mantenuto ad un livello di aggiornamento supportato da parte del fornitore. Nel tempo, i produttori di software smetteranno di supportare le versioni più datate del software. L'organizzazione dovrebbe considerare i rischi di impiego di software non supportato.

Il ciclo di vita di un sistema complesso come un Sistema D'Arma o un di un Impianto Complesso come l'Automazione di Piattaforma di Nave è, con buona previsione, molto più lungo rispetto a quello di un software. A partire dai Sistemi Operativi, il supporto offerto dai fornitori di software e hardware COTS è generalmente limitato nel tempo.

minimale

Ove tecnicamente possibile dovranno essere selezionate soluzioni hardware e software con prospettive di supportato in vita il più esteso possibile, valutando l'offerta degli stessi fornitori (ad esempio soluzioni *Long Term Servicing Branch* - LTSB) o di altre aziende e organizzazioni in grado di subentrare a supporto di software ad esempio Open Source.

avanzato

Per i sistemi destinati ad essere impiegati in scenari operativi dovrà essere possibile effettuare gli aggiornamenti software critici (non rimandabili) anche in modalità remota (attraverso reti sicure) o isolata (mediante supporti di memorizzazione trasportabili protetti da manomissioni).

minimale

Gli aggiornamenti e le nuove funzionalità per applicazioni, sistemi operativi e *firmware* devono essere installati sui sistemi in servizio solo dopo test di non regressione estensivi e completati con successo.

I test dovrebbero includere anche verifiche di usabilità, di sicurezza, sugli effetti su altri sistemi e di facilità d'uso e dovrebbero essere effettuati su sistemi separati come test bed o prototipi. Per questo la realizzazione di un idoneo test bed per gli impianti IT/OT è una attività di *de-risking* molto importante.

minimale

Le versioni precedenti dei software e dei firmware devono essere conservate come misura di contingenza allo scopo di garantire una strategia di *rollback* preventiva all'implementazione in servizio degli aggiornamenti.

I sistemi in servizio non dovrebbero ospitare al loro interno piattaforme di sviluppo o i sorgenti degli applicativi a meno che questi non siano necessari alla manutenzione degli impianti a alla loro condotta in assetto degradato. La conservazione dei sorgenti e di questi ambienti di sviluppo deve essere protetta da accessi non autorizzati.

2.10 Ciclo di vita del software - Gestione delle vulnerabilità tecniche

I produttori di hardware e software dovrebbero essere sempre pronti a correggere eventuali problematiche di sicurezza correlate ai propri prodotti. La scelta di prodotti COTS dovrebbe essere guidata anche dalla capacità dei singoli produttori di supportare nel tempo le proprie soluzioni hardware e software (vedasi anche §**Errore. L'origine riferimento non è stata trovata.**.

In caso di sviluppo hardware e/o software specifico per le esigenze di un sistema IT/OT il fornitore sarà chiamato a intervenire su eventuali difetti del proprio prodotto in modo tempestivo. L'eventuale scoperta di vulnerabilità tecniche non precedentemente note dovrà essere riportata immediatamente al produttore per un suo intervento correttivo.

Ad ogni modifica hardware o software potrà essere richiesto un aggiornamento del *vulnerability assessment* e del *risk assessment* di cui al capitolo 10. Valgono pertanto i requisiti di cui al para 2.7.2 in merito alla modifica e aggiornamento del software.

2.11 Limitazioni all'installazione del software

L'installazione non controllata di software su dispositivi informatici può introdurre vulnerabilità e quindi fughe di informazioni, perdita di integrità o altri incidenti relativi alla sicurezza delle informazioni, oppure alla violazione di diritti di proprietà intellettuale.

Su tutti i sistemi IT/OT della Difesa esistono specifiche policy che dovranno essere applicate per impedire agli utenti l'installazione e l'impiego di software non specificatamente autorizzato.

In relazione a quanto specificato per la definizione dei privilegi degli utenti, la possibilità di installare o eseguire nuovi programmi deve essere limitata agli amministratori o manutentori dei sistemi, e comunque tale attività dovrà essere registrate nei log di sistema.

Eventuali sistemi di controllo automatico della configurazione del software dovranno segnalare eventuali anomalie rispetto alla configurazione prevista indipendentemente dal livello di autorizzazione degli amministratori che hanno effettuato la modifica (rischio di *scalata dei privilegi*). L'amministrazione di questi sistemi di monitoraggio della configurazione non dovrà essere in carico agli stessi amministratori di sistema locali, ma dovrà garantita/autorizzata dagli Enti competenti di F.A. o della Difesa.

2.12 Sicurezza delle comunicazioni – Reti

La protezione delle comunicazioni di un sistema IT/OT è determinante per garantirne la sicurezza complessiva. Per questo è necessario assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.

Dettagli aggiuntivi sulla sicurezza delle reti possono essere trovate nella ISO/IEC_27033.

2.12.1 Controlli di rete

Dovrebbero essere attuati controlli per assicurare la sicurezza delle informazioni nelle reti e la protezione dei servizi ad esse relativi dagli accessi non autorizzati.

L'obbiettivo dei sistemi di controllo è la salvaguardia della **riservatezza** e dell'**integrità** dei dati in transito sulle reti e proteggere i sistemi e le applicazioni collegate.

La protezione crittografica applicata alle comunicazioni dovrà essere sempre coerente con il livello di protezione applicato alle informazioni trattate.

Il livello di protezione delle comunicazioni sarà proporzionale all'esposizione delle reti a possibili minacce tecniche (da, richiedendo quindi maggiori precauzioni in caso di impiego di reti pubbliche, reti ad accesso condiviso (con diverse organizzazioni) e reti wireless.

La connessione alle reti di un sistema IT/OT dovrà essere sempre limitata alle sole utenze utili al funzionamento corretto dei sistemi.

minimale

Molti Sistemi IT/OT sono progettati tenendo conto di margini di crescita temporali delle reti. Le connessioni disponibili, come ad esempio le porte di rete dovranno essere protette dall'uso improprio, limitandone la funzionalità a livello amministrativo. I dispositivi di rete dovranno pertanto permettere la disabilitazione delle porte disponibili mediante autenticazione amministrativa (locale o centralizzata).

Per accedere alle risorse di rete i sistemi dovranno prevedere delle forme di autenticazione coerenti con i requisiti di autenticazione di cui al §2.4.

minimale

Per i sistemi IT/OT *mission critical*, ed in particolare per i sistemi che assolvono funzioni di sicurezza per uomini e mezzi, dovranno essere implementati meccanismi di controllo e ridondanza in grado di garantire la **disponibilità** dei servizi di rete e dei sistemi ad essa collegati in caso di incidente. Per questi sistemi di comunicazione sarà richiesta una configurazione almeno "sigle point fault tollerant", ovvero in grado di poter gestire senza interruzione significativa dei servizi un incidente/guasto in uno dei suoi componenti

A protezione delle comunicazioni di rete potranno essere impiegati sistemi di analisi del traffico di rete come i sistemi SIEN e gli IDS.

Per l'implementazione dei sistemi SIEN e IDS gli apparati di rete dovranno essere configurabili in modo de permettere la registrazione del traffico mediante soluzioni come SPAN/Mirror port o similari.

L'uso di eventuali sonde di rete (TAP) potrà essere pianificato in fase di progettazione delle reti del sistema IT/OT ed eventualmente modificato alla luce dei risultati delle attività di VA&PT.

I sensori (sonde, span/mirror ports) saranno collegati ai SIEN e IDS mediante reti di management distinte almeno dal punto di vista logico.

2.12.2 Segregazione delle reti

Per aumentare il livello di sicurezza di un sistema IT/OT complesso è opportuno dividere le reti in distinti domini. I domini possono essere individuati in base a livelli di confidenzialità delle informazioni trattate, a livello unità organizzative, a livello di funzioni applicative o una combinazione delle stesse.

La segregazione dei domini può essere effettuata sia utilizzando reti fisiche distinte sia reti logiche mediante ad esempio VPNs (*Virtual Private Networks*) o VLAN (*Virtual Local Area Network*).

minimale

La segregazione delle reti è richiesta anche per garantire i requisiti di banda dati per le applicazioni mission critical (specie per i sistemi OT) dove la latenza massima per le comunicazioni fra i sottosistemi può diventare determinante per la sicurezza di uomini e mezzi. In questi casi anche l'uso della crittografia potrebbe essere non tecnicamente applicabile per via della complessità degli algoritmi ed il carico elaborativo sui dispositivi di automazione locale e/o IoT. Pertanto la segregazione divine necessaria anche a protezione di protocolli di comunicazione non intrinsecamente non sicuri (es. comunicazioni in chiaro PLC to PLC e PLC to Server).

Il perimetro di ogni dominio deve essere ben definito a livello progettuale. L'accesso tra diversi domini di rete può essere consentito attraverso specifici gateway (per esempio firewall, router, server con funzioni di gateway).

La segregazione dei domini dovrà essere coerente con le politiche di sicurezza applicabili al progetto del sistema IT/OT e coerente con le politiche di controllo degli accessi (vedere para 2.4).

2.12.3 Segregazione delle reti - reti wireless

L'autenticazione, la crittografia e le tecnologie per il controllo di accesso utente delle moderne reti wireless conformi agli standard, **se correttamente realizzate**, possono essere sufficienti per la realizzazione di connessioni dirette alla rete interna dell'organizzazione. (CEI UNI ISO/IEC 27002 2014-05)

Le reti wireless possono essere considerate con *perimetro di rete scarsamente definibile*. Per le applicazioni critiche devono essere considerate come **connessioni esterne** e segregate dall'accesso alle reti interne, a meno di uso di idonei gateway e di tecniche di protezione coerenti con l'assunzione di **collegamento dall'esterno alla rete interna,** e comunque conformemente alle politiche di accesso applicabili al sistema.

Per i sistemi per i quali l'accesso esterno non sia consentito dalle politiche di sicurezza le reti wireless dovranno essere isolate dal resto del sistema.

2.12.4 Protezione delle transazioni dei servizi applicativi

Le informazioni coinvolte nelle transazioni dei servizi applicativi dovrebbero essere protette al fine di prevenire trasmissioni incomplete, errori di instradamento, alterazione non autorizzata di messaggi, divulgazione non autorizzata, duplicazione non autorizzata di messaggi o attacchi di tipo "replay". (cit. ISO27002 §14.1.3).

A tale scopo dovrà essere considerato a valle del risk assessment l'impiego di sistemi crittografia per garantire autenticità, integrità e confidenzialità delle informazioni critiche della transazione.

Anche i protocolli di comunicazione dovranno essere scelti in modo adeguato al livello di sicurezza dei dati trasmessi alla tipologia di applicazione.

La registrazione delle transazioni dovrà essere effettuata al di fuori di ogni ambiente pubblicamente accessibile, riferendosi sia a dispositivi di storage di rete sia a supporti di memorizzazione accessibili da personale non specificatamente autorizzato.

Annesso 2 – *Common Criteria Evaluation Assurance Level*

1 Introduzione

Come anticipato, I Common Criteria (CC) definiscono una scala di 7 livelli di garanzia o di *assurance*. Scopo di una valutazione è ottenere la garanzia che il ToE raggiunga i suoi obiettivi di sicurezza. Con la versione 3 dei CC, sono stati introdotti tre nuovi livelli di assurance denominati *Composed Assurance Packages (CAP)* e che sono CAP-A (il più basso), CAP-B e CAP-C (il più alto).

La garanzia dipende da:

a. il livello di dettaglio dell'analisi del valutatore;

b. il livello dell'attività di test svolta dal fornitore e dal valutatore;

c. il rigore della documentazione prodotta dal fornitore.

Per ogni livello sono definiti i requisiti di garanzia, che individuano azioni a carico del valutatore o dello sviluppatore del ToE oppure requisiti cui deve soddisfare la documentazione di valutazione. I requisiti di garanzia vengono espressi utilizzando un catalogo predefinito di componenti di *assurance* (contenuti nella Parte 3 dei CC).

In altri termini, i livelli EAL sono pacchetti predefiniti (*package*) di componenti di *assurance* che possono essere anche parzialmente modificati attraverso le operazioni:

- ⇨ aumento (aggiunta al pacchetto o al livello di componenti contenute nel catalogo);
- ⇨ estensione (aggiunta al pacchetto o al livello di componenti non contenute nel catalogo).

Nel paragrafo successivo sono riportate le principali caratteristiche per ciascun livello di garanzia previsto.

2 *Evaluation Assurance Level* (EALs)

2.1 EAL 1 *(Functionally Tested)*

Si applica quando si richiede un minimo di garanzia di sicurezza del prodotto ma si ritiene che le minacce alla sicurezza siano poco rilevanti. Prevede una verifica della correttezza delle *Security Function* (SF) senza il coinvolgimento degli sviluppatori. **Minaccia bassa**.

2.2 EAL 2 *(Structurally Tested)*

Si applica quando si richiede un livello di garanzia di sicurezza moderato del prodotto ma il completo sviluppo si ritiene che le minacce alla sicurezza siano poco rilevanti come sopra con attenzione spedizione, test e sviluppo con la cooperazione degli sviluppatori. Ricerca vulnerabilità note. **Minacce medio-basse**.

2.3 EAL 3 (*Methodically Tested & Checked*)

Si applica quando si richiede un moderato livello di sicurezza e richiede un approfondimento del ToE e del suo sviluppo senza prevedere modifiche sostanziali al processo di sviluppo esistente o *re-engineering* del TOE. **Minaccia media.**

2.4 EAL 4 (*Methodically Designed, Tested & Reviewed*)

Si applica quando i sistemi sono sviluppati correttamente anche senza specialisti in sicurezza e si rendono necessarie eventuali piccole modifiche ai processi di sviluppo. La ricerca è basata sull'individuazione delle vulnerabilità più evidenti. **Minaccia medio-alta**.

2.5 EAL 5 (*Semi-formally Designed & Tested*)

Si applica quando si richiede un elevato livello di sicurezza ed il progetto architetturale e di dettaglio del prodotto sono rigorosi e descritti con un linguaggio formale. Richiede l'impiego di progettisti adeguatamente esperti in sicurezza ed un maggior uso di risorse. **Minaccia elevata**.

2.6 EAL 6 *(Semi-formally Verified Designed & Tested)*

Si applica quando si richiede un altissimo livello di sicurezza del prodotto anche con costi elevati. E' necessaria una stretta corrispondenza tra progetto di dettaglio, source coding e schemi HW. **Grave minaccia**.

2.7 EAL 7 (*Formally Verified Designed & Tested*)

Si applica nello sviluppo di sistemi/SW che gestiscono informazioni o funzioni critiche la cui compromissione causerebbe un danno gravissimo. Richiedono che le funzioni di sicurezza ed il progetto architetturale siano descritti con linguaggio formale consistente con il modello formale della Security Policy. Necessita di dimostrazioni formali fin dalla fase progettuale. Dimostrazione di assenza vulnerabilità per accesso ai dati. **Gravissima minaccia**.

3 *Composed Assurance Packages* (CAPs)

3.1 CAP- A *(Structurally composed)*

è applicabile in quelle circostanze ove, per un TOE composto, gli sviluppatori o gli utenti richiedono un livello basso o moderato di sicurezza garantita, indipendentemente in assenza della pronta disponibilità di una completa documentazione di sviluppo.

3.2 CAP- B *(Methodically composed)*

è applicabile in quelle circostanze ove, per un TOE composto, gli sviluppatori o gli utenti richiedono un livello moderato di sicurezza garantita indipendentemente, e una accurata investigazione del TOE composto e del suo sviluppo senza una sostanziale re-ingegnerizzazione.

3.3 CAP- C *(Methodically composed, tested and reviewed)*

è applicabile in quelle circostanze ove, per un TOE composto, gli sviluppatori o gli utenti richiedono un livello da moderato a elevato di sicurezza garantita indipendentemente e sono preparate a ricorrere a costi addizionali di re-ingegnerizzazione specifici per la sicurezza.

Annesso 3 – *Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks*

Nel caso in cui i sistemi ICT in fase di acquisizione debbano essere interfacciati anche con sistemi NATO, sarà necessario che gli stessi seguano le indicazioni riportate nella pubblicazione NATO "*Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks"*.

Questo Annesso riporta quindi i requisiti minimi di difesa informatica per la protezione delle reti collegate alla NATO che gestiscono informazioni con classifica non superiore a "*NATO UNCLASSIFIED*".

Per completezza di informazione, la NATO, similarmente a quanto descritto nelle presenti linee guida, adotta un approccio alla sicurezza CIS e alla difesa informatica basato sul rischio. Pertanto, i requisiti stabiliti in questo documento potranno essere adattati sulla base di una dettagliata valutazione del rischio che riguarda una particolare rete correlata alla NATO.

Nella seguente tabella viene indicato come i singoli requisiti NATO siano coerenti o meno con quelli indicati in Annesso 1. Si tenga conto che alcuni dei requisiti indicati sono legati a processi di gestione che esulano dagli obbiettivi della NAV e rientrano nella definizione di policy da parte dei competenti Enti della Difesa.

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
1. PREVENT			
1.1. Communication & Information Systems (CIS) Protection			
1.1.1. Firewalls to limit the network traffic to a defined and managed set of network ports	**M**		Y
1.1.2. Email gateways which are capable of scanning incoming emails for malicious code, with regularly updated signatures for detecting such code	**M**		N.A.
1.1.3. Software solutions deployed at the endpoint systems to control the installation, spread and execution of malicious code, for which the signatures for detection are updated at least once per day (e.g. antivirus products)	**M**		Y
1.1.4. Measures (dedicated software or through configuration) to limit and control the introduction of external devices to the endpoints and ensure that only authorised devices can be connected	**M**		Y
1.1.5. Firewalls which can apply filtering at the application layer for a more fine-grained control of incoming and outgoing network traffic	R		Y
1.1.6. Measures to limit and control the introduction of devices to the network infrastructure (e.g. by implementing certificate based network access control)	R		Y
1.1.7. Measures to implement web content filtering (e.g. reverse web proxies)	R		Y
1.1.8. Measures to mitigate Denial of Service attacks	R		Y

[34] *(M)andatory or (R)ecommended*.

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
1.1.9. Host Intrusion Prevention software deployed on every endpoint to provide behaviour based detection of malicious activity to better mitigate against known, as well as emerging (including zero-day) attacks	R	While this is quite an effective security control, it should be considered as part of a defence-in-depth strategy, complementing other intrusion detection and prevention controls as reflected in 2.1.5 below	Y
1.2. Data Protection			
1.2.1. Measures to protect against unauthorised disclosure of Personally Identifiable Information (PII) (e.g. mandatory compliance with the General Data Protection Regulation (GDPR) where applicable)	**M**		N.A.
1.2.2. Measures to periodically scan the network, including the endpoints, in order to detect existence of classified information to identify and mitigate spillages and cross-domain violations	**M**	While the frequency is not specified, it is recommended to have such checks at least once a month	Y
1.2.3. Data loss prevention mechanisms to be deployed on endpoints and/or network boundaries	R	Such mechanisms can be very effective in detecting the existence of classified information and preventing its leakage	Y
1.3. Identity & Access Management			
1.3.1. Identification and authentication mechanisms to ensure only authorised users have access to the CIS and the information contained within	**M**		Y
1.3.2. Measures to manage the lifecycle of user, system and application accounts, their creation, use and deletion, applying the least required privilege principle	**M**		Y
1.3.3. Advanced identification and authentication mechanisms that provide a higher level of assurance of ensuring only authorised users have access (i.e. implementing multi-factor authentication)	R		Y
1.4. Asset & Configuration Management			

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
1.4.1. Measures to maintain secure configurations for all hardware and software, by applying security patches in a timely manner	**M**		Y
1.4.2. Measures to restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services	**M**	There are varying levels of detail in which one can implement this important control. The level of restrictions for non-essential functionalities should be determined as a result of risk assessment. The 'hardening' requirements for national unclassified networks could be used as guidance in this regard	Y
1.4.3. Established change management processes to track, review, approve/disapprove, and audit changes to information systems	R		Y
2. DEFEND			
2.1. Detect			
2.1.1. Tools to monitor and log activity within the network	**M**	The level of detail for logging is intentionally not specified. Whatever the level chosen, this control shall not breach any applicable data protection regulations	Y
2.1.2. Tools to monitor and log activity on the endpoints, to include servers	**M**		Y
2.1.3. Standard procedures and processes for the users of the CIS to report any computer or network anomalies they may notice	**M**		Y
2.1.4. A capability (person or a team) that will analyse any reported (by automated tools or by end-users) suspicious activity and decide whether it should be handled as an incident	**M**		Y
2.1.5. Intrusion Detection devices that are regularly updated with signatures to detect malicious activity in the networks	R		Y

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
2.1.6. Specialized network appliances that allow 'full packet capture' functionality, triggered by suspicious network activity, to enable detailed post-incident investigation within an acceptable time delay	R		Y
2.1.7. Specialized software deployed on endpoints, to be triggered on demand, allowing for capturing forensic images of storage and memory devices	R		Y
2.2. Respond			
2.2.1. Documented incident handling and response procedures that include a definition of roles and phases for handling incidents	**M**		N.A.
2.2.2. A capability (designated person or team) to execute the incident handling and response procedures when necessary	**M**		N.A.
2.2.3. A set of contingency plans to be applied in case of incidents	**M**		N.A.
2.2.4. Designated personnel trained in digital forensics procedures, to undertake activities related with the identification, collection and preservation of digital information on security incidents	R		N.A.
2.3. Recover			
2.3.1. Measures and the ability to restore CIS to fully operational status, restoring system and information integrity, and service availability	**M**		Y
2.3.2. Pre-agreed and documented prioritization of which systems are most critical for urgent recovery	R		Y
2.3.3. Pre-defined lists of critical systems that should not be impacted, as well as critical data that should not be lost when executing recovery procedures	R		Y

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
3. ASSESS[35]			
3.1. Manage Risk			
3.1.1. Procedures to continuously assess the risk to organisational operations (including mission, functions, image, or reputation), resulting from potential exploitation of CIS vulnerabilities	**M**	These two mandatory requirements refer to the adoption of a risk management approach to CIS Security and cyber defence as is mandated by NATO Security Policy	Y
3.1.2. Established procedures to assess and accept / mitigate / transfer the identified risks	**M**		Y
3.2. Assess Cyber Defence of Communication and Information Systems			
3.2.1. A capability (designated person or team) to conduct cyber defence assessments on a periodical basis to discover the vulnerabilities and exposures of CIS	**M**	It is recommended to conduct detailed assessments at least once a year. In case the designated person or team has the specialised tools to conduct automated vulnerability assessments, this frequency can be increased in order to quickly identify known vulnerabilities and mitigate them	Y
3.2.2. A capability (person or a team) to support the change management process by conducting security assessments (including scanning for vulnerabilities, detecting bad practices of development, also conducting penetration testing) on any software or hardware that is being evaluated for approval before deployment on the network	R		Y
3.3. Audit			

[35] In linea con l'approccio di autovalutazione raccomandato, le valutazioni o gli *audit* di cui alla presente sezione saranno condotti dalla Nazione che ospita la rete NATO in esame.

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
3.3.1. Periodical security audits and inspections to verify that the cyber defence of the NATO related network is in compliance with the minimum requirements laid out within this document.	**M**	In line with the recommended self-assessment approach, this should be conducted by the the Host Nation of the NATO related network in question. The periodicity of this audit and verification should be aligned with the specific agreement to be captured within the MoU / MoA	N.A.
4. SUSTAIN			
4.1. Educate, Train, and Exercise			
4.1.1. Education and awareness programmes that leverage the use of digital as well as printed media to ensure end-users are made aware of the general threats and vulnerabilities applicable to the CIS they use, in order that they acknowledge their responsibility to maintain the protective security measures in place and adopt 'cyber hygiene' in their way of working	**M**		N.A.
4.1.2. Recurring training for personnel responsible for executing cyber defence activities	**M**	While one can provide dedicated cyber defence training opportunities to personnel, it is also possible to incorporate cyber defence training into the overall training and education programmes (e.g. network and system administrators training)	N.A.
4.1.3. Participate in NATO exercises focusing on cyber defence, giving their personnel the opportunity to witness and act within the context of simulated cyber threat/attack/crisis scenarios	R		N.A.
5. INFORM			
5.1. Collect			

Cyber Defence Requirements	M / R[34]	Remarks	Nav 50 Annex 1 Compliance
5.1.1. Means for the personnel responsible for detecting incidents, to access all security related logs spread throughout the network	**M**		Y
5.1.2. Specialized software and / or appliances (e.g. a Security Incident and Event Management tool and its sub-components for log aggregation) to automatically collect all relevant logs in a central repository to facilitate analysis	R	Since the cyber defence of NATO related networks fall under national responsibility, this centralised collection of security logs should be conducted by the relevant national entities (e.g. national Computer Emergency Response Teams)	Y
5.2. Analyse			
5.2.1. A capability (person or a team) with the required training to conduct post-incident analysis activities, leveraging the information collected from the networks, to conduct root cause analysis and identify user mistakes, unpatched vulnerabilities or potential gaps in preventive mechanisms that may have led to the incident	**M**		Y
5.3. Evaluate			
5.3.1. A capability (person or a team) and the required tools to evaluate security information collected through long periods, to enable correlation and trends analysis, to be complemented with threat information in order to achieve cyberspace situational awareness.	R		Y
5.4. Report & Share			
5.4.1. Standard procedures and processes to share information about cyberattacks and incidents affecting NATO Related Networks, and the information contained therein, with NATO	**M**	The Host Nation responsible for the NATO related network should share, as soon as possible, information about cyberattacks and incidents affecting the network, and the information contained therein, with NATO (e.g. NATO cyber defence POC identified within the MoU / MoA)	N.A.