UNIVERSITÀ DEGLI STUDI DI ROMA

"TOR VERGATA"

FACOLTÀ DI INGEGNERIA

MASTER DI II LIVELLO IN INGEGNERIA E DIRITTO INTERNAZIONALE DELLO SPAZIO NEI SISTEMI DI COMUNICAZIONE, NAVIGAZIONE E SENSING SATELLITARE

"SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI DEL CENTRO NAZIONALE PRS"

Tutor

Ing. Mauro CARDONE

Candidato

CC (AN) Stefano D'AGOSTINO

Anno Accademico 2018/2019

INDICE

ACRONIMI

AgD	Agenzia per l'Italia Digitale
AL	Assurance Level
ANPRS	Autorità Nazionale PRS
ANS	Autorità Nazionale per la Sicurezza
ASI	Agenzia Spaziale Italiana
CAP	Composed Assurance Level
CC	Common Criteria
CED	Centro Elaborazione Dati
CEN	Comitato Europeo di Normazione
Ce.Va.	Centro di Valutazione
CIS	Communication and Information System
CNP	Centro Nazionale PRS
COTS	Commercial off the shelf
CPA	Competent PRS Authority
CS	Commercial Service
DIS	Dipartimento delle Informazioni per la Sicurezza
EAD	Elaborazione Automatica dei Dati
EAL	Evaluation Assurance Level
ESA	European Space Agency
F.A.	Forza Armata
FF.AA.	Forze Armate
GLONASS	GLObal NAvigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSMC	Galileo Security Monitoring Center
ICT	Information and Communications Technology
INFOSEC	Information Security
ISO	International Organization for Standardization
IT	Information Tecnology
ITSEC	Information Technology Security Evaluation Criteria
MEO	Medium Earth Orbit

NATO	North Atlantic Treaty Organization
NDA	National Distribution Agency
NIST	National Institute of Standards and Technology
NOS	Nulla Osta di Segretezza
OCS	Organo Centrale di Sicurezza
OdV	Oggetto della Valutazione
OS	Open Service
PDCA	Plan, Do, Check, Act
PCM	Presidenza del Consiglio dei ministri
PRS	Public Regulated Service
RISS	Requisiti di interconnessione di sicurezza per un sistema
RESS	Requisiti elettronici di sicurezza per un sistema specifico
RSC	Requisiti di sicurezza per comunità di sistemi
RSI	Requisiti iniziali di sicurezza
RSS	Requisiti di sicurezza di un sistema specifico
SAR	Search and Rescue Support Service
SoL	Safety of Life Service
ST	Security Target
TEMPEST	Transient Electro-Magnetic Pulse Emanation Standard
ToE	Target of Evaluation
TS	Traguardo di Sicurezza
U.C.Se.	Ufficio Centrale per la Segretezza
UNI	Union Network International

1. INTRODUZIONE

Il presente lavoro ha lo scopo di descrivere il Sistema di gestione per la sicurezza delle informazioni, per prodotti o sistemi operanti nel settore dell'Informazione e della Comunicazione. Adesso più che mai è tempo di investire in sicurezza informatica. Il pirata informatico è il nuovo nemico da combattere, una minaccia che colpisce tutti senza distinzione, soprattutto aziende e istituzioni, che trattano informazioni sensibili e preziose. Lo scopo di chi pratica questa attività è quello di entrare in possesso di dati riservati, ci possono essere delle motivazioni ideologiche e politiche, ma nella maggior parte dei casi ci sono motivi economici.

Il percorso che verrà seguito per sviluppare un sistema di gestione sicura delle informazioni partirà dalla definizione dei concetti base in materia di sicurezza ICT (*Information and Communications Technology*) e di certificazione.

La base di partenza per raggiungere questo obiettivo è lo standard ITSEC (*Information Technology Security Evaluation Criteria*), che verrà descritto a livello generale nel prossimo capitolo. Nel terzo capitolo, invece, verrà analizzata la normativa vigente in materia e, quindi, le procedure per effettuare la valutazione del rischio di un sistema di Elaborazione Automatica dei Dati (EAD) militare utilizzando lo standard ITSEC, e la conseguente omologazione del sistema.

Quindi, deve essere individuato il livello di sicurezza che si vuole ottenere attraverso la valutazione del rischio. Il livello di sicurezza deve essere raggiunto attraverso opportune azioni di trattamento del rischio. Nel caso in cui questo livello non possa essere raggiunto, le carenze devono essere analizzate e, se il caso, accettate.

La valutazione del rischio deve essere ripetuta nel tempo per verificare se il livello di sicurezza desiderato e quello attuato siano ancora validi. Queste attività di valutazione, azione o accettazione e ripetizione costituiscono la gestione del rischio (*risk management*).

Come già anticipato, l'analisi del rischio verrà condotta utilizzando la normativa nazionale, che definisce gli standard minimi di sicurezza per la protezione delle informazioni classificate, ma nello stesso tempo consente al valutatore di ampliare le misure di sicurezza minime proposte, per ottenere il livello di sicurezza desiderato. Per fare questo si impiegheranno i controlli di sicurezza, ossia le misure utili per garantire la sicurezza delle informazioni, secondo lo standard internazionale della famiglia ISO 27000. Inoltre, negli ultimi anni le minacce cyber sono diventate un vero pericolo per tutti i sistemi informatici pertanto si è reso necessario l'utilizzo di adeguate contromisure per contrastare quest'ulteriore minaccia. A tal proposito si utilizzeranno le misure di sicurezza cibernetica del framework statunitense del NIST.

Nell'ultima parte del documento si fornirà un esempio di applicazione dell'ITSEC per sviluppare l'analisi di rischio del Centro Nazionale Galileo PRS (*Public Regulated Service*), sviluppando la valutazione secondo quanto stabilito dalla normativa nazionale vigente per sistemi sottoposti alla tutela del Segreto di Stato.

Il PRS del sistema di navigazione satellitare Galileo dell'Unione Europea è un servizio di navigazione crittografato per utenti autorizzati governativi e applicazioni sensibili che richiedono alta continuità. Al fine di poter utilizzare nel miglior modo i servizi offerti dal PRS, l'Italia dovrà dotarsi di un Centro Nazionale PRS (CNP).

L'importanza del Centro risiede nella necessità di gestire, a livello nazionale, l'interfaccia con il Sistema Galileo e con la comunità degli utenti dei comparti Sicurezza, Difesa, Gestione Emergenze ed Infrastrutture Critiche per le applicazioni nazionali del Servizio PRS. Per analogia e contiguità con i sistemi miliari e per gli aspetti innovativi che in esso

sono introdotti, si propone per il CNP di seguire l’iter di omologazione previsto per tutti i sistemi EAD militari che trattano informazioni classificate ed eseguire una specifica analisi del rischio.

2. CONSIDERAZIONI SULLA SICUREZZA DELLE INFORMAZIONI

Il termine Sicurezza ICT ha assunto, soprattutto negli ultimi anni, una serie di significati differenti legati principalmente al particolare ambito di riferimento e, conseguentemente, molteplici definizioni e caratterizzazioni. La natura di questo fenomeno è sicuramente da ricercarsi nella vastità del settore al quale essa si riferisce ed alla continua evoluzione tecnologica che porta, spesso, ad una ridefinizione dei concetti fondamentali ai quali essa è legata.

Se si volesse fornire una definizione univoca di quello che la Sicurezza ICT oggi rappresenta probabilmente ci si dovrebbe riferire ad una molteplicità di aspetti tecnici, tecnologici, organizzativi e procedurali volti a proteggere un bene di una organizzazione (*asset*, nella terminologia corrente). Nell'ambito delle Certificazioni per la sicurezza ICT, in accordo a quanto specificato nella serie di standard ISO 27000, il bene essenziale da salvaguardare è rappresentato dall'informazione. Per essa devono essere garantite alcune caratteristiche di base, ovvero:

- Riservatezza (o segretezza), intesa come la possibilità di fruire dell'informazione stessa solo da parte di soggetti autorizzati, impedendone l'accesso sia intenzionale che accidentale per chiunque altro.
- Integrità, intesa come la protezione dell'informazione da alterazioni non autorizzate, siano esse intenzionali o accidentali.
- Disponibilità, intesa come la possibilità di fruire delle informazioni, da parte di chi ne abbia accesso, ogniqualvolta sia necessario, anche in presenza di fenomeni ostativi intenzionali o accidentali.
- Autenticazione, intesa come il processo di riconoscimento delle credenziali dell'utente in modo di assicurarsi dell'identità di chi invia messaggi o esegue operazioni.

Con queste premesse, la definizione del termine Sicurezza nello specifico ambito del settore dell'informazione è esprimibile come:

"la sicurezza nel settore della tecnologia dell'informazione consiste nella protezione della riservatezza, integrità, disponibilità delle informazioni mediante il contrasto delle minacce originate dall'uomo o dall'ambiente, al fine di impedire, a coloro che non siano stati autorizzati, l'accesso, l'utilizzo, la divulgazione, la modifica delle informazioni stesse, e di garantirne l'accesso e l'utilizzo a coloro che siano stati autorizzati." [1]

Sul piano reale, tuttavia, questa definizione si scontra con numerose difficoltà oggettive che rendono impossibile garantire con certezza assoluta le caratteristiche sopra descritte, prime fra tutte quelle legate agli aspetti economici della realizzazione della sicurezza ICT.

Appare chiara, allora, la necessità di individuare dei compromessi, accettati in modo consapevole ed esplicito da parte dei soggetti interessati, che tengano conto da una parte di queste limitazioni e dall'altra dei livelli di garanzia che si vogliono raggiungere circa la sicurezza ICT all'interno di ogni singola realtà aziendale o organizzativa.

Questi compromessi possono essere individuati solo adottando un processo organico e strutturato di analisi e realizzazione della sicurezza, accettando che questa non consiste nella semplice adozione di un prodotto o di regole generalizzabili, ma che come processo la sua implementazione varia a seconda della realtà a cui si riferisce.

[1] Vds. Organismo di Certificazione di Sicurezza (OCSi), *Linee guida provvisorie parte 1 (LGP1) – Descrizione Generale dello Schema Nazionale,* dicembre 2004, pag. 9.

Alla luce di queste considerazioni, implementare la sicurezza ICT vuol dire:

- Individuare le risorse da proteggere (*asset*)
- Individuare le minacce che gravano sulle risorse
- Individuare le vulnerabilità proprie delle risorse
- Definire un livello accettabile di rischio
- Determinare le specifiche di sicurezza

A questo processo, che è stato standardizzato in varie normative internazionali, tra cui la ISO 27001, si dà generalmente il nome di “Analisi dei rischi”.

Senza scendere ulteriormente nel dettaglio di questi concetti, occorre a questo punto specificare quale sia il ruolo delle certificazioni di sicurezza: la valutazione, e quindi la certificazione, consente di verificare quanto un processo o un sistema sia capace di rispettare determinati requisiti di sicurezza, attraverso l’utilizzo di metodologie che definiscono criteri standard per la valutazione di tali requisiti.

Attraverso l’Analisi dei rischi, allora, è possibile definire in quali ambiti di una specifica organizzazione potrebbe essere richiesta una certificazione di sicurezza condotta da una terza parte indipendente.

È da notare, però, che la certificazione, pur rappresentando un notevole valore aggiunto, non riesce ad elevare il livello di sicurezza se non è accompagnata dalla costante e puntuale applicazione delle normative e prescrizioni di sicurezza. In altre parole, la certificazione è da considerarsi in questo senso come condizione necessaria ma non sufficiente. È altrettanto importante notare come l’attenzione agli aspetti di sicurezza deve essere considerata come principio fondamentale sin dalle fasi iniziali di sviluppo di un qualsiasi sistema, prodotto o processo che voglia definirsi sicuro, e non solo come rimedio occasionale a problematiche emerse o vulnerabilità.

a. Descrizione dello standard ITSEC

Lo standard ITSEC, acronimo di *Information Technology Security Evaluation Criteria* è uno dei primi standard sviluppati espressamente per la valutazione (e certificazione) di sistemi e prodotti nell’ambito della tecnologia dell’informazione e della comunicazione.

Sviluppato in modo congiunto da Francia, Germania, Gran Bretagna e Olanda, è stato pubblicato in versione definitiva nel giugno del 1991, raccogliendo da subito il pieno consenso della Commissione della Comunità Europea.

Nel corso degli anni lo standard, già approvato da organismi istituzionali, è stato largamente impiegato e sperimentato; per questo motivo ITSEC è considerato tutt’oggi una dei principali criteri attraverso il quale formulare un giudizio in materia di sicurezza e qualità di un sistema o prodotto informatico.

ITSEC è da molti considerato il progenitore dei moderni criteri di valutazione per prodotti e sistemi IT; in effetti questo standard è stato il primo ad introdurre dei concetti di base, poi largamente riutilizzati, tra i quali:

- la considerazione per le misure di sicurezza non solo di carattere tecnico, ma anche organizzativo, ambientale (intendendo le caratteristiche di sicurezza dell’ambiente in cui il prodotto/sistema deve operare) e fisico;
- la possibilità di valutare gli aspetti di sicurezza di prodotti hardware, software o firmware, indistintamente;
- l’identificazione univoca del promotore della valutazione;

- l’identificazione di enti preposti alla valutazione, formalmente accreditati per condurre le attività (nello Schema Nazionale sono i Centri di Valutazione, o Ce.Va.);
- l’identificazione univoca dell’oggetto della valutazione (ToE, *Target of Evaluation*, o in italiano OdV, Oggetto della Valutazione);
- la definizione del Traguardo di Sicurezza, TS (o in inglese *Security Target*, ST);
- la presenza di livelli di severità della valutazione – flessibili – (*Assurance Leve*l, AL).

Tra questi riveste un ruolo molto importante il traguardo di sicurezza, soprattutto per la rilevanza che questo attribuisce non solo allo specifico oggetto della valutazione, ma anche all’ambiente per cui questo è progettato (come per esempio nelle reti di calcolatori).

Per iniziare a descrivere il processo logico di valutazione in ITSEC, allora, possiamo partire proprio dal TS. Come vedremo anche in seguito, quando andremo ad analizzare la metodologia adottata nella normativa nazionale per l’analisi del rischio di sistemi informatici militari, per definire un Traguardo di Sicurezza secondo lo standard è necessario:

- definire gli obiettivi di sicurezza, a partire dai requisiti operativi del prodotto/sistema e dell’ambiente di utilizzo in termini di riservatezza, integrità e disponibilità;
- individuare un insieme di minacce a cui il prodotto/sistema può essere esposto;
- definire le funzioni di sicurezza che il prodotto/sistema deve prevedere e offrire;
- individuare gli altri possibili meccanismi di sicurezza presenti e/o utilizzati dal prodotto/sistema.

A fronte di questi ragionamenti e di questa “collezione” di informazioni sull’OdV, è possibile redigere un TS, basandosi sul modello offerto dallo schema stesso, ovvero un documento composto da quattro parti fondamentali:

- la politica di sicurezza del sistema o la descrizione del prodotto;
- la specifica delle funzioni di sicurezza;
- il livello minimo dichiarato di robustezza dei meccanismi di sicurezza;
- Il livello di valutazione desiderato (*Assurance Level*, o AL).

La valutazione viene completata fornendo il livello di *Assurance* associato all’OdV, secondo una scala che va da E0, ovvero nessuna fiducia, a E6, ovvero fiducia massima. Per l’individuazione di questo valore si passano al vaglio una lunga serie di fattori, ad esempio l’analisi della fase di sviluppo (e quindi dei requisiti), il progetto architetturale, il progetto di dettaglio e la realizzazione. È prevista anche la conduzione di prove indipendenti (ai livelli più alti) per confermare ed ampliare con i relativi risultati la documentazione fornita.

Come detto la definizione dell’ambiente è considerato molto importante dai criteri, anche di quello di sviluppo; per questo secondo lo standard bisogna considerare tre aspetti principali: il controllo di configurazione, i linguaggi di programmazione utilizzati (e i rispettivi compilatori) e la sicurezza dell’ambiente di sviluppo stesso.

Si precisa che oltre allo standard ITSEC, un altro standard, impiegato per la valutazione e certificazione di sistemi nell’ambito della tecnologia dell’informazione e della comunicazione, è quello dei *Common Criteria* secondo la ISO 15408, che non viene trattato in questo elaborato, ma è stato brevemente descritto in Allegato A.

3. PROCEDURA PER L'OMOLOGAZIONE DI SISTEMI EAD MILITARI E RELATIVI STANDARD DI SICUREZZA

La normativa nazionale PCM-ANS/TI-001 definisce le procedure per l'omologazione di sistemi/reti EAD militari ai fini della sicurezza nel campo delle tecnologie dell'informazione e fornisce le linee guida generali per l'elaborazione dei requisiti di sicurezza.

I requisiti di sicurezza vengono formulati nella prima fase di un progetto e sono sviluppati ed aggiornati durante lo sviluppo dello stesso, svolgendo diversi ruoli nelle differenti fasi attraverso le quali si perviene alla realizzazione ed all'operatività completa di un prodotto, sistema o rete EAD.

I requisiti di sicurezza sono richiesti come parte integrante della documentazione generale di un progetto. Tale documentazione viene sottoposta all'approvazione dell'Organo Centrale di Sicurezza (OCS).

a. Requisiti di sicurezza e procedura per l'omologazione di sistemi EAD

In relazione all'oggetto della valutazione vengono individuati i tipi di requisiti di sicurezza che sono richiesti nelle varie fasi del processo di omologazione. In particolare, si individuano i requisiti di seguito elencati:

- Requisiti iniziali di sicurezza (RSI): in tale documento si descrive genericamente il sistema in termini di ubicazione, classifica dei dati da gestire, quantità dei dati da gestire, configurazione hardware e software e collegamenti esterni. Inoltre, sono richieste indicazioni sulla categoria TEMPEST[2] dell'hardware e sulle funzioni di sicurezza del software.
- Requisiti di sicurezza di un sistema specifico (RSS): in tale documento, oltre a contenere tutte le informazioni descritte nel RSI, illustra nel dettaglio le politiche di sicurezza che hanno portato all'individuazione della categoria TEMPEST dell'hardware e le funzioni di sicurezza del software, descrive le modalità operative del sistema e individua le minacce[3], vulnerabilità[4] e contromisure.
- Requisiti elettronici di sicurezza per un sistema specifico (RESS): in tale documento vengono dettagliate le funzioni di sicurezza non pertinenti alle discipline di sicurezza fisica, del personale e procedurale che il fornitore deve implementare nel sistema per soddisfare i livelli di funzionalità richiesti dal committente. In particolare, deve contenere l'architettura funzionale del sistema, le soluzioni tecniche adottate e una dettagliata descrizione del sistema in termini di controllo accessi, integrità, disponibilità e sicurezza delle periferiche.
- Requisiti di interconnessione di sicurezza per un sistema (RISS): tale documento viene redatto solo quando sono presenti almeno due sistemi EAD interconnessi. La struttura di tale documento è analoga a quella dell'RSS ma contiene anche il tipo di collegamento, la natura fisica dell'interconnessione e l'estensione fisica della rete.
- Requisiti di sicurezza per comunità di sistemi (RSC): tale documento viene redatto solo se è presente una comunità di sistemi, cioè se un insieme di sistemi EAD

[2] Transient Electro-Magnetic Pulse Emanation Standard – Termine utilizzato per indicare il fenomeno delle emissioni compromettenti non intenzionali che interessa apparati elettronici ed elettromeccanici che elaborano segnali. La categoria TEMPEST è la corrispondenza tra le caratteristiche intrinseche dell'apparato/sistema e i requisiti riportati nella direttiva PCM-ANS/TI-004.

[3] Possibilità di compromissione accidentale o deliberata della sicurezza di un sistema EAD, consistente nella perdita di riservatezza, nella modifica, nella distruzione dei dati o interruzione del servizio.

[4] Debolezza che può dar luogo o facilitare l'attuazione di una minaccia. Ad ogni minaccia corrisponde una o più vulnerabilità; ogni vulnerabilità può essere contrastata con una o più contromisure.

sono connessi tra di loro e alcuni dei quali possono anche non trattare informazioni classificate. Il documento ha lo scopo di delineare i livelli di sicurezza comuni ai quali tutti i sistemi interconnessi devono ottemperare.

Si riporta, in Figura 1, lo schema della procedura nazionale per l'omologazione dei sistemi EAD, in cui si evidenzia l'organo competente responsabile della compilazione del documento e l'organo che deve approvare o concordare il documento al fine di ottenere l'omologazione finale del sistema.

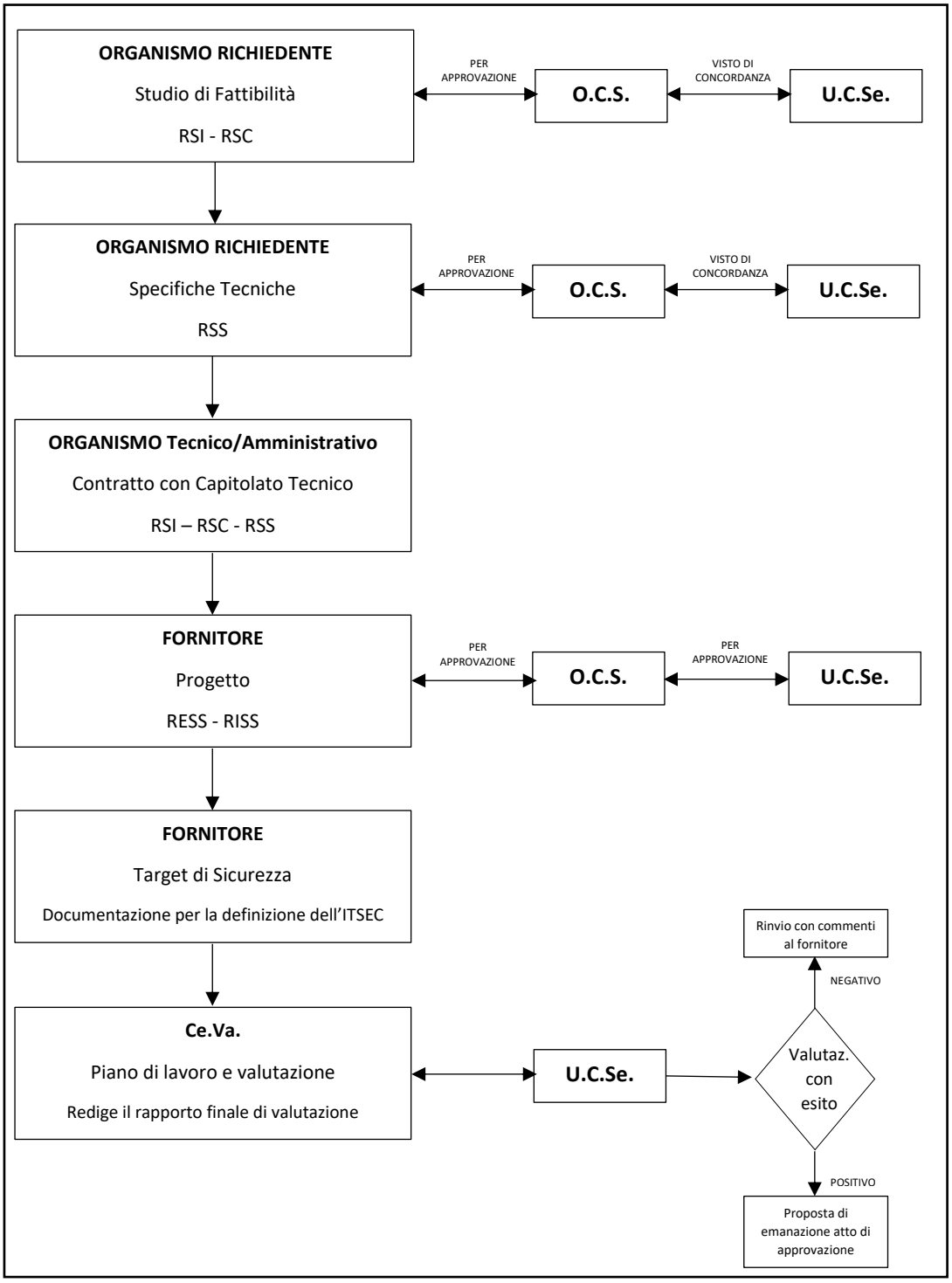

Figura 1 Schema della procedura nazionale per l'omologazione di sistemi/reti EAD

b. Standard di sicurezza per sistemi/reti EAD militari

Nel presente paragrafo vengono definiti gli standard minimi di Sicurezza, riportati nella normativa nazionale PCM-ANS/TI-002, per la protezione nel campo delle tecnologie dell'informazione di sistemi/reti EAD destinati a gestire dati coperti dal Segreto di Stato o di vietata divulgazione.

La politica di sicurezza da adottare è quella per cui, per determinare le appropriate misure di sicurezza di un sistema informatico, è necessaria una analisi del rischio che consiste nella identificazione della minaccia e del grado di vulnerabilità del sistema, fornendo parametri sui meccanismi di protezione da adottare. Si precisa che le misure di sicurezza descritte in seguito rappresentano il minimo necessario per garantire la riservatezza, l'integrità e la disponibilità delle informazioni.

La gestione del rischio, nell'ambito della sicurezza EAD, consiste nel realizzare un livello minimo di protezione delle informazioni tramite l'implementazione di opportune misure di sicurezza.

Gestire i rischi concernenti la sicurezza nelle tecnologie delle informazioni (INFOSEC), significa individuare cosa è sottoposto a rischio, l'estensione di quest'ultimo e le conseguenti misure da adottare.

Il rischio può essere ridotto, eliminato, evitato e accettato. L'obiettivo della metodologia utilizzata per l'analisi del rischio è quello di fornire degli standard applicativi in grado di ridurre in maniera accettabile il rischio. La riduzione del rischio può essere ottenuta implementando sull'architettura del sistema opportune componenti di sicurezza fisica, procedurale, del personale e tecnica.

La gestione del rischio coinvolge la pianificazione, l'organizzazione, la direzione ed il controllo delle risorse, al fine di assicurare che il rischio rimanga entro limiti accettabili in base al rapporto costo/efficacia. In campo INFOSEC, la gestione del rischio presenta alcune particolari difficoltà che nascono dalla natura dinamica dei fattori di rischio e dalla rapida evoluzione della tecnologia. Un errore nel non considerare adeguatamente e tempestivamente i fattori di rischio si può tradurre nell'adozione di misure di sicurezza non efficaci o inutilmente costose. Pertanto, la gestione del rischio INFOSEC deve essere considerata come parte integrante dell'intero ciclo di vita del sistema.

c. Analisi del Rischio

Per ogni sistema EAD che tratta informazioni classificate è necessario redigere un insieme di norme e procedure che disciplinano le modalità di gestione, distribuzione e protezione delle informazioni sensibili. Esse costituiscono la cosiddetta "politica di sicurezza" la quale fornisce la base per l'individuazione degli obiettivi di sicurezza del sistema, tramite l'effettuazione dell'analisi del rischio.

L'analisi del rischio, condotta secondo lo schema metodologico rappresentato in Figura 2, è la disciplina che si incarica di:

- individuare le risorse da proteggere;
- individuare i tipi e i livelli delle minacce che insistono sul sistema;
- individuare le vulnerabilità intrinseche del sistema;
- calcolare la vulnerabilità iniziale del sistema;
- individuare le misure di sicurezza da adottare.

L'individuazione delle risorse da proteggere

Nel contesto dell'analisi del rischio, il primo passo fondamentale è l'esatta individuazione dei componenti del sistema da proteggere. I componenti così

determinati individuano l'ambiente operativo e successivamente sarà possibile individuare le minacce che vi insistono. Occorre considerare il sistema nel suo insieme, senza tralasciare alcun componente, quindi sia la struttura che ospita il sistema che il personale che vi opera.

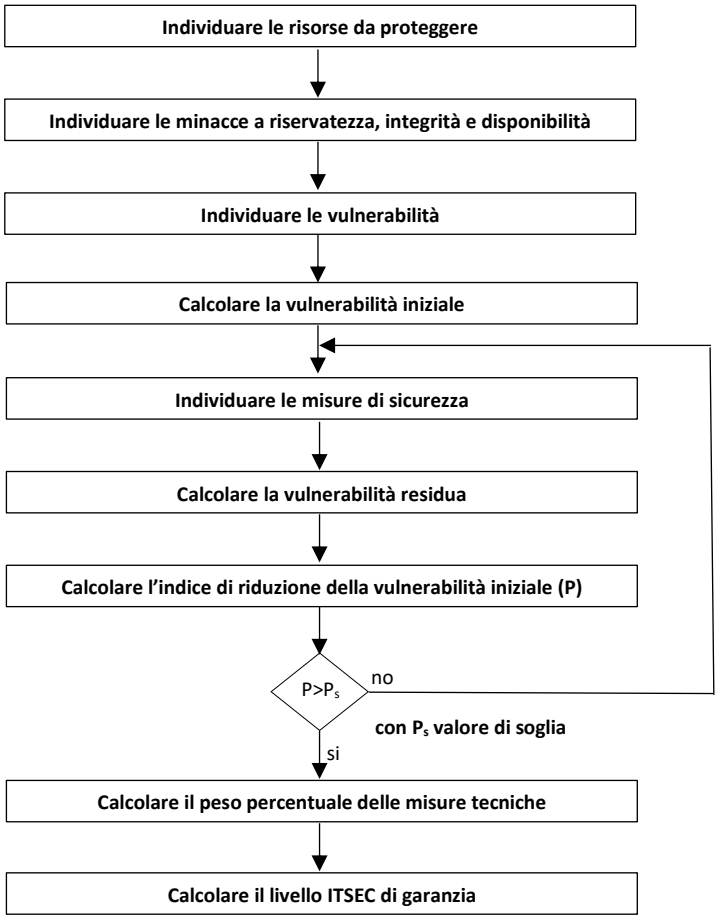

Figura 2 Schema metodologico per il calcolo del livello di garanzia

L'individuazione della minaccia

Generalmente, una minaccia può essere definita come la possibilità di compromissione accidentale o deliberata della sicurezza di un sistema o rete EAD, consistente nella perdita di riservatezza delle informazioni, nella modifica/distruzione dei dati o nella interruzione del servizio.

L'identificazione della minaccia è una parte essenziale dell'analisi del rischio. Le origini delle minacce possono essere descritte[5], genericamente, come segue:

- Minaccia interna: proveniente da ogni "soggetto" che abbia accesso legittimo al sistema/rete EAD, che possono causare danno non intenzionale per uso scorretto, incidenti, errore umano, oppure danno intenzionale, per disonestà o malcontento.
- Minaccia esterna: proveniente da ogni "soggetto" esterno al sintema/rete EAD, che possa causare danno non intenzionale o intenzionale, tramite accesso logico non autorizzato, intercettazione, interferenza/disturbo od introduzione abusiva di software dannoso.
- Minaccia fisica/ambientale: che coinvolge l'integrità fisica del sistema (es. furto, incendio, allagamento sabotaggio).

[5] Vds. Presidenza del Consiglio dei ministri – Autorità Nazionale per la Sicurezza, PCM-ANS/TI-002 Standard di sicurezza per sistemi/reti EAD militari, 1995.

Alla valutazione della minaccia contribuiscono i seguenti elementi:

- le capacità dei potenziali aggressori (servizi di intelligence ostili, gruppi sovversivi, terroristi, criminali, hackers e mezzi d'informazione) supportate dal progresso tecnologico;
- il grado di esposizione a cui i sistemi sono soggetti (determinati dalla loro collocazione geografica e/o collegamenti);
- il potenziale interesse del contenuto (espresso in termini di classifica, tipologia e quantità dei dati).

Le capacità offensive dei potenziali aggressori variano in funzione delle motivazioni, risorse ed esperienze dei potenziali aggressori e sono definite sulla base della esposizione dei sistemi a paesi con servizi di intelligence ostili, a paesi i quali seppure non esplicitamente ostili sono decisamente non amichevoli, a paesi amici o neutrali. Quindi, va evidenziato che la minaccia ai sistemi connessi in rete varia in relazione alla tipologia delle differenti aree geografiche in cui la rete si estende. Inoltre, vanno considerati altri potenziali aggressori, quali, ad esempio, terroristi e membri inaffidabili del personale interno/esterno.

Se si considera la sensibilità del contenuto o l'appetibilità dei dati, costituiscono un obiettivo di interesse per i potenziali aggressori anche le informazioni di intelligence, di sicurezza, militari, tecnologiche, politiche, personali ed economiche. Esempi di obiettivi sensibili, infatti, sono:

- Uffici NATO o della Unione Europea;
- Uffici di Sicurezza e di Intelligence;
- Ministeri, incluse le FF.AA.;
- Industrie abilitate in ambito governativo;
- Centri EAD di FA, inclusi sistemi su unità mobili.

In Allegato B si ripota il catalogo delle minacce a sistemi/reti EAD, secondo la normativa PCM-ANS/TI-002.

L'individuazione delle vulnerabilità

Una vulnerabilità di un sistema informativo può essere definita come una debolezza o mancanza di controlli che può dar luogo o agevolare l'attuazione di una minaccia, con conseguente compromissione, danneggiamento e/o impossibilità dell'accesso alle informazioni di interesse.

In Allegato C si ripota il catalogo delle vulnerabilità a sistemi/reti EAD, secondo la normativa PCM-ANS/TI-002.

d. Misure di sicurezza

La scelta delle misure di sicurezza dipende da diversi fattori, che tengono conto della situazione ambientale preesistente:

- il teatro operativo;
- la sensibilità delle informazioni da proteggere;
- il livello di abilitazione degli utenti;
- la necessità di conoscere degli utenti.

In generale, un sistema EAD può essere classificato, a seconda del livello di sensibilità delle informazioni trattate, del livello di abilitazione e della "necessità di conoscere" degli utenti, secondo una delle seguenti modalità operative:

- *Dedicato*: modalità operativa in cui tutti i soggetti che accedono al sistema EAD sono abilitati al massimo livello delle informazioni memorizzate, elaborate o trasmesse dal sistema stesso ed hanno la stessa necessità di conoscere per tutte

le informazioni memorizzate, elaborate o trasmesse dal sistema. La comune necessità di conoscere indica che non è necessario, per le caratteristiche di sicurezza del sistema, fornire la separazione delle informazioni nel sistema stesso; inoltre altre caratteristiche di sicurezza (per esempio fisica e procedurale) dovranno essere conformi ai requisiti per il più alto livello di classifica delle informazioni memorizzate, elaborate o trasmesse dal sistema.

- *Alla più alta classifica*: modalità operativa in cui tutti i soggetti che accedono al sistema EAD sono abilitati al massimo livello delle informazioni memorizzate, elaborate o trasmesse dal sistema, ma non tutti hanno una comune necessità di conoscere tali informazioni. Tale modalità operativa permette, contemporaneamente, la memorizzazione, l'elaborazione e la trasmissione di informazioni con differente livello di classifica. La mancanza della comune necessità di conoscere indica l'esigenza, per le caratteristiche di sicurezza del sistema, di fornire accessi selettivi e quindi la separazione delle informazioni presenti nel sistema. Altre caratteristiche di sicurezza (per esempio fisica e procedurale) dovranno essere conformi ai requisiti per il più alto livello di classifica delle informazioni del sistema. Inoltre, tutte le informazioni memorizzate, elaborate o comunque disponibili per il sistema, insieme ad ogni output generato, saranno protette alla stregua delle informazioni di massimo livello memorizzate, elaborate o trasmesse, fino a quando non sarà determinato altrimenti; a meno che non sia stato raggiunto un accettabile livello di affidabilità nella capacità del sistema EAD di identificare le informazioni ed apporre la relativa classifica in modo corretto.
- *Multilivello*: modalità operativa in cui non tutti i soggetti che accedono al sistema EAD sono abilitati al massimo livello di classifica delle informazioni memorizzate, elaborate o trasmesse dal sistema, e non tutti gli individui che accedono al sistema hanno una comune necessità di conoscere. Tale modalità operativa permette, contemporaneamente, la memorizzazione e la trasmissione di informazioni di differente livello di classifica. La presenza di individui non autorizzati al massimo livello, associata alla mancanza di una comune necessità di conoscere, indica l'esistenza di particolari requisiti per gli aspetti di sicurezza del sistema, che forniscono l'accesso selettivo e la separazione delle informazioni del sistema EAD. Per il sistema EAD, altre caratteristiche di sicurezza (per esempio fisica e procedurale) dovranno essere conformi ai requisiti per le informazioni al massimo livello di classifica memorizzate, elaborate o trasmesse.

Occorre considerare che i sistemi militari EAD installati su specifiche piattaforme beneficiano, di massima, di una particolare situazione operativa per cui:

- tutti gli addetti e gli utenti che hanno accesso (fisico e logico) sono abilitati al massimo livello di classifica delle informazioni trattate dal sistema;
- sono già in atto speciali misure di sicurezza fisica / ambientale e procedurale tali da assicurare un rigoroso controllo dell'accesso fisico per il personale che lavora nelle "piattaforme" in esame e per il personale che non è addetto al sistema EAD.

Da ciò deriva che l'implementazione della modalità multilivello risulta raramente applicabile. Infatti, nella politica di sicurezza devono essere rispettate le due seguenti condizioni:

- gli sviluppatori e manutentori del sistema siano forniti di NOS ed autorizzazioni sufficienti, cosi da ritenere improbabile l'introduzione di logica illegittima (elaborazione o inserimento di programmi pregiudizievoli per la sicurezza);
- siano previsti dispositivi (hardware/software) che provvedano al controllo della configurazione del sistema, al fine di evitare l'introduzione di logica illegittima prima e durante le operazioni del sistema.

Le misure di sicurezza applicabili ad un sistema/rete EAD possono essere fondamentalmente di 4 tipi:

- **Misure fisiche**: consistono nell'applicazione di una serie di barriere per la protezione delle aree riservate EAD e dei terminali remoti e/o stazioni di lavoro (tale controllo si risolve nella limitazione dell'accesso fisico, per impedire l'ingresso a persone non autorizzate e consentirlo solo a coloro i quali devono operare per precise necessità) e nella prevenzione dalle conseguenze di disastri naturali, accidentali o dolosi, quali fumo, incendio, inondazioni, ecc.
- **Misure personali**: la sicurezza relativa al personale richiede che le persone assegnate ad aree riservate EAD debbano avere una abilitazione di sicurezza al più alto livello di classifica delle informazioni cui possono accedere. Ciò si applica anche al personale assegnato ad aree riservate di terminali e/o workstation remote. È richiesto che i soggetti che abbiano accesso temporaneo alle aree riservate EAD vengano adeguatamente scortati e controllati. Tutto il personale addetto al sistema / rete EAD dovrà svolgere un adeguato programma di istruzione, per la sensibilizzazione su tutti i rischi per la sicurezza connessi con l'elaborazione automatica dei dati. La ripartizione dei compiti e delle responsabilità dovrà essere tale che una stessa persona non abbia la completa conoscenza o il totale controllo delle "chiavi di sicurezza" dell'intero sistema o del software. Dovrà essere di massima definito il numero minimo di componenti del personale operativo addetto alle aree EAD classificate.
- **Misure procedurali**: riguardano la sicurezza relativa alla fase operativa di elaborazione dei dati classificati. Tali misure vanno inserite nel "Regolamento interno di sicurezza EAD", comprendente tra l'altro istruzioni su responsabilità e controlli, sicurezza fisica (descrizione infrastruttura, protezioni, modalità di controllo per l'accesso fisico), sicurezza personale (elenco persone abilitate e modalità di istruzione INFOSEC), sicurezza tecnica (descrizione delle procedure relative alla gestione della sicurezza), procedure di backup e piano di emergenza, procedure di gestione di terminali remoti.
- **Misure Tecniche (Hardware e Software)**: qualunque accorgimento tecnico realizzato specificamente sul sistema / rete EAD da proteggere, in base alle caratteristiche tecniche dello stesso. Tali misure sono quindi legate direttamente al tipo di apparato e sistema che viene utilizzato.

La sicurezza globale di un sistema / rete EAD non potrà mai derivare dalla implementazione di un unico tipo di misure di sicurezza, in quanto nessuna di queste potrà mai fornire la garanzia di assoluta efficacia, a causa della complessità ed articolazione del sistema stesso. Nella selezione delle misure da adottare occorrerà quindi scegliere una opportuna combinazione dei diversi tipi di misure, individuando quali di esse possano colmare le lacune intrinseche delle altre.

Lo schema metodologico, descritto in Figura 2, introduce l'indice *"P"* che da una misura della riduzione della vulnerabilità iniziale sulla base delle misure di sicurezza individuate. Se *P* risulta maggiore del valore di soglia P_S=30 si ha una ragionevole certezza che le misure di sicurezza riducono in maniera efficace la vulnerabilità iniziale. Se *P* risulta minore o uguale a P_S=30 occorre riconsiderare le misure di sicurezza individuate precedentemente fino al raggiungimento di un *P* accettabile.

e. Modalità di calcolo del livello di garanzia

Lo schema metodologico permette di derivare, a fronte del calcolo del peso percentuale delle misure tecniche implementate, il livello di garanzia delle funzionalità richieste, riconducibile ai criteri ITSEC. Nell'applicazione pratica della metodologia occorre tenere presente che:

- ogni minaccia si manifesterà con frequenza indeterminata;
- la frequenza del verificarsi di una minaccia non può essere alterata; l'influenza su una minaccia è una o più contromisure;
- le contromisure riducono il livello di vulnerabilità relativo ad una minaccia, e non la frequenza del suo verificarsi;
- tutte le vulnerabilità hanno rispettive contromisure;
- la vulnerabilità decresce al crescere delle contromisure;
- con l'applicazione di contromisure si può ottenere una riduzione della vulnerabilità sino a valori accettabili.

Calcolo del livello di minaccia
La minaccia a un sistema/rete EAD è funzione dei seguenti parametri:

- la capacità offensiva C_{OFF}
- il grado di esposizione (Teatro Operativo) G_{ESP}
- l'appetibilità dei dati A_{DAT}

La **capacità offensiva** può essere quantificata secondo i seguenti parametri:

LIVELLO TECNICO DELL'AGGRESSORE	C_{OFF}
Basso	1
Medio	2
Alto	3

Il **grado di esposizione** prevede i seguenti teatri operativi:

GRADO DI ESPOSIZIONE	G_{ESP}
Sistema situato in paese amico	1
Sistema operante in paese neutrale	2
Sistema operante in paese nemico	3

L'**appetibilità dei dati** è suddivisa per ambiente che tratta le informazioni:

APPETIBILITA DEI DATI	A_{DAT}
Servizi di Intelligence	1
Ambasciate e Consolati	2
Installazioni militari	3
Industrie civili	4

Il livello della minaccia L_M è dato dalla seguente formula:

$$L_M = C_{OFF} * G_{ESP} * A_{DAT}$$

Pertanto, il livello della minaccia L_M è compreso tra 1 e 36.

Calcolo della vulnerabilità iniziale
Il calcolo della vulnerabilità iniziale (in assenza di contromisure), per ogni singola minaccia è:

$$V_I = \sum_{i=1}^{n} V_I$$

dove V_I assume il peso rappresentato dal numero minimo di contromisure da adottare per ridurre l'incidenza della vulnerabilità a valori accettabili; con l'indice *i* si intendono tutte le vulnerabilità associate alla minaccia in esame. Tale sommatoria verrà effettuata per ciascuna minaccia. L'assegnazione dei pesi equivalente al numero minimo di contromisure è una operazione soggettiva che risente dell'esperienza, in ambito operativo e di sicurezza, di chi elenca le possibili vulnerabilità e propone le relative misure di sicurezza.

Calcolo della vulnerabilità residua
Associando ad ogni contromisura un peso pari a 5, il valore delle contromisure sarà dato da:

$$C_M = n * 5$$

dove *n* è il numero delle contromisure adottate (che comprenderanno quelle procedurali, fisiche, tecniche, personali ed eventuali altre classi adottate).

Poiché la complessità e la sensibilità di un sistema dipende anche da parametri quali la classifica delle informazioni, la quantità delle informazioni trattate, il numero degli utenti che operano sul sistema e le modalità operative dello stesso, è opportuno introdurre un fattore correttivo "*β*" che tenga conto dei diversi valori assunti dai suddetti parametri indicati con:

- Classifica delle informazioni trattate — L_{CLA}
- Modalità operativa del sistema — M_{OPE}
- Numero utenti del sistema — N_{UTE}
- Quantità delle informazioni elaborate — Q_{INF}

Le variabili assumono i seguenti valori:

LIVELLO CLASSIFICA	L_{CLA}
Riservato	1
Riservatissimo	2
Segreto	3
Segretissimo	4

MODALITA OPERATIVA DEL SISTEMA	M_{OPE}
Dedicato	1
Alla più alta classifica	2
Multilivello	3

N_{UTE} è il numero effettivo degli utenti che hanno accesso al sistema.

Q_{INF} è la stima, espressa in Mb, della quantità di informazioni classificate trattate dal sistema.

Il fattore correttivo *β* sarà così calcolato:

$$\beta = (M_{OPE} * \log N_{UTE}) * (L_{CLA} * \log Q_{INF})$$

dove $\log N_{UTE}$ è il fattore di complessità del sistema, mentre $\log Q_{INF}$ è il fattore di sensibilità delle informazioni trattate.

Partendo dal livello della minaccia L_M, dal livello della vulnerabilità iniziale V_I, dal valore delle contromisure C_M e dal Fattore di Correzione *β* si ottiene la vulnerabilità residua V_R:

$$V_R = V_I - \frac{C_M}{\beta + L_M}$$

questa relazione indica che la vulnerabilità residua è uguale a quella iniziale, diminuita di un valore dipendente dalle contromisure scelte. L'applicazione delle misure di sicurezza, infatti, riduce la vulnerabilità iniziale.

La quantità $\beta+L_M$ riduce l'efficacia delle contromisure C_M. Infatti, al crescere di $\beta+L_M$, il rapporto decresce e quindi il peso delle contromisure viene diminuito.

Calcolo dell'indice "*P*" di riduzione della vulnerabilità iniziale
Una volta calcolati i valori di vulnerabilità iniziale (V_I) e i valori di vulnerabilità residua (V_R), si procederà al calcolo del valore *P.* L'indice *P* considera tutti i valori di

vulnerabilità relativi alle minacce possibili per il sistema, esso infatti è costruito sottraendo tutte le vulnerabilità residue da quelle iniziali, rapportando il risultato al valore di vulnerabilità iniziale:

$$P = \frac{V_I - V_R}{V_I} * 100$$

P fornisce il valore percentuale che indica la variazione della vulnerabilità iniziale del sistema una volta applicate le contromisure. Se il valore di *P* è maggiore della soglia P_s=30, si prosegue nel calcolo del peso percentuale delle misure tecniche implementate.

Calcolo del peso percentuale delle misure tecniche implementate

Indicando con n_T il numero di misure tecniche adottate e con n il numero complessivo di contromisure si ha:

$$M_T = \frac{n_T}{n} * 100$$

che indica, percentualmente, la quantità di misure tecniche rispetto al totale delle misure adottate nell'analisi del rischio.

Livello di garanzia

Una volta calcolato il valore di M_T, mediante l'utilizzo della Tabella 1 si deriva il livello di garanzia (conforme ai requisiti ITSEC):

M_T [%]	Livello di garanzia (E)
$M_T \leq 10$	E0
$10 < M_T \leq 30$	E1
$30 < M_T \leq 60$	E2
$60 < M_T \leq 75$	E3
$75 < M_T \leq 90$	E4
$90 < M_T \leq 95$	E5
$95 < M_T \leq 100$	E6

Tabella 1 Tabella del livello di garanzia

4. SISTEMA DI NAVIGAZIONE GALILEO E SERVIZIO PRS

Galileo è il sistema globale di navigazione satellitare (GNSS) dell'Unione europea progettato per inviare segnali radio per il posizionamento, la navigazione e la misurazione del tempo.

Il sistema Galileo è il programma nato dalla collaborazione tra Unione Europea e Agenzia Spaziale Europea (ESA) per migliorare l'autonomia tecnologica dell'Europa e definire gli standard internazionali per i sistemi di navigazione. Il programma Galileo riveste un'importanza strategica per l'indipendenza dell'Unione a livello di servizi di navigazione, posizionamento e invio di segnali orari via satellite oltre a fornire un contributo importante per una crescita intelligente, sostenibile e inclusiva di tutti i Paesi dell'Unione Europea.

Lo scopo finale del programma è la realizzazione di un sistema di navigazione satellitare, capace di fornire un servizio di posizionamento globale affidabile e ad alta precisione, interoperabile con il sistema statunitense GPS e il sistema russo GLONASS.

Il Parlamento europeo e il Consiglio hanno ricordato che il sistema Galileo è un sistema civile, realizzato secondo norme civili, in base a esigenze civili e sotto il controllo delle istituzioni dell'Unione. Però il sistema, pur essendo concepito per usi civili, è in grado di offrire un'accuratezza inferiore ai 10 centimetri nel posizionamento, precisione mai raggiunta prima. Inoltre, il sistema non è soggetto alle limitazioni o alle interruzioni tipiche di altri sistemi pensati per scopi militari, a cominciare dal GPS americano.

Galileo ha enormi potenzialità di impiego nei più diversi settori, dall'energia ai trasporti, dall'agricoltura alla finanza. A regime, Galileo consisterà di 30 satelliti (27 operativi e 3 di riserva) orbitanti su 3 piani inclinati di 56° sull'equatore (MEO, *Medium Earth Orbit* circolare) a 23.222 km quota. Il periodo orbitale sarà di circa 14 ore e 4 minuti con periodo di ripetizione della traccia al suolo di 10 giorni.

Il programma di lancio, con razzi Soyuz e Ariane, è iniziato il 21 ottobre 2011 con la partenza dei primi due satelliti dalla base di Kourou nella Guyana Francese ed è proseguito con il lancio della seconda coppia, IOV3 e IOV4, a ottobre 2012. La messa in orbita dei primi quattro satelliti costituiva la configurazione minima necessaria per poter validare il segnale, cominciare a fornire i primi servizi di navigazione e procedere a testare la piena funzionalità dei segmenti spaziali e di terra.

I primi servizi sono disponibili dalla fine del 2016. Le cinque tipologie di servizio offerte dal sistema Galileo si distinguono in base al tipo di segnale, in chiaro o criptato, e alle diverse necessità degli utilizzatori finali. Si distinguono in:

- *Open Service* (OS) – Il servizio si basa su segnali in chiaro e gratuiti per tutti, è destinato al mercato di massa e calcola il posizionamento con un'accuratezza inferiore al metro per la navigazione dei veicoli e i servizi di localizzazione sui telefoni cellulari.
- *Commercial Service* (CS) – Il servizio si basa su un segnale criptato che permette un'offerta commerciale dedicata di posizionamento e tempo per applicazioni specializzate.
- *Public Regulated Service* (PRS) – Il servizio ad accesso controllato fornisce il posizionamento e il tempo a utenti specifici come gli operatori per la sicurezza (forze di polizia, militari) che richiedono elevata affidabilità e continuità del segnale ed è dotato di sistemi antidisturbo e rilevamento affidabile dei problemi.
- *Search and Rescue Support Service* (SAR) – Il servizio è in grado di rilevare i segnali di emergenza, trasmettendoli in tempo reale ai centri di soccorso. Sarà utilizzato per la gestione di allarmi e la localizzazione di utenti in pericolo.

- *Safety of Life Service* (SoL) – Il servizio avvisa automaticamente gli utenti entro pochi secondi in caso di avarie dei satelliti o problemi analoghi riguardanti le prestazioni. Questo rende il servizio adatto alle applicazioni in cui la sicurezza è fondamentale (ad es. nella guida di treni, automobili, imbarcazioni ed aerei).

In particolare, il servizio PRS (*Public Regulated Service*) di Galileo è un servizio di navigazione crittografato per utenti autorizzati governativi e applicazioni sensibili che richiedono alta continuità.

Il PRS è simile ai servizi GNSS aperti e commerciali di Galileo, ma con alcune importanti differenze:

- Il PRS garantirà una migliore continuità del servizio agli utenti autorizzati quando l'accesso ad altri servizi di navigazione potrebbe essere compromesso.
- In caso di interferenze dannose, PRS aumenta la probabilità della disponibilità continua del segnale.

Inoltre, non è semplice attaccare il segnale PRS perché è più resistente a:

- *Spoofing,* cioè alla trasmissione di segnali GNSS contraffatti che potrebbero costringere un ricevitore a calcolare una posizione errata e indurre l'utente a credere di trovarsi in una posizione diversa da quella in cui si trova effettivamente. In questo caso PRS garantisce agli utenti autorizzati come forze di emergenza, polizia e altre autorità pertinenti di mantenere la capacità di servire il pubblico utilizzando le informazioni autentiche di posizionamento GNSS fornite da PRS.
- *Jamming*, ovvero la trasmissione intenzionale di segnali in radiofrequenza che possono interferire con i segnali GNSS portando a un degrado o al blocco dei servizi di navigazione e temporizzazione GNSS. PRS riduce questo rischio e semplifica l'identificazione di potenziali jammer.

Nel 2019 è iniziata la fase di sperimentazione del PRS, un servizio di alta precisione pensato per fornire dati di posizionamento per lo sviluppo di applicazioni sensibili, destinato ad utenti espressamente autorizzati dai governi nazionali.

Non appena l'intera costellazione Galileo sarà dispiegata ci sarà il passaggio graduale del servizio Galileo PRS da una fase iniziale alla piena capacità operatività. Parallelamente, a livello nazionale, si dovrà procedere, in modo progressivo, alla definizione e costruzione di una Capacità Nazione PRS. Si precisa che, ad oggi, l'Italia ha già sviluppato un proprio ricevitore, che ha confermato durante i test la fruibilità del segnale sulla base delle specifiche fornite dall'ESA.

Il sistema Galileo, una volta raggiunta la piena capacità operativa, garantirà all'Unione Europea sia l'autonomia strategica nel settore della navigazione satellitare sia la possibilità di utilizzare i propri servizi sinergicamente con quelli offerti da altri sistemi di navigazione satellitare, come il GPS. In particolare, il servizio PRS è stato concepito per essere autonomo ma anche interoperabile con il servizio GPS Militare.

a. Politica di Utilizzo del servizio PRS

Il Parlamento europeo e il Consiglio, con la Decisione n. 1104 del 2011, hanno stabilito che uno degli obiettivi del programma Galileo è che i segnali emessi da tale sistema possano essere utilizzati specialmente per offrire un servizio pubblico regolamentato (PRS), riservato unicamente agli utilizzatori autorizzati dai governi per applicazioni sensibili che richiedono un efficace controllo dell'accesso e un elevato livello di continuità di servizio.

Tra i vari servizi offerti da Galileo, il PRS è quello più protetto e più sensibile, è quindi adatto ai servizi che richiedono una garanzia di solidità e di assoluta affidabilità.

Infatti, deve garantire una continuità di servizio a beneficio degli utenti, anche nelle situazioni di crisi.

L'infrazione alle regole di sicurezza durante l'utilizzo di questo servizio non si limitano all'utilizzatore interessato, ma potrebbero estendersi a tutti gli utilizzatori. L'impiego e la gestione del PRS devono essere rigorosamente limitati a determinate categorie di utilizzatori che dovranno essere controllati in modo continuativo.

In merito ai principi generali di accesso al servizio PRS, il suo impiego è limitato agli Stati membri, al Consiglio Europeo, alla Commissione Europea che possono accedervi in modo discrezionale, illimitato e continuativo in tutto il mondo. Ogni Stato membro deve decidere autonomamente quali siano gli utilizzatori del PRS autorizzati e quali siano gli utilizzi che possano esserne fatti. Inoltre, ogni Stato deve fare in modo di impedire l'impiego dei segnali emessi per il PRS da parte di persone fisiche o giuridiche non autorizzate, e quindi evitare un utilizzo ostile del servizio nei suoi confronti di tutti gli Stati membri.

Al fine di promuovere la tecnologia europea su scala mondiale, è stato previso che paesi terzi e organizzazioni internazionali possano diventare partecipanti al PRS mediante la conclusione di accordi separati. Inoltre, sarà possibile, anche, autorizzare la fabbricazione di ricevitori PRS, ad eccezione dei moduli di sicurezza, purché siano impiegati tutti i requisiti utilizzati dagli Stati membri.

La decisione sopra menzionata prevede, inoltre, che i partecipanti al PRS nominino una "Autorità responsabile per il PRS" per la gestione e il controllo degli utilizzatori, che garantisca una gestione efficace dell'impiego del PRS e assicuri il controllo permanente degli utilizzatori nazionali. In Italia tale Autorità è alle dipendenze del Presidente del Consiglio dei ministri e risiede nell'Ufficio del Consigliere Militare. Gli Stati membri che non nominano l'Autorità responsabile per il PRS devono in ogni caso designare un punto di contatto per la gestione delle interferenze elettromagnetiche dannose con ripercussioni sul PRS.

L'Autorità Nazionale Responsabile per il PRS italiana ha identificato, tra le priorità nazionali, lo sviluppo di un Centro Nazionale PRS (CNP) e di un prototipo di Ricevitore a "doppia costellazione" (Galileo PRS più GPS). L'indisponibilità di un CNP e di un ricevitore PRS comporterebbe un impatto di natura operativa connesso alla fruizione limitata di uno strumento ad alta valenza strategica, senza poi tralasciare quello di natura economica, per i mancati sviluppi industriali.

L'importanza del Centro risiede nella necessità di gestire, a livello nazionale, l'interfaccia con il Sistema Galileo e con la comunità degli utenti (Forze Armate, Corpi di Polizia, ecc.) per le applicazioni nazionali del Servizio PRS, in accordo alla Direttiva Europea. Mentre obiettivo dello sviluppo del prototipo di ricevitore è di dotare gli utenti nazionali di un ricevitore a doppia costellazione che da una parte mantiene la compatibilità in termini di funzionalità, operatività e delle interfacce con gli attuali ricevitori GPS in dotazione e dall'altra offrirà nuove funzionalità, modi operativi e performance esclusivi del Galileo PRS.

b. La missione e il valore strategico del Centro Nazionale PRS

I servizi GNSS, inizialmente nati con il GPS, rappresentano oggigiorno una componente rilevante nel mondo dell'informazione, sono completamente integrati in svariati apparati e sistemi e sono utilizzati in numerose applicazioni che spaziano dalla difesa fino alla vita quotidiana delle persone.

Tuttavia, il crescente utilizzo del GPS e la crescente dipendenza da tale sistema rappresentano una potenziale minaccia: poiché il GPS *open service* non offre

protezione contro attacchi di *spoofing* e *jamming*, un utilizzatore potrebbe essere oggetto di azioni ostili volte ad inibire il servizio GPS ed ottenere un vantaggio su qualcuno/qualcosa. In questo contesto, tra i servizi offerti dal sistema Galileo, il servizio PRS è il più sicuro ed è pertanto il più indicato per quelle applicazioni che richiedono un elevato grado di continuità e robustezza del servizio.

La gestione del Servizio PRS, offerto dal Sistema Galileo, rientra nelle competenze della *Competent PRS Authority* (CPA), come stabilito dalle norme comunitarie. La CPA ha il compito, a livello nazionale, di interfacciarsi con gli utenti nazionali PRS e con la manifattura nazionale e, in ambito europeo, con il Sistema Galileo attraverso il *Galileo Security Monitoring Center* (GSMC).

Per poter fruire del servizio PRS a livello nazionale è necessario dotarsi di un Centro Nazionale PRS: il Centro rappresenta quindi l'elemento abilitante per permettere di dischiudere i vantaggi offerti dal servizio PRS alle comunità di utenti cui è rivolto. Il Centro deve essere in grado di configurarsi quale *asset* con le funzionalità di una Subagenzia della *National Distribution Agency* (NDA), specifica per le esigenze del Galileo PRS. Pertanto, il CNP sarà l'assetto che dovrà supportare la CPA nell'assolvimento della propria missione, svolgendo le seguenti funzioni essenziali:

- gestire la richiesta di ricevitori;
- gestire la richiesta e la distribuzione delle chiavi per l'accesso al servizio;
- gestire le richieste di servizio PRS da parte degli utenti nazionali
- gestire il mantenimento della configurazione;
- gestire eventuali incidenti di sicurezza;
- gestire eventuali segnalazioni di interferenza.

La modularità del progetto offre l'opportunità di sviluppare, con la massima celerità, le funzionalità principali che sono necessarie per la fruizione piena del servizio, e quindi evitare che l'indisponibilità del Centro possa impedire all'Italia una fruizione operativa del servizio. Altre funzioni collaterali verranno identificate nell'ambito di un'attività di ricerca condotta dall'Agenzia Spaziale Italiana (ASI), per cercare di espandere le funzioni del Centro alle esigenze degli utilizzatori. In maniera incrementale, sarà possibile sviluppare le capacità a valore aggiunto per massimizzare i benefici attesi dagli utenti.

c. Benefici derivanti dallo sviluppo del ricevitore a doppia costellazione

I ricevitori GPS sono oramai un elemento che appartiene alla nostra vita quotidiana, allo stesso tempo può essere visto come un nostro punto di debolezza da chi vorrebbe ottenere un vantaggio sulla nostra vita privata. Per questo motivo, nasce l'esigenza di sviluppare un sistema che garantisca un servizio affidabile per gli utenti autorizzati. I servizi Galileo PRS sono i più sicuri ed utilizzati per applicazioni che richiedono un elevato grado di continuità e robustezza del servizio.

Lo sviluppo di ricevitori a doppia costellazione (Galileo PRS e GPS) rappresenta una delle priorità individuate dall'Autorità Nazionale Responsabile per il PRS.

L'interoperabilità tra il servizio Galileo PRS e il servizio GPS, quindi la "dualità" del ricevitore, consentirà un miglioramento della continuità e della disponibilità dei servizi di navigazione. Inoltre, tale integrazione permetterà all'utenza autorizzata di poter fruire di un servizio robusto basato su una doppia sorgente di dati di navigazione che potrebbe mitigare i tentativi di "inganno" sulla posizione e di "mascheratura" sul segnale ricevuto.

Questa soluzione "duale" prevede due catene elaborative distinte che possono interagire tramite opportuni algoritmi di fusione dei dati e, comunque, sotto il controllo

dell'utente. La tipologia di segnali che possono essere accoppiati può essere di differente natura: segnali Galileo OS e GPS civile, per usi non governativi, e segnali Galileo PRS e GPS militare per usi governativi. Tale approccio garantisce all'Utenza Nazionale di:

- Mantenere l'accesso ai servizi GPS già in uso;
- Sperimentare l'utilizzo combinato dei servizi Galileo e GPS;
- Usufruire di un ricevitore Galileo PRS e GPS militare ad elevatissime performance, innovativo, ad accesso autorizzato ed in grado di offrire nuove funzionalità e modi operativi.

Per garantire l'accesso simultaneo e combinato al servizio Galileo PRS e GPS militare è necessario che il prototipo sia in grado di ospitare due diversi moduli crittografici.

Lo sviluppo del prototipo ha come obiettivo quello di coprire i requisiti utente e minimizzare i rischi tecnologici. Per raggiungere tale obiettivo verranno adottate strategie finalizzate a:

- Utilizzare componenti hardware COTS affidabili e sviluppati in paesi dell'Unione Europea;
- Garantire la manutenzione e gli upgrades dei componenti software e firmware del prototipo
- Possibilità di accedere, oltre al servizio Galileo PRS e GPS militare, anche ai servizi *open* quali Galileo OS e GPS C/A;
- Utilizzare algoritmi di *signal processing* allo stato dell'arte implementabili in piattaforme possibilmente riconfigurabili.

d. Potenziali Utenti PRS

Si ritiene utile, prima di affrontare il contesto degli utenti PRS, definire i partecipanti al PRS che sono gli Stati membri, il Consiglio, la Commissione nonché, se debitamente autorizzati, le agenzie dell'Unione, i paesi terzi e le organizzazioni internazionali; mentre per utilizzatori del PRS si intendono le persone fisiche o giuridiche debitamente autorizzate dai partecipanti al PRS a possedere o utilizzare un ricevitore PRS.

Come conseguenza di queste definizioni, i potenziali utenti dell'Italia, che accedono al servizio PRS o interessati all'utilizzo del servizio PRS e che hanno contribuito alla definizione dei requisiti del CNP e del ricevitore PRS, sono:

- Presidenza del Consiglio dei ministri con le sue Agenzie di sicurezza;
- Ministero della Difesa;
- Ministero dell'Interno.

Altri attori, intendendo il PRS in tutte le sue declinazioni applicative, sono stati identificati in altre aree applicative, tra le quali:

- Ministero delle Infrastrutture e Trasporti (settore infrastrutture e trasporti, ecc.);
- Ministero dello Sviluppo Economico (settore telecomunicazioni ed energia);
- Dipartimento della Protezione Civile;
- Gestori di infrastrutture critiche (Banca d'Italia, Eni, Enel, ecc.).

Nella Tabella 2 si riportano le varie applicazioni che il servizio PRS potrebbe garantire agli utenti PRS istituzionali precedentemente descritti:

Settore	Ambito	Applicazione
Militare	Sistemi avionici	Aerei da trasporto, Caccia, Elicotteri, Droni
	Munizionamento	Guida munizioni
	Sistemi terrestri	Veicoli terrestri, Carri, Trasporto truppe, Equipaggiamento tattico, Palmari
	Sistemi navali	Unità navali, Sommergibili
	Sistemi logistici	Veicoli terrestri, Palmari
Sicurezza pubblica	Carabinieri, Polizia di Stato, Guardia di Finanza, Guardia Costiera	Aerei, Elicotteri, Droni, Veicoli terrestri, Equipaggiamento, Palmari, Sorveglianza, Navi
	Protezione civile, Forestale, Vigili del Fuoco	Aerei, Elicotteri, Droni, Veicoli terrestri, Palmari

Tabella 2 Applicazioni del servizio PRS

La definizione dei requisiti per poter sviluppare il CNP e il ricevitore PRS è avvenuta attraverso un gruppo di lavoro interministeriale composto dagli utenti interessati ai servizi PRS. Questo gruppo di lavoro ha analizzato le esigenze di tutti gli utenti relativamente al ricevitore PRS e al Centro Nazionale PRS, affrontando le seguenti aree tematiche: l'organizzazione e il personale, le infrastrutture e i materiali e il concetto di impiego.

Il processo di definizione dei requisiti è stato di tipo iterativo su due livelli:

- Il primo livello è stato all'interno della singola area tematica, con l'obiettivo di raccogliere le esigenze che provenivano da differenti organizzazioni;
- Il secondo livello è stato tra aree tematiche, attraverso uno scambio di input in maniera coordinata e concorrente.

Attraverso tale approccio è stato possibile generare una serie di risultati che sono stati utilizzati per l'avvio del processo di *procurement* e allo stesso tempo valorizzare al meglio la fase di studio che porterà all'affinamento dei requisiti.

5. APPROCCIO PER L'ANALISI DEL RISCHIO DEL CNP

La sicurezza delle Informazioni, come già detto, è assicurata quando vengono assicurate le tre caratteristiche di fruizione:

- Riservatezza, proteggono i dati al fine di contrastare la divulgazione non autorizzata;
- Integrità, contrastano le modifiche non autorizzate dei dati;
- Disponibilità, contrastano la indisponibilità malevola dei dati/servizi;
- Autenticazione, contrastano l'accesso non autorizzato ai dati.

Gli obiettivi di sicurezza dovrebbero essere utilizzati per guidare gli sforzi impiegati nella modellazione delle minacce. Per determinare gli obiettivi sicurezza, occorre identificare prima di tutto le informazioni da proteggere e i requisiti di conformità (criteri di protezione, leggi sua privacy, regolamenti e standard).

L'approccio utilizzato per effettuare l'analisi del rischio del CNP, partendo dal quadro normativo nazionale vigente (PCM-ANS/TI-002) e sposandone appieno la metodologia di base, si è ampliato il catalogo delle misure di sicurezza aprendolo alla gestione delle minacce cyber, non contemplate nella normativa nazionale, e all'adozione dei controlli dello standard ISO 27002.

a. Cyber Security

Partendo dall'ambiente Cyber, in questo paragrafo si descrive l'approccio con cui è stato affrontato il concetto di *Cyber Security* nell'ambito del programma CNP nelle fasi di Progettazione, Realizzazione e Manutenzione del sistema. In ciascuna delle fasi di progetto è importante affrontare il problema della *cyber security* che durante la fase di analisi del rischio si traduce nell'identificazione di minacce, vulnerabilità e contromisure.

La normativa nazionale, utilizzata per l'analisi del rischio, risulta abbastanza datata e pertanto non include tutte quelle misure di sicurezza cibernetica emerse negli ultimi anni, pertanto si ricorre al Framework di cyber sicurezza del NIST (*National Institute of Standards and Technology*). Il NIST agisce nell'ambito del Dipartimento del Commercio degli Stati Uniti, creando standard per molti settori dell'infrastruttura statunitense. Il framework cyber è stato creato con la partecipazione sia dell'industria sia del governo, ed è composto da standard, linee guida e prassi riguardanti la sicurezza delle infrastrutture critiche. Il framework utilizza comuni motori economici del settore per guidare e gestire i rischi, proteggere le informazioni e le persone che utilizzano i servizi aziendali.

Sicurezza della Progettazione

L'approccio alla sicurezza nella progettazione di un sistema CIS è oggi l'unico modo percorribile per garantire la sicurezza dei dati che il sistema tratta ed al contempo garantire la sicurezza del sistema stesso. Le nuove minacce informatiche rendono indispensabile l'uso di strumenti e pratiche avanzate per la mitigazione del rischio considerando che gli attacchi sono spesso il risultato di vulnerabilità che si celano all'interno della progettazione del software. Le vulnerabilità del software sono una realtà legata al fatto che le politiche di qualità del software ed i relativi investimenti sono spesso focalizzati sulla correzione dei bug funzionali e sulle sue performance ma molto spesso si trascurano l'attuazione di pratiche di progettazione e programmazione che garantiscano la sicurezza del sistema.

Negli ultimi anni ha avuto inizio una incrementale diffusione della "buona condotta" in materia di sicurezza applicativa riconducibile ad:

- una buona ingegnerizzazione del software;
- una piena comprensione delle minacce da contrastare;

- una maggiore conoscenza dei difetti propri dei linguaggi di programmazione adottati.

La progettazione di software sicuro non è un'attività semplice ma una strategia che potrebbe, rendere più facilmente analizzabili le minacce potenziali a cui il sistema è soggetto e permettere di definire i requisiti di sicurezza nella progettazione di applicazioni più sicure.

Nel corso della fase di progettazione è necessario garantire anche un adeguato livello di sicurezza applicativa e infrastrutturale attraverso l'analisi e la modellazione delle minacce inerenti agli applicati coinvolti, delle interfacce e degli agenti che potrebbero minacciare il sistema.

Sicurezza nella Realizzazione

La fase di Realizzazione del software introduce sicuramente vulnerabilità e problemi di sicurezza come la gestione delle interfacce e la sincronizzazione tra le diverse componenti software. Vale la pena perciò introdurre nel processo di sviluppo del software strumenti in grado di valutare la sicurezza. Tali strumenti dovrebbero implementano funzionalità come:

- l'analisi del codice e la conseguente emissione di una relazione sui risultati ottenuti da cui nascono le opportune raccomandazioni al team di sviluppo;
- la verifica dell'architettura, dell'applicazione e conseguente identificazione delle violazioni alla "buona condotta" e allo standard di riferimento.

L'analisi svolta dai suddetti strumenti costituisce un valido riferimento per una corretta gestione della realizzazione del software da indirizzare al team di sviluppo ed a tutti coloro che hanno un ruolo importante nella fase di realizzazione del software.

Al fine di intraprendere un'attività di sviluppo che possa prevenire problematiche di sicurezza nel codice e fornire allo stesso tempo un valido strumento per l'individuazione di possibili vulnerabilità presenti nel codice sorgente, l'Agenzia per l'Italia Digitale (AgD) ha emesso delle linee guida per la generazione del codice sicuro.

Sicurezza nella Manutenzione

Dopo la realizzazione del sistema e la sua messa in operazione un aspetto importante da non sottovalutare è la modalità di manutenere il sistema garantendone sempre un adeguato livello di sicurezza. É possibile separare le problematiche in:

- Sicurezza dell'Ambiente IT (*Information Tecnology*)
- Sicurezza del Software Proprietario

Sicurezza dell'Ambiente IT: Per mantenere sicuro il software proprietario è importante prima di tutto mantenere sicuro l'ambiente IT in cui esso opera. Per raggiungere tale obiettivo l'attività primaria da attuare sull'ambiente IT è quella di mettere in atto un'attività di *patching* programmato sull'ambiente IT considerando il Sistema Operativo e i COTS installati. Il problema della gestione delle patch è un concetto chiave per la sicurezza cyber dove le patch di Sistema Operativo e COTS vengono identificate come uno strumento per gestire le vulnerabilità e le lacune di sicurezza dell'intero sistema. I produttori di software forniscono regolarmente patch per i loro prodotti che vanno installate per aggiornare i sistemi e spesso per risolvere non solo problemi funzionali ma anche falle di sicurezza.

Oggi i Sistemi Operativi prevedono il rilascio di patch con un dettaglio granulare pertanto è più facile identificare le singole patch e l'obiettivo con cui sono rilasciate. Naturalmente la gestione delle patch è un processo complesso quando il sistema si trova in un contesto operativo pertanto l'attività va gestita con particolare attenzione.

Sicurezza del software proprietario: Come previsto dalla normativa vigente, dall'analisi del rischio viene calcolato un livello di garanzia che identifica il livello di profondità di valutazione a cui il sistema viene sottoposto. A seguito della valutazione e certificazione di tutte le modifiche a cui il sistema è sottoposto, nella sua vita operativa il software proprietario dovrà essere sottoposto a un processo di mantenimento della certificazione conseguita.

É evidente che nel corso della sua vita operativa il software proprietario è sottoposto a campagne di *patching* funzionale per risolvere bug operativi pertanto al fine di agevolare il mantenimento della certificazione, si propone di sottoporre a valutazione il sistema in tutte le fasi di realizzazione.

b. La serie dello standard ISO 27000

ISO (*International Organization for Standardization*) è un'organizzazione internazionale indipendente e non governativa che ha creato più di 20.000 serie di standard in una vasta gamma di settori, tra cui i servizi di ristorazione, la tecnologia e l'agricoltura. La serie 27000 è stata utilizzata per il tema della sicurezza informatica, in particolare da 27001 a 27006:

ISO-27001 Fornisce i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni.

ISO-27002 Stabilisce linee guida e principi generali per avviare, implementare, mantenere e migliorare la gestione della sicurezza delle informazioni all'interno di un'organizzazione.

ISO-27003 Guida applicativa del sistema di gestione della sicurezza delle informazioni.

ISO-27004 Fornisce indicazioni su sviluppo e utilizzo di misure e misurazioni per la valutazione dell'efficacia di un sistema di gestione della sicurezza delle informazioni implementato.

ISO-27005 Fornisce linee guida per la gestione del rischio di sicurezza delle informazioni in un'organizzazione.

ISO-27006 Requisiti per gli enti che si occupano di revisione e certificazione dei sistemi di gestione della sicurezza delle informazioni.

L'approccio utilizzato nella serie 27000 della ISO è quello dell'analisi "per processi", e uno degli obiettivi principali e l'implementazione di un sistema di gestione ciclico capace di migliorare continuamente i processi gestiti. Tale approccio per processi è esplicitamente definito in ISO 27001 del 2005 che definisce i concetti fondamentali di Sistema di Gestione per la Sicurezza dell'Informazione (SGSI) e di Politica di Sicurezza.

L'SGSI viene definito come quell'insieme di responsabilità, ruoli organizzativi, modalità operative, procedure, istruzioni di lavoro, tecnologie e ambienti fisici che consentono ad un'organizzazione di tenere sotto controllo e di migliorare la sicurezza delle informazioni, adeguando continuamente le proprie componenti all'evoluzione tecnologica, in armonia con la Politica di Sicurezza.

I sistemi di gestione definiti secondo questi principi sono in grado quindi di mantenere e migliorare nel tempo le proprie caratteristiche.

Lo standard ISO 27001 è basato sul modello PDCA (Plan, Do, Check, Act), che è uno strumento per conseguire il miglioramento e si può applicare a tutte le organizzazioni, processi e attività. Il ciclo PDCA (Figura 3) è costituito da quattro fasi:

- pianificare (plan): individuare le attività, i processi e gli strumenti da utilizzare per conseguire i risultati previsti;
- realizzare (do) quanto pianificato;
- verificare (check) quanto realizzato rispetto a quanto pianificato;
- intervenire (act) se a fronte delle verifiche si individuano carenze.

Figura 3 Ciclo PDCA (Plan – Do – Check – Act)

Pianificare: questa fase del ciclo PDCA è spesso fraintesa: quando si chiede di pianificare, non necessariamente si chiede di predisporre piani molto dettagliati con ogni fase da completare. Il dettaglio della pianificazione dipende dalla dimensione e criticità del progetto: la pianificazione deve comunque evidenziare tutte le attività da completare e le loro interrelazioni, in modo da non avere conflitti tra di esse.
Per l'SGSI con pianificare si intende stabilire la politica di sicurezza, gli obiettivi, i processi e le procedure rilevanti per la gestione del rischio e per il miglioramento della sicurezza delle informazioni, secondo le politiche e gli obiettivi dell'organizzazione.

Fare: questa fase è quella che trova sempre attuazione e consiste nel realizzare quanto pianificato. In molti casi, quando la pianificazione è carente, la realizzazione risulta a sua volta di scarsa qualità o più costosa di quanto lo sarebbe stata se si fosse prestata maggiore attenzione alla pianificazione.
Per l'SGSI con fare si intende implementare e utilizzare la politica di sicurezza, i controlli, i processi e le procedure.

Verificare: questa fase consiste nel verificare che quanto fatto sia efficace[6]. Per questo, è opportuno riportare la seguente definizione della ISO/IEC 27000.

Le verifiche, nel caso di progetti o produzioni complesse, non andrebbero effettuate solo al termine dei lavori, ma anche in fasi intermedie, per risolvere tempestivamente eventuali difficoltà. Questa fase è spesso ignorata o sottovalutata: nella pratica si discute spesso su cosa fare, senza analizzare successivamente se quanto deciso è stato attuato efficacemente.
Le verifiche vanno stabilite nella fase di pianificazione, per decidere quando farle e come farle.
Per l'SGSI con verificare si intende valutare e, dove applicabile, misurare le prestazioni dei processi di sicurezza rispetto alla politica di sicurezza, agli obiettivi e all'esperienza pratica, riferire i risultati alla direzione per la revisione.

Intervenire: se nella pratica le verifiche sono svolte regolarmente, gli interventi successivi sono molto più rari, nonostante siano fondamentali. Alcune volte gli interventi devono essere effettuati quando si individuano errori o situazioni impreviste, altre volte quando si individuano degli elementi da migliorare.

[6] Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati pianificati raggiunti.

Per l'SGSI con verificare si intende intraprendere azioni correttive e preventive basate sui risultati della revisione della direzione, allo scopo di ottenere il miglioramento continuo dell'SGSI.

Poiché lo standard non impone una metodologia per la valutazione dell'analisi del rischio i documenti relativi alla valutazione del rischio devono illustrare l'approccio, la metodologia e le tecniche scelte per tale attività. Devono essere documentate le motivazioni che hanno spinto a tali scelte, evidenziando la coerenza con i requisiti di sicurezza con la missione e la dimensione dell'organizzazione e con i rischi da affrontare.

c. Peculiarità fra standard

La Tabella 3 mostra una sintesi di comparazione delle peculiarità dello schema nazionale, la cui adozione e prevista dal quadro normativo per i sistemi che trattano informazioni classificate, e la famiglia di standard ISO 27000.

Normativa nazionale	ISO 27000
È orientata al Sistema	È orientata alle informazioni
È un obbligo di legge	È una scelta dell'organizzazione
Consente il trattamento di informazioni classificate	Consente di implementare un Sistema di gestione per la sicurezza delle informazioni
Definisce una Metodologia di Analisi di Rischio	Definisce i requisiti per l'Analisi di Rischio
Catalogo estendibile e personalizzabile di minacce e vulnerabilità	Catalogo estendibile e personalizzabile di minacce e vulnerabilità
Catalogo estendibile e personalizzabile di misure di sicurezza	Controlli obbligatori ed eventuali altri controlli aggiuntivi scelti dall'organizzazione
Definisce il livello di garanzia come output dell'analisi di rischio	L'analisi di rischio non definisce il livello di garanzia
Il valutatore è autorizzato dal DIS	Il valutatore è autorizzato da ISO/CEN/UNI

Tabella 3 Comparazione tra normativa nazionale e ISO 27000

È da evidenziare che i riferimenti citati nella Tabella, pur avendo due orientamenti differenti ed essendo stati pensati con finalità completamente diverse, prevedono in alcuni casi verifiche riguardanti aspetti similari. Quando ciò avviene, l'uso congiunto dei due approcci può identificarsi come un tentativo di ottimizzare quanto richiesto dallo schema nazionale. L'approccio di estendere la metodologia di analisi di rischio prevista dalla normativa vigente con quanto proposto dallo standard ISO 27000 è stata la base di partenza per migliorare l'analisi del rischio.

d. Metodologia per l'Analisi di Rischio

Al fine di condurre l'analisi di rischio in linea con l'approccio anticipato in precedenza, si è proceduto nel seguente ordine:

1. Avviare il processo di analisi a partire dalla normativa vigente ed in particolare dal catalogo fornito dalla PCM-ANS/TI-002, in termini di Minacce, Vulnerabilità e Contromisure;
2. Estendere il catalogo di cui al punto precedente al fine a contemplare nuovi elementi quali Minacce, Vulnerabilità e Contromisure, in particolare per la *compliance* allo standard ISO 27002;

3. Considerare i parametri di input all'analisi di rischio che concorrono all'individuazione delle minacce e delle vulnerabilità ad esse associate ed allo stesso tempo considerare i parametri di output che forniscono una visione semplificata dei risultati della metodologia operata;
4. Identificazione del livello di garanzia delle funzionalità richieste al sistema a fronte delle misure tecniche in termini percentuali

La normativa PCM-ANS/TI-002 identifica un catalogo di Minacce, Vulnerabilità e Contromisure a cui far riferimento nell'ambito dell'esecuzione dell'analisi di rischio del sistema da proteggere. Pertanto, tale catalogo è stato preso a riferimento per l'analisi di rischio del Centro Nazionale PRS.

e. Ampliamento del Catalogo di Minacce e Vulnerabilità

Alle minacce e vulnerabilità già previste dalla normativa nazionale, elencate negli Allegati B e C, si è proceduto con uno studio di estensione dei cataloghi di minacce e vulnerabilità a tre livelli.

Come prima cosa è stata fatta un'analisi, a livello generale, delle minacce e vulnerabilità presenti sulla normativa e quelle non trattate dalla normativa, che risulta abbastanza vecchia rispetto all'evoluzione tecnologica degli ultimi anni, portando così ad un ampliamento del catalogo di primo livello.

Come seconda cosa sono state analizzate le possibili minacce e vulnerabilità tipiche di una organizzazione militare, struttura militare o struttura strategica di interesse nazionale, portando ad un ampliamento del catalogo di secondo livello.

Infine, sono state considerate tutte quelle minacce e vulnerabilità a cui sono soggette le apparecchiature che lavorano nel campo satellitare, sia come segmento Spazio che come Segmento Terra, incrementando ulteriormente il catalogo delle minacce e vulnerabilità.

Questo studio ha portato ad un ampliamento del catalogo con 14 minacce e 19 vulnerabilità aggiuntive, che si riportano in Allegato D. Si precisa che non tutte le minacce e vulnerabilità presenti sulla PCM-ANS/TI-002 e su questo ampliamento del catalogo sono state considerate nell'analisi del rischio del Centro Nazionale PRS, ma solo quelle che sono state considerate possibili partendo dall'Architettura fisica e funzionale del CNP, che è descritta nella prima bozza di "Progetto preliminare" del sistema. Quindi, riprendendo lo schema metodologico riportato in Figura 2 del capitolo 3 e partendo dal catalogo esteso delle minacce e vulnerabilità, è stato calcolato il livello di garanzia del Centro, che non potrà essere descritto nel dettaglio in questo documento perché ha un livello di classifica.

f. Ampliamento del Catalogo di Contromisure

Invece, il catalogo di contromisure presente sulla normativa PCM-ANS/TI-002, utilizzato come base di partenza, è stato ampliato considerando le problematiche Cyber emerse negli ultimi anni oltre ai controlli forniti dalla famiglia ISO 27000.

I controlli della famiglia ISO 27000, in particolare quelli contenuti nello standard ISO 27002, che si riportano in Allegato E, per livello di granularità possono essere associati alle contromisure della PCM-ANS/TI-002, pertanto è stato esteso il catalogo di base della PCM-ANS/TI-002 con nuove contromisure che mappano i controlli della ISO 27002. Il nuovo catalogo esteso di contromisure, inserendo i controlli previsti dalla ISO ha incrementato il numero di misure fisiche, personali, procedurali e tecniche previste nella PCM-ANS/TI-002 e ha creato una nuova classe di contromisure denominata Comunicazione.

Oltre all'estensione dei controlli previsti dalla ISO 27002, è stata operata un'ulteriore estensione attraverso un'analisi delle sottocategorie di controlli previste dal framework NIST, riportato in Allegato F, sia perché è universalmente riconosciuto come framework di *cyber security* sia perché contiene una mappatura con i controlli previsti dallo standard ISO 27002. Dall'analisi è emerso che le contromisure previste dalla PCM-ANS/TI-002, estese con i controlli previsti dalla famiglia ISO 27000, coprono già alcune categorie del framework di *cyber security* più recente.

Laddove invece le contromisure previste dalla normativa nazionale non sono sufficienti a consentire una copertura equivalente rispetto alle categorie di controlli del framework sono state aggiunte delle contromisure aggiuntive raggruppate in una nuova ulteriore classe di contromisure denominata Cyber.

Va notato che sia la famiglia ISO 27000 che i framework NIST includono delle classi di misure relative alla risposta agli incidenti cibernetici e al ripristino dei servizi. Queste misure sono pensate per una condizione post incidente, ovvero nella condizione in cui le contromisure implementate non sono state sufficienti a contrastare la minaccia. Pertanto, non sono state incluse nell'estensione di tale catalogo perché non contribuiscono alla riduzione del rischio iniziale.

g. Descrizione del Tool per l'Analisi del Rischio

Al fine di ottenere il livello di garanzia del Centro Nazionale PRS è stato creato un tool, che comunque si potrà utilizzare per qualsiasi sistema EAD da certificare, per rendere automatizzato il calcolo del livello di garanzia, come descritto nel paragrafo e. del terzo capitolo.

Nella prima schermata del tool bisogna associare minacce, vulnerabilità e contromisure. A titolo di esempio si riporta in Figura 4 una prima parte della tabella di correlazione tra minacce, vulnerabilità e contromisure, che rappresenta il primo step dell'analisi del rischio. La correlazione rappresentata nella figura non rappresenta il caso reale del CNP ma è un esempio di associazione estratta dall'allegato 7 della PCM-ANS/TI-002.

TABELLE DI CORRELAZIONE
MINACCE / VULNERABILITÀ / CONTROMISURE

VULNERABILITÀ	Vi	CONTROMISURE	N	Nt
Minaccia: MASCHERAMENTO			**Vi=7**	
Supervisione non adeguata	**1**	**pe5.** Creazione di uno staff di supporto agli utenti, che effettui controlli sulla sicurezza, e fornisca assistenza sulle problematiche legate alla sicurezza	**1**	
		pe6. Designazione del responsabile della sicurezza	**1**	
Personale non addestrato	**3**	**pe4.1** Test di reparto per valutare il grado di alfabetizzazione informatica del personale	**1**	
		pe4.2 Corso interno di utilizzo delle procedure sulla base dei test effettuati	**1**	
		pe4.3 Esami finali di valutazione del grado di conoscenza acquisito	**1**	
		pe4.4 Verifiche periodiche della conoscenza	**1**	
		pe4.5 Creazione di gruppi di lavoro a secondo della competenza specifica	**1**	
Uso scorretto delle informazioni da parte degli utenti finali	**3**	**pe3.1** Motivare il personale a seguire la politica della società o dell'Ente di appartenenza	**1**	
		pe3.3 Mantenere costante l'attenzione alle norme di sicurezza, adottando poster, lettere circolari, video didattici.	**1**	
		pe3.5 Verificare regolarmente l'addestramento del personale relativo alla sicurezza	**1**	
		pe3.6 Mantenere informato il personale sulle novità legate alla sicurezza	**1**	

Figura 4 Tabella di correlazione minacce/vulnerabilità/contromisure

Nella seconda schermata del tool, si troverà la tabella riepilogativa dell'analisi del rischio, come si può vedere in Figura 5. Nella tabella seguente, nelle celle colorate di azzurro si trovano i numeri che vengono calcolati dalla tabella di correlazione precedente (a titolo di esempio si riporta Vi=7, N=11, Nt=0), nelle celle colorate di verde si dovranno inserire i valori del livello di minaccia e della complessità sensibilità del sistema, mentre le celle gialle vengono calcolate come già descritto nel terzo capitolo.

CALCOLO FINALE		
Vulnerabilità iniziale	*Vi*	7
Numero contromisure	*N*	11
Numero contromisure tecniche	*Nt*	0
Valore contromisure	*Cm*	
Capacità offensiva	*Coff*	
Grado di esposizione	*Gesp*	
Appetibilità dei dati	*Adat*	
Livello minaccia	*Lm*	
Modalità operativa	*Mope*	
Numero utenti	*Nute*	
Classifica informazioni	*Lcla*	
Quantità informazioni	*Qinf*	
Fattore correttivo Beta	*ß*	
Vulnerabilità residua	*Vr*	
Percentuale contromisure tecniche	*Mt*	
Livello garanzia		**E__**
Indice "P"		

Figura 5 Tabella per il calcolo del livello di garanzia

6. CONCLUSIONI E CONSIDERAZIONI

In questo elaborato è stato introdotto il Sistema di gestione per la sicurezza delle informazioni, per i sistemi di elaborazione automatica dei dati. Partendo dalla definizione di sicurezza nel settore informatico sono state definite le procedure per garantire un ambiente più sicuro a livello generale, e se si parla di strutture strategiche di consentire anche la tutela del Segreto di Stato. Ad esempio, istruire gli utenti può risultare un'impresa enorme, ma se lo si fa nel modo corretto permette di ottenere un buon livello di difesa e monitoraggio, che potrebbe aumentare notevolmente la protezione una volta creati dei solidi valori di riferimento.

Un altro pilastro fondamentale per garantire la sicurezza di un sistema è il controllo, che deve essere effettivo ed efficace. Se un aggressore, per entrare in possesso di informazioni sensibili, cercasse di entrare fisicamente nell'edificio, che ospita il sistema, con la forza, il sotterfugio o di nascosto, un basso livello di controllo d'accesso fisico potrebbe mettere i dati o i sistemi a rischio. Logicamente, oltre al controllo di accesso fisico al sistema bisogna porre attenzione anche al controllo di accesso logico, che con i pirati informatici sta diventando una pratica molto diffusa.

La misurazione della sicurezza, basata sul livello di garanzia, di un sistema EAD è stata effettuata utilizzando lo standard ITSEC, in particolare per sistemi o reti militari è stata utilizzata la procedura di omologazione prevista dalla PCM-ANS/TI-001 ed è stata condotta l'analisi del rischio secondo la PCM-ANS/TI-002. Inoltre, è stata ampliata questa normativa nazionale utilizzando i controlli di sicurezza previsti dalla famiglia ISO 27000 e dal framework cyber del NIST. Questo ampliamento dei cataloghi di minacce, vulnerabilità e contromisure è stato necessario visto il mancato aggiornamento della normativa nazionale, che è stata redatta nel 1995, alla repentina evoluzione tecnologica degli ultimi decenni.

L'analisi del rischio, condotta secondo la normativa nazionale e ampliata con gli standard internazionali, ha trovato applicazione nel Centro Nazionale PRS (CNP), dove PRS è il servizio governativo con accesso controllato del sistema Galileo.

Considerata l'elevata valenza strategica del CNP, l'Italia, come anche tutte le altre nazioni della Comunità Europea, sta conducendo uno studio di fattibilità per realizzare il CNP e l'Autorità nazionale PRS della Presidenza del Consiglio dei ministri, con il supporto dell'Agenzia Spaziale Italiana, ha commissionato all'industria nazionale del settore spaziale la definizione e la progettazione preliminare del CNP. Come in tutti i sistemi o reti EAD che trattano informazioni sensibili anche per il CNP, il progetto preliminare si concluderà con la definizione dei processi operativi per la gestione dei servizi PRS e quindi con l'architettura funzionale del Centro, in questa fase è indispensabile effettuare, anche, la valutazione del rischio e quindi stabilire i requisiti di sicurezza del Centro Nazionale PRS, che saranno la base di partenza per la redazione delle Specifiche tecniche per la realizzazione del Centro.

In questo documento, partendo dall'architettura funzionale del CNP, sono state analizzate tutte le probabili minacce a cui il Centro potrebbe essere soggetto e le conseguenti vulnerabilità, inoltre sono state proposte le contromisure necessarie per assicurare un livello di garanzia adeguato alle informazioni che verranno trattate. Si precisa che nel documento è stata trattata solo la metodologia utilizzata e non è stato possibile fornire i risultati dell'analisi del rischio dato che questi sono classificati, e sono contenuti in un documento separato a questo elaborato. L'analisi del rischio dovrà essere rivista e modificata in funzione degli ultimi documenti sullo studio di fattibilità che verranno consegnati nei prossimi mesi, per poi definire i requisiti di sicurezza specifici e attivare l'iter di approvazione.

BIBLIOGRAFIA

Libri

- Lee Brotherston, Amanda Berlin, *La sicurezza dei dati e delle reti aziendali*, Tecniche Nuove, Milano, 2018.
- Cesare Gallotti, *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001:2013*, Lulu.com, 2017.
- Luigi Lo Russo, Elena Bianchi, *Sistemi e reti Per l'articolazione informatica. Per gli Ist. tecnici settore tecnologico*, Hoepli, Milano, 2017.

Normative e Standards

- International Organization for Standardization, *Information technology - Security techniques - Information security management systems - Requirements,* ISO/IEC 27001:2005.
- International Organization for Standardization, *Information technology - Security techniques - Code of practice for information security management,* ISO/IEC 27002:2005.
- International Organization for Standardization, *Information technology - Security techniques - Information security management systems implementation guidance,* ISO/IEC 27003:2010.
- International Organization for Standardization, *Information technology - Security techniques - Information security management – Monitoring, measurement, analysis and evaluation,* ISO/IEC 27004:2016.
- International Organization for Standardization, *Information technology - Security techniques - Information security risk management,* ISO/IEC 27005:2011.
- International Organization for Standardization, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems,* ISO/IEC 27006:2015.
- Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, *recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*.
- Decreto del Presidente del Consiglio dei ministri n. 7 del 12 giugno 2009, *Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica.*
- Decreto del Presidente del Consiglio dei ministri n. 4 del 6 novembre 2015, *Disciplina della firma digitale dei documenti classificati.*
- Decreto del Presidente del Consiglio dei ministri n. 5 del 6 novembre 2015, *Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva.*
- Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*.
- Legge n. 124 del 3 agosto 2007, *Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*.
- Presidenza del Consiglio dei ministri, *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*, marzo 2017.
- Presidenza del Consiglio dei ministri – Autorità Nazionale per la Sicurezza, *PCM-ANS/TI-001 Procedura nazionale per l'omologazione di sistemi/reti EAD militari*, 1995.

- Presidenza del Consiglio dei ministri – Autorità Nazionale per la Sicurezza, *PCM-ANS/TI-002 Standard di sicurezza per sistemi/reti EAD militari*, 1995.
- Organismo di Certificazione di Sicurezza (OCSi), *Linee guida provvisorie parte 1 (LGP1) – Descrizione Generale dello Schema Nazionale,* dicembre 2004.
- Decisione N. 1104/2011/UE Parlamento Europeo e del Consiglio del 25 ottobre 2011, *relativa alle regole di accesso al servizio pubblico regolamentato offerto dal sistema globale di navigazione satellitare istituito dal programma Galileo.*
- Decisione (UE, Euratom) 2015/444 della Commissione del 13 marzo 2015, *sulle norme di sicurezza per proteggere le informazioni classificate UE.*

Documentazione tecnica

- Agenzia Spaziale Italiana, *Allegato tecnico gestionale per la Realizzazione del Centro Nazionale PRS GALILEO (CNP)*.
- Presidenza del Consiglio dei ministri – Autorità Nazionale PRS, *Requisiti Utente del Centro Nazionale PRS (CNP).*
- Presidenza del Consiglio dei ministri – Autorità Nazionale PRS, *Requisiti Utente del Prototipo Rx a doppia costellazione.*
- Telespazio, *Vulnerability and Risk analysis (as designed) del Centro Nazionale PRS (CNP).*
- Telespazio, *Accreditation & Certification Plan del Centro Nazionale PRS (CNP).*

A. *Common Criteria* secondo lo standard ISO 15408[7]

La valutazione dell'affidabilità di un prodotto informatico, hardware o software o firmware, è uno dei problemi più difficili da risolvere in tutto il campo dell'informatica.

Per questo motivo ci sono metodologie per dimostrare quanta fiducia si possa riporre nelle misure di sicurezza di un prodotto informatico. La principale di queste metodologie fa riferimento ai cosiddetti *Common Criteria*, al momento quelli in grado di fornire i risultati più attendibili. Sono indicati anche come CC e sono stati recepiti come standard internazionale ISO 15408.

Lo scopo principale dello sviluppo dei CC è quello di formare una comune base per la valutazione delle proprietà di sicurezza di prodotti e sistemi IT, che presenti la giusta flessibilità per permettere la comparazione dei risultati tra laboratori di analisi indipendenti. L'intento dei CC è inoltre quello di rimpiazzare i precedenti criteri di sicurezza attivi in Nord America ed Europa, rimanendo comunque utilizzabili in ogni altra parte del mondo.

Il processo di valutazione è costruito in modo tale da stabilire un "livello di confidenza" tramite il quale stabilire quanto il prodotto o il sistema valutato rispetti i requisiti (di sicurezza) propri del determinato livello di "*assurance*" scelto. In questo modo il risultato della valutazione può aiutare gli utilizzatori della tecnologia IT in questione a determinare in che modo e in che misura il prodotto stesso sia sicuro, nel contesto specificato, e quali dei rischi impliciti nel suo utilizzo possano essere ritenuti tollerabili.

A tale scopo, i CC contengono un insieme comune di requisiti per le funzioni di sicurezza, mappati su dei livelli di *assurance* fissati in fase di valutazione.

Lo standard prevede sette livelli di garanzia crescenti, da EAL1 (Evaluation Assurance Level) a EAL7, dipendenti dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo. Ovviamente, più documenti a supporto della valutazione sono analizzati e analisi tecniche e test sono fatti, più si hanno prove che il processo di sviluppo sia stato orientato agli aspetti di sicurezza, in particolar modo se sono stati impiegati dei sistemi formali a dimostrazione della rigorosità dello stesso.

Tutti i livelli superiori al primo richiedono la collaborazione degli sviluppatori. Vi sono anche altri 3 livelli utilizzati esclusivamente per prodotti che integrano prodotti diversi (quelli che in precedenti versioni dei CC erano chiamati sistemi) denominati CAP (*Composed Assurance Level*) dal livello A al C, validi solo ed esclusivamente per prodotti già certificati e non sottoposti a ulteriori sviluppi per la loro integrazione. Per quanto di possibile interesse, soprattutto in Italia dove la maggior parte delle organizzazioni effettua integrazione di prodotti e più raramente lo sviluppo, questa classificazione non sembra avere avuto successo e pertanto non sarà ulteriormente analizzata.

La valutazione di un prodotto a livello EAL1 è la valutazione di un qualcosa visto come una scatola nera (*black-box*), che diventa sempre più grigio chiaro a livelli EAL2 e EAL3, per divenire una white-box dal livello EAL4 in poi.

In conclusione, per avere prodotti nei quali avere un buon livello di fiducia, questi dovrebbero essere valutati almeno a livello EAL4 (quello a partire dal quale i valutatori iniziano ad analizzare il codice) per scongiurare ad esempio la possibilità di attacchi *buffer overflow*; livelli superiori sarebbero ovviamente migliori ma, data la complessità, i costi crescono notevolmente e sono giustificati solo se opportune analisi del rischio lo suggeriscono e se il livello della minaccia è molto elevato.

[7] Vds. Cesare Gallotti, *Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001:2013*, Lulu.com, 2017, pag 415-426.

La certificazione è riferibile esclusivamente ad una specifica e determinata versione dell'Oggetto di Valutazione, impiegata solo nella configurazione valutata e nelle condizioni previste. Pertanto, l'utente deve verificare la versione acquistata e al fatto che eventuali cambiamenti, anche correttivi, dovrebbero richiedere un'ulteriore verifica.

Gli schemi di certificazione italiani sono due: uno relativo ai prodotti e sistemi correlati alla sicurezza nazionale e alle informazioni classificate, regolato dal DPCM dell'11 aprile 2002, e l'altro relativo alla sicurezza "commerciale" (richiamato anche dalle norme che regolamento la firma digitale e i dispositivi utilizzati per apporla sui documenti), regolato dal DPCM del 30 ottobre 2003.

Il primo schema è obbligatorio nel caso che con il prodotto debbano essere trattate informazioni classificate mentre non sussistono al momento obblighi per il secondo schema.

Diffusione dei *Common Criteria*

L'ISO 15408 è considerato il miglior sistema per valutare l'affidabilità di un prodotto e quindi ci si aspetterebbe un uso intensivo di questa metodologia. Purtroppo, alcuni aspetti ne limitano il ricorso. I principali sono gli alti costi della valutazione dovuti alla lunghezza del processo, difficilmente inferiore all'anno (anche se negli USA si sta cercando di ridurla a sei mesi) spesso dovuto alle difficoltà che molti produttori incontrano nel fornire gli elementi per provare la correttezza delle loro attività. Per risolvere questo e altri problemi, gli stessi *Common Criteria* sono in continua evoluzione per meglio adattarli alle esigenze degli utilizzatori. I tempi lunghi per la valutazione comportano altri problemi, per cui i prodotti certificati rischiano di essere spesso obsoleti.

L'impiego di prodotti certificati è un'attività relativamente semplice, tanto semplice che, se male utilizzata, rischia di creare essa stessa aree di vulnerabilità. Ciò accade perché non sempre i prodotti certificati sono impiegati al meglio e nella configurazione prevista. È infatti opinione comune che variare anche di poco la configurazione di un sistema certificato non rappresenti un grave errore, ma non è così. Infatti, un piccolo cambiamento della configurazione prevista invalida la certificazione.

L'onerosità della valutazione può portare un produttore a scegliere di certificare solo una parte delle funzioni di sicurezza del proprio prodotto. Un venditore disonesto, però, potrebbe utilizzare lo stesso sistema per mascherare la presenza di funzioni di sicurezza per qualche motivo "deboli", facendo valutare le sole funzioni sufficientemente robuste.

Un altro problema lo si riscontra nell'utilizzo dei *Common Criteria* in Paesi, come l'Italia, dove le organizzazioni sono normalmente specializzate nell'integrazione di prodotti commerciali (COTS, *commercial off the shelf*) e non nello sviluppo di prodotti propri. L'integratore non è solitamente in possesso di tutta la documentazione di sviluppo dei prodotti utilizzati (informazioni riservate, solitamente cedute dietro lauto pagamento a partner con elevati volumi di vendite, situazione atipica nel nostro Paese) e quindi non può valutare i prodotti se non a bassi livelli di garanzia fino, al massimo, a EAL3, e talvolta anche meno.

Questi livelli servono per garantire un adeguato livello di protezione solo nei confronti di attaccanti con capacità di attacco alquanto limitate. Questo, ovviamente, non fornisce alcuna garanzia nei confronti dei numerosi malintenzionati tecnicamente preparati e agguerriti come quelli delle ricche organizzazioni di intelligence o di certe multinazionali.

Comunque, una valutazione *Common Criteria* è solo il primo importante passo per l'utilizzo in sicurezza di un prodotto. Infatti, la valutazione viene effettuata in laboratori dove la realtà è simulata e dove tutte le predisposizioni sono pedissequamente rispettate, contrariamente a quanto avviene nei sistemi effettivamente utilizzati.

Inoltre, nella valutazione si fanno delle ipotesi di utilizzo non sempre attuate. Ecco perché, una volta installato il sistema, si devono utilizzare anche altri sistemi per ridurre al minimo le possibilità d'errore, facendo per esempio dei *penetration test* periodici per le verifiche del rispetto delle predisposizioni.

B. Catalogo delle minacce a sistemi EAD secondo la PCM-ANS/TI-002

MASCHERAMENTO
Mascheramento di un soggetto che fornisce una falsa identità ad un sistema al fine di guadagnarne l'accesso.

PROCEDURA DI ACCESSO INCONDIZIONATO
Termine per indicare un programma definito anche come "rompere il vetro in caso di emergenza" (spesso utility di sistema operativo) che aggiri (by-pass) tutte le protezioni del sistema. Programma utilizzato dai sistemisti / amministratori di rete per ripristinare un sistema in caso di guasto software o hardware e riguadagnarne l'accesso.

ATTACCO DI CAVALLO DI TROIA
"Cavallo di Troia" può essere definito un programma con funzioni apparentemente utili ma che al suo interno contiene codice indirizzato al danneggiamento, distruzione dei dati e del sistema operativo.

ATTACCO DI VIRUS INFORMATICO
Attacco ad un sistema perpetrato da un codice che si replica automaticamente unendosi ad altri programmi, ma che non può essere eseguito in maniera autonoma. Dopo essere diventato ospite all'interno di un altro programma, si installa in memoria e generalmente attacca il sistema distruggendo o modificando i dati in esso contenuti.

VERME DI RETE
Verme di rete è un programma che è in grado di essere eseguito autonomamente (a differenza dei virus) ed è in grado di propagarsi su una rete individuando automaticamente i nodi ed i servers. Generalmente non distrugge le informazioni memorizzate, bensì riduce l'efficienza del sistema rallentandolo o effettuando uno shut down.

SOTTRAZIONE DATI INOSSERVATA
Prelievo di informazioni in piccole quantità in modo inosservato anche utilizzando "cavalli di Troia".

PORTE DI ACCESSO NASCOSTE
Possibilità nascoste di accesso al cuore del sistema lasciate dai programmatori che hanno creato il software.

BOMBE LOGICHE
Porzioni di codice inserite nel sistema che, innescate da eventi particolari, effettuano azioni distruttive.

ATTACCO ASINCRONO
Metodi altamente sofisticati in grado di intercettare i colloqui tra programmi applicativi e sistema operativo in sistemi multi-tasking modificando i dati finali o in casi limite bloccando il sistema operativo stesso.

COVERT STORAGE CHANNEL
Convoglia le informazioni cambiando i dati memorizzati, modifica i nomi dei files, riempie i dischi con dati inutili in modo da obbligare il sistema ad utilizzare altre risorse per riguadagnare spazio utile.

COVERT TIMING CHANNEL
Convoglia le informazioni ad ogni esecuzione temporale di una procedura utilizzando le temporizzazioni (clock) del sistema.

INSERIRE FALSE INFORMAZIONI
Inserimento di informazioni errate all'interno di un sistema da parte di personale abilitato al suo accesso.

ERRORE ACCIDENTALE
Errore non voluto determinato da disconoscenza delle norme operative o da particolari condizioni ambientali relativamente alle sole componenti client.

INTERRUZIONE DEL SERVIZIO
Quando un soggetto domina volutamente le risorse del sistema, interrompendone o rallentandone il funzionamento.

RITRASMISSIONE PLAYBACK
Si verifica quando un soggetto registra un messaggio legittimo utilizzando mezzi hardware o software, ed in seguito lo ritrasferisce sul sistema per ottenere l'accesso.

VIOLAZIONE DELLE PROCEDURE DI LOGIN
Tramite applicazioni software disegnate ad hoc, o ripetuti tentativi, un soggetto non autorizzato penetra nel sistema.

INTERCETTAZIONE E SPIONAGCIO
Intercettazione delle emanazioni elettromagnetiche generate da cavi elettrici o monitor. Coloro che effettuano lo spionaggio spesso non sanno quando le informazioni utili possano transitare, per questo devono collezionare grandi quantità di dati e cercare successivamente le voci di interesse.

ACCODAMENTO PER ACCESSO
Accesso illegittimo ad un sistema ottenuto “accodandosi” elettronicamente o fisicamente ad un soggetto autorizzato.

CERCARE TRA I RIFIUTI
Cercare tra i rifiuti informazioni utili per guadagnare l’accesso fisico.

FURTO FISICO SUPPORTI
Furto di supporti di memorizzazione che contengono dati sensibili.

INTERFERENZE ELETTROMAGNETICHE
Interferenze a dispositivi hardware prodotte da campi elettrici o magnetici.

ALIMENTAZIONE ELETTRICA
I dispositivi di alimentazione possono subire interruzioni nel loro funzionamento, determinando perdite/modifiche dei dati elaborati.

DANNEGGIAMENTO ACCIDENTALE SUPPORTI
Danneggiamento non voluto dei supporti di memorizzazione che può portare a perdite di dati.

INCENDIO
Incendio dei locali dove è situato il sistema EAD e/o i supporti di memorizzazione.

ALLAGAMENTO
Allagamento dei locali dove è situato il sistema EAD e/o i supporti di memorizzazione.

CADUTA FULMINI
Distruzione del sistema o di parti di esso in seguito a caduta di fulmini.

SABOTAGGIO
Interruzione/modifica del funzionamento di dispositivi hardware/software che può portare a perdita di riservatezza/integrità/disponibilità dei dati.

DISTRUZIONE AREA CED
Danneggiamento grave delle attrezzature e dei dati memorizzati in seguito a esplosioni, atti di teppismo.

C. Catalogo delle vulnerabilità per sistemi EAD secondo la PCM-ANS/TI-002

CANALI DI COMUNICAZIONE NON ADEGUATAMENTE PROTETTI
Canali (che trasportano dati riservati) non sottoposti a procedure di sicurezza (dispositivi crittografici) oppure non fisicamente inaccessibili.

MODIFICHE NON CONTROLLATE AL SISTEMA OPERATIVO
Possibile inserimento non controllato da parte del personale tecnico di procedure/funzioni all'interno del sistema operativo che disabilitino o danneggino le procedure di sicurezza.

MODIFICHE NON CONTROLLATE AL SOFTWARE APPLICATIVO
Possibili modifiche delle procedure e dei programmi applicativi non documentate dai sistemisti / programmatori.

MANCATO CONTROLLO PERIODICO DELLE PROCEDURE INSTALLATE SUL SISTEMA
Operazione da attuare al fine di identificare programmi/procedure non previste dal progetto del sistema, inserite successivamente senza autorizzazione.

SFRUTTAMENTO DI "BUCHI" DEL SISTEMA OPERATIVO
Sfruttamento, a fini illeciti, di "bugs" dei sistemi operativi.

INSUFFICIENTE RILEVAMENTO DEGLI ERRORI
Errori di sistema (che potrebbero inficiare le caratteristiche di sicurezza del sistema) non valutati o sottovalutati nella loro importanza.

APPLICAZIONI SOFTWARE NON COLLAUDATE
Uso di programmi non adeguatamente testati e certificati.

INADEGUATO CONTROLLO DEGLI ACCENSI LOGICI
Il sistema EAD non prevede valide procedure di accounting degli utenti, permettendo così il furto dei dati, il loro danneggiamento e la loro modifica.

PROCEDURE DI ACCESSO INESISTENTI
Il sistema è aperto all'accesso logico di chiunque, non prevede alcun tipo di protezione.

PROCEDURE DI INPUT/OUTPUT ERRATE
Errori di sistema relativi ad operazioni di I/O che possono portare a perdite di dati.

ERRORI NEI PROGRAMMI
Malfunzionamenti delle applicazioni, non intenzionali, che possono pregiudicare la sicurezza delle informazioni.

PROCEDURE DI EMERGENZA NON COLLAUDATE
Procedure da attuare in caso di emergenza, non sufficientemente collaudate che possono portare a perdita di informazioni e di riservatezza delle stesse.

MANCANZA DI PROCEDURE DI EMERGENZA
Mancanza di procedure di sicurezza: salvataggio, distruzione informazioni, backup su supporti diversificati, chiusura dei locali contenenti il sistema EAD e/o i dati.

SUPERVISIONE NON ADEGUATA
Insufficiente controllo degli utenti e del loro accesso al sistema.

DISCONOSCENZA DELLE PROCEDURE DI SICUREZZA
Il personale addetto non è a conoscenza delle procedure di sicurezza e dei regolamenti, ed attua comportamenti che possano pregiudicare la sicurezza (es. dare la propria password ad un collega).

PERSONALE NON ADDESTRATO
Uso scorretto delle applicazioni (che trattano dati riservati) da parte del personale, non addestrato adeguatamente, con conseguente cancellazione/modifica/inserimento di dati ed informazioni sensibili.

USO SCORRETTO DELLE INFORMAZIONI RISERVATE DA PARTE DEGLI UTENTI FINALI
Divulgazione, alterazione, distruzione di informazioni a scopi illegali.

IMPROPRIA MANIPOLAZIONE DELLE MEMORIE DI MASSA
Impropria manipolazione dei supporti magnetici/ottici che contengono i dati/software del sistema, che può portare a perdita/modifica dei dati memorizzati.

CAMBIO DI CONFIGURAZIONE HARDWARE DEL SISTEMA
Modifica dei dispositivi hardware (aggiunta, modifica, eliminazione) che devono essere soggetti a periodico inventario e controllo.

MANCANZA DI SOFTWARE DEPUTATO AL CONTROLLO DELLE CONFIGURAZIONI HARDWARE
Mancanza di software che verifichi regolarmente la presenza ed il funzionamento dei dispositivi hardware costituenti il sistema.

INSUFFICIENTE SEPARAZIONE AREE LOGICHE DI LAVORO
Il sistema operativo non prevede sicuri sistemi di separazione tra le aree logiche di lavoro.

CAMBIO CONFIGURAZIONE SOFTWARE DEL SISTEMA
Modifica dei programmi e delle procedure (aggiunta, modifica, eliminazione) che devono essere soggette a periodico inventario e controllo.

APPLICAZIONI SOFTWARE NON AUTORIZZATE
Presenza sul sistema di programmi non previsti / autorizzati che possano effettuare azioni deleterie per la sicurezza (es. programmi installati dagli utenti senza autorizzazione).

MATERIALE DI SCARTO ABBANDONATO
Fogli, tabulati, supporti magnetici abbandonati che possono essere utilizzati per ottenere informazioni utili per guadagnare l'accesso ad un sistema.

INSUFFICIENTE SORVEGLIANZA DELLE INFORMAZIONI
Dati non sorvegliati, disponibili a video, su tabulato, su supporti magnetici, accessibili da parte di personale non autorizzato.

PROTEZIONE AL FUOCO INADEGUATA
Mancanza di un sistema antincendio specifico per la salvaguardia di un sistema EAD e dei dati in esso contenuti (es. casseforti ignifughe).

PROTEZIONE DAGLI ALLAGAMENTI INADEGUATA
Mancanza di un sistema antiallagamento specifico per la salvaguardia di un sistema EAD e dei dati in esso contenuti (es. paratie stagne).

PROTEZIONE DA TEMPERATURA ELEVATA INADEGUATA
Inadeguato monitoraggio della temperatura e raffreddamento degli apparati elettronici.

ALIMENTAZIONE ELETTRICA INSTABILE
Alimentazione del sistema instabile per mancanza di sistemi di controllo e sistemi UPS.

EMANAZIONI ELETTROMAGNETICHE
Apparati non appropriatamente protetti da emanazioni elettromagnetiche.

DISPOSITIVI HARDWARE NON FISICAMENTE BLOCCATI
Mancanza di dispositivi di sicurezza che impediscano l'asportazione delle periferiche (dischi rigidi, schede, nastri).

INADEGUATO CONTROLLO DEGLI ACCESSI ALL'AREA CED
Il controllo del personale e dei visitatori non è rigoroso.

MANCANZA DI CONTROLLO DEGLI ACCESSI ALL'AREA CED
Non esiste alcun controllo (personale, elettronico, fisico).

SINTEMA NON PROTETTO DAI FULMINI
Non sono previsti parafulmini e linee di terra.

SISTEMA NON PROTETTO A CARICHE ELETTROSTATICHE
Non è prevista la protezione del sistema da cariche elettriche, tramite messa a terra.

NESSUNO CONTROLLO SULLE TEMPORIZZAZIONI (CLOCK) DEL SISTEMA
Non è possibile impedire l'acceso al clock del sistema da parte di procedure non autorizzate.

MALFUNZIONAMENTO DISPOSITIVI HARDWARE
Una periferica o un dispositivo, in seguito a un malfunzionamento o guasto, compromette la sicurezza del sistema, permettendo l'accesso a soggetti non autorizzati.

SISTEMA NON PROTETTO DALLE ESPLOSIONI
L'area CED che contiene le informazioni classificate non è adeguatamente protetta dalle esplosioni.

D. Ampliamento del catalogo minacce/vulnerabilità della PCM-ANS/TI-002

Minacce:

- Furto di documenti
- Accesso non autorizzato alle aree fisiche EAD
- Alterazione dei dati
- Dati corrotti
- Attacco fisico alle funzionalità di terra
- Intercettazioni dei dati
- Jamming
- Minacce software
- Accesso non autorizzato
- Furto elettronico dei dati
- Minacce dell'ambiente Spazio
- Minacce fisiche del Segmento Spazio
- Minacce elettroniche del Segmento Spazio
- Ripudio delle azioni

Vulnerabilità:

- Errori software
- Bug hardware
- Modifiche ai dati e alla configurazione software
- Criminali e terroristi
- Impulsi elettromagnetici
- Servizi di intelligence stranieri
- Sovversivi e attivisti politici
- Hackers
- Minacce GEO Satcomm
- Micro meteoriti
- Detriti spaziali
- Radiazione cosmica
- Scarica elettrostatica
- TEMPEST
- Meccanismi di validazione degli input non implementati

- Protezione dei log non adeguata
- Eccezioni software non gestite
- Dati scambiati senza firme
- Dati scambiati senza cifratura

E. Controlli previsti dallo standard ISO 27002

Punto		Descrizione
Obiettivo:	A.05.01	**Indirizzi della direzione per la sicurezza delle informazioni** Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.
Controllo:	A.05.01.01	**Politiche per la sicurezza delle informazioni** È stato definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti un insieme di politiche per la sicurezza delle informazioni?
Controllo:	A.05.01.02	**Riesame della politica per la sicurezza delle informazioni** Sono state riesaminate ad intervalli pianificati le politiche per la sicurezza delle informazioni o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia?
Obiettivo:	A.06.01	**Organizzazione interna** Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione.
Controllo:	A.06.01.01	**Ruoli e responsabilità per la sicurezza delle informazioni** Sono state definite ed assegnate Tutte le responsabilità relative alla sicurezza delle informazioni?
Controllo:	A.06.01.02	**Separazione dei compiti** Sono state separati i compiti e le aree di responsabilità in conflitto tra loro per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione?
Controllo:	A.06.01.03	**Contatti con le autorità** Sono mantenuti appropriati contatti con le autorità pertinenti?
Controllo:	A.06.01.04	**Contatti con gruppi specialistici** Sono mantenuti appropriati contatti con gruppi specialistici o altri contesti ed associazioni professionali frequentate da specialisti della sicurezza delle informazioni?
Controllo:	A.06.01.05	**Sicurezza delle informazioni nella gestione dei progetti** La sicurezza delle informazioni è stata indirizzata nell'ambito della gestione dei progetti, a prescindere dal tipo di progetto?
Obiettivo:	A.06.02	**Dispositivi portatili e telelavoro** Obiettivo: Assicurare la sicurezza del telelavoro e nell'uso di dispositivi portatili.
Controllo:	A.06.02.01	**Politica per i dispositivi portatili** è stata adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall'uso di dispositivi portatili?
Controllo:	A.06.02.02	**Telelavoro** è stata attuata una politica e delle misure di sicurezza a suo supporto per proteggere le informazioni accedute, elaborate o memorizzate presso siti di telelavoro?

Obiettivo:	A.07.01	**Prima dell'impiego** Obiettivo: Assicurare che il personale e i collaboratori comprendano le proprie responsabilità e siano adatti a ricoprire i ruoli per i quali sono presi in considerazione.
Controllo:	A.07.01.01	**Screening** **Sono** stati svolti dei controlli per la verifica del background effettuati su tutti i candidati all'impiego in accordo con le leggi, con i regolamenti pertinenti e con l'etica e sono gli stessi proporzionati alle esigenze di business, alla classificazione delle informazioni da accedere e ai rischi percepiti?
Controllo:	A.07.01.02	**Termini e condizioni di impiego** Gli accordi contrattuali con il personale e con i collaboratori hanno specificato le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni?
Obiettivo:	A.07.02	**Durante l'impiego** Obiettivo: Assicurare che il personale e i collaboratori siano a conoscenza delle loro responsabilità per la sicurezza delle informazioni e vi adempiano.
Controllo:	A.07.02.01	**Responsabilità della direzione** La direzione ha richiesto a tutto il personale e ai collaboratori di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione?
Controllo:	A.07.02.02	**Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni** Tutto il personale dell'organizzazione e, quando pertinente, i collaboratori, hanno ricevuto un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa?
Controllo:	A.07.02.03	**Processo disciplinare** è stato istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni?
Obiettivo:	A.07.03	**Cessazione e variazione del rapporto di lavoro** Obiettivo: Tutelare gli interessi dell'organizzazione come parte del processo di variazione o di cessazione del rapporto di lavoro.
Controllo:	A.07.03.01	**Cessazione o variazione delle responsabilità durante il rapporto di lavoro** Sono stati definiti, comunicati al personale o al collaboratore e resi effettivi le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro?
Obiettivo:	A.08.01	**Responsabilità per gli asset** Obiettivo: Identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione.
Controllo:	A.08.01.01	**Inventario degli asset** Sono stati identificati tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni? è stato compilato e mantenuto aggiornato un inventario di questi asset?
Controllo:	A.08.01.02	**Responsabilità degli asset** Gli asset censiti nell'inventario hanno un responsabile?
Controllo:	A.08.01.03	**Utilizzo accettabile degli asset**

		Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni sono state identificate, documentate e attuate?
Controllo:	A.08.01.04	**Restituzione degli asset** Tutto il personale e gli utenti di parti esterne hanno restituito tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato?
Obiettivo:	A.08.02	**Classificazione delle informazioni** Obiettivo: Assicurare che le informazioni ricevano un adeguato livello di protezione in linea con la loro importanza per l'organizzazione.
Controllo:	A.08.02.01	**Classificazione delle informazioni** Le informazioni sono state classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate?
Controllo:	A.08.02.02	**Etichettatura delle informazioni** è stato sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione?
Controllo:	A.08.02.03	**Trattamento degli asset** è stato sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione?
Obiettivo:	A.08.03	**Trattamento dei supporti** Obiettivo: Prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti.
Controllo:	A.08.03.01	**Gestione dei supporti rimovibili** Sono state sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione?
Controllo:	A.08.03.02	**Dismissione dei supporti** La dismissione dei supporti non più necessari è avvenuta in modo sicuro, attraverso l'utilizzo di procedure formali?
Controllo:	A.08.03.03	**Trasporto dei supporti fisici** I supporti che contengono informazioni sono stati protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto?
Obiettivo:	A.09.01	**Requisiti di business per il controllo degli accessi** Obiettivo: Limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni.
Controllo:	A.09.01.01	**Politica di controllo degli accessi** è stata definita, documentata ed aggiornata una politica di controllo degli accessi sulla base dei requisiti di business e di sicurezza delle informazioni?
Controllo:	A.09.01.02	**Accesso alle reti e ai servizi di rete** Sono stati forniti agli utenti solo degli accesi alle reti ed ai servizi di rete per il cui uso sono stati specificatamente autorizzati?
Obiettivo:	A.09.02	**Gestione degli accessi degli utenti** Obiettivo: Assicurare l'accesso agli utenti autorizzati e prevenire accessi non autorizzati a sistemi e servizi.
Controllo:	A.09.02.01	**Registrazione e de-registrazione degli utenti** è stato attuato un processo formale di registrazione e de-registrazione per abilitare l'assegnazione dei diritti di accesso?

Controllo:	A.09.02.02	**Provisioning degli accessi degli utenti**
		è stato attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi?
Controllo:	A.09.02.03	**Gestione dei diritti di accesso privilegiato**
		Sono stati limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato?
Controllo:	A.09.02.04	**Gestione delle informazioni segrete di autenticazione degli utenti**
		è stata controllata attraverso un processo di gestione formale l'assegnazione di informazioni segrete di autenticazione deve essere controllata?
Controllo:	A.09.02.05	**Riesame dei diritti di accesso degli utenti**
		I responsabili degli asset hanno riesaminato ad intervalli regolari i diritti di accesso degli utenti?
Controllo:	A.09.02.06	**Rimozione o adattamento dei diritti di accesso**
		I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni sono stati rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione?
Obiettivo:	A.09.03	**Responsabilità dell'utente** Obiettivo: Rendere gli utenti responsabili della salvaguardia delle loro informazioni di autenticazione.
Controllo:	A.09.03.01	**Utilizzo delle informazioni segrete di autenticazione**
		Gli utenti devono essere tenuti a seguire le prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione.
Obiettivo:	A.09.04	**Controllo degli accessi ai sistemi e alle applicazioni** Obiettivo: Prevenire l'accesso non autorizzato a sistemi ed applicazioni.
Controllo:	A.09.04.01	**Limitazione dell'accesso alle informazioni**
		L'accesso a informazioni e funzioni di sistemi applicativi è stato limitato secondo le politiche di controllo degli accessi?
Controllo:	A.09.04.02	**Procedure di log-on sicure**
		è stato controllato da procedure di log-on sicure, quando richiesto dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni?
Controllo:	A.09.04.03	**Sistema di gestione delle password**
		I sistemi di gestione delle password sono interattivi e assicurano password di qualità?
Controllo:	A.09.04.04	**Uso di programmi di utilità privilegiati**
		L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema è stato limitato e strettamente controllato?
Controllo:	A.09.04.05	**Controllo degli accessi al codice sorgente dei programmi**
		Gli accessi al codice sorgente dei programmi sono stati limitati?
Obiettivo:	A.10.01	**Controlli crittografici** Obiettivo: Assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni.
Controllo:	A.10.01.01	**Politica sull'uso dei controlli crittografici**

		è stata sviluppata e attuata una politica sull'uso dei controlli crittografici per la protezione delle informazioni?
Controllo:	A.10.01.02	**Gestione delle chiavi**
		è stata sviluppata e attuata una politica sull'uso, sulla protezione e sulla durata delle chiavi crittografiche attraverso il loro intero ciclo di vita?
Obiettivo:	A.11.01	**Aree sicure** Obiettivo: Prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni dell'organizzazione e alle strutture di elaborazione delle informazioni.
Controllo:	A.11.01.01	**Perimetro di sicurezza fisica**
		Sono stati definiti ed usati dei perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni?
Controllo:	A.11.01.02	**Controlli di accesso fisico**
		Le aree di sicurezza sono protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi?
Controllo:	A.11.01.03	**Rendere sicuri uffici, locali e strutture**
		è stata progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti?
Controllo:	A.11.01.04	**Protezione contro minacce esterne ed ambientali**
		è stata progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti?
Controllo:	A.11.01.05	**Lavoro in aree sicure**
		Sono state progettate e attuate procedure per lavorare nelle aree sicure?
Controllo:	A.11.01.06	**Aree di carico e scarico**
		I punti di accesso, come le aree di carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, sono stati controllati e, se possibile, isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati?
Obiettivo:	A.11.02	**Apparecchiature** Obiettivo: Prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività operative dell'organizzazione.
Controllo:	A.11.02.01	**Disposizione delle apparecchiature e loro protezione**
		Le apparecchiature sono state disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato?
Controllo:	A.11.02.02	**Infrastrutture di supporto**
		Le apparecchiature sono state protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari?
Controllo:	A.11.02.03	**Sicurezza dei cablaggi**
		I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi sono stati protetti da intercettazioni, interferenze o danneggiamenti?
Controllo:	A.11.02.04	**Manutenzione delle apparecchiature**
		Le apparecchiature sono correttamente mantenute per assicurare la loro continua disponibilità e integrità?

Controllo:	A.11.02.05		**Trasferimento degli asset**
			Apparecchiature, informazioni o software non sono stati portati all'esterno del sito senza preventiva autorizzazione?
Controllo:	A.11.02.06		**Sicurezza delle apparecchiature e degli asset all'esterno delle sedi**
			Sono state previste misure di sicurezza per gli asset all'esterno delle sedi dell'organizzazione, considerando i diversi rischi derivanti dall'operare all'esterno dei locali dell'organizzazione stessa?
Controllo:	A.11.02.07		**Dismissione sicura o riutilizzo delle apparecchiature**
			Tutte le apparecchiature contenenti supporti di memorizzazione sono state controllate per assicurare che ogni dato critico od il software concesso in licenza sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo?
Controllo:	A.11.02.08		**Apparecchiature incustodite degli utenti**
			Gli utenti hanno assicurato che le apparecchiature incustodite siano appropriatamente protette?
Controllo:	A.11.02.09		**Politica di schermo e scrivania puliti**
			Sono state adottate sia una politica di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni?
Obiettivo:	A.12.01	**Procedure operative e responsabilità** Obiettivo: Assicurare che le attività operative delle strutture di elaborazione delle informazioni siano corrette e sicure.	
Controllo:	A.12.01.01		**Procedure operative documentate**
			Sono state documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano?
Controllo:	A.12.01.02		**Gestione dei cambiamenti**
			I cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni sono stati controllati?
Controllo:	A.12.01.03		**Gestione della capacità**
			L'uso delle risorse è stato monitorato e messo a punto? Sono state fatte proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste?
Controllo:	A.12.01.04		**Separazione degli ambienti di sviluppo, test e produzione**
			Gli ambienti di sviluppo, test e produzione sono separati per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione?
Obiettivo:	A.12.02	**Protezione dal malware** Obiettivo: Assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware.	
Controllo:	A.12.02.01		**Controlli contro il malware**
			Sono stati attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti?
Obiettivo:	A.12.03	**Backup** Obiettivo: Proteggere dalla perdita di dati.	
Controllo:	A.12.03.01		**Backup delle informazioni**

		Sono state effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata?
Obiettivo:	A.12.04	**Raccolta di log e monitoraggio** Obiettivo: Registrare eventi e generare evidenze.
Controllo:	A.12.04.01	**Raccolta di log degli eventi** La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni è stata effettuata, mantenuta e riesaminata periodicamente?
Controllo:	A.12.04.02	**Protezione delle informazioni di log** Le strutture per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati?
Controllo:	A.12.04.03	**Log di amministratori e operatori** Le attività degli amministratori e degli operatori di sistema sono sottoposte a log, e questi sono protetti e riesaminati periodicamente?
Controllo:	A.12.04.04	**Sincronizzazione degli orologi** Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza sono sincronizzati rispetto a una singola sorgente temporale di riferimento?
Obiettivo:	A.12.05	**Controllo del software di produzione** Obiettivo: Assicurare l'integrità dei sistemi di produzione.
Controllo:	A.12.05.01	**Installazione del software sui sistemi di produzione** Sono state attuate procedure per controllare l'installazione del software sui sistemi di produzione?
Obiettivo:	A.12.06	**Gestione delle vulnerabilità tecniche** Obiettivo: Prevenire lo sfruttamento di vulnerabilità tecniche.
Controllo:	A.12.06.01	**Gestione delle vulnerabilità tecniche** Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati sono ottenute in modo tempestivo, l'esposizione a tali vulnerabilità è stata valutata e appropriate misure sono state intraprese per affrontare i rischi relativi?
Controllo:	A.12.06.02	**Limitazioni all'installazione del software** Sono state stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti?
Obiettivo:	A.12.07	**Considerazioni sull'audit dei sistemi informativi** Obiettivo: Minimizzare l'impatto delle attività di audit sui sistemi di produzione.
Controllo:	A.12.07.01	**Controlli per l'audit dei sistemi informativi** I requisiti e le attività di audit che prevedono una verifica dei sistemi di produzione sono stati attentamente pianificati e concordati per minimizzare le interferenze con i processi di business?
Obiettivo:	A.13.01	**Gestione della sicurezza della rete** Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.
Controllo:	A.13.01.01	**Controlli di rete** Le reti devono sono gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni?
Controllo:	A.13.01.02	**Sicurezza dei servizi di rete**

		I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete sono stati identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno?
Controllo:	A.13.01.03	**Segregazione nelle reti** Nelle reti sono segregati gruppi di servizi, di utenti e di sistemi informativi?
Obiettivo:	A.13.02	**Trasferimento delle informazioni** Obiettivo: Mantenere la sicurezza delle informazioni trasferite sia all'interno di un'organizzazione sia con qualsiasi entità esterna.
Controllo:	A.13.02.01	**Politiche e procedure per il trasferimento delle informazioni** Esistono politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l'uso di tutte le tipologie di strutture di comunicazione?
Controllo:	A.13.02.02	**Accordi per il trasferimento delle informazioni** I trasferimenti sicuri di informazioni di business tra l'organizzazione e le parti esterne sono stati indirizzati in appositi accordi?
Controllo:	A.13.02.03	**Messaggistica elettronica** Le informazioni trasmesse attraverso messaggistica elettronica sono protette in modo appropriato?
Controllo:	A.13.02.04	**Accordi di riservatezza o di non divulgazione** I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni sono stati identificati, riesaminati periodicamente e documentati?
Obiettivo:	A.14.01	**Requisiti di sicurezza dei sistemi informativi** Obiettivo: Assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi. Questo include anche i requisiti specifici per i sistemi informativi che forniscono servizi attraverso reti pubbliche.
Controllo:	A.14.01.01	**Analisi e specifica dei requisiti per la sicurezza delle informazioni** I requisiti relativi alla sicurezza delle informazioni sono inclusi all'interno dei requisiti per i nuovi sistemi informativi o per l'aggiornamento di quelli esistenti?
Controllo:	A.14.01.02	**Sicurezza dei servizi applicativi su reti pubbliche** Le informazioni coinvolte nei servizi applicativi che transitano su reti pubbliche sono protette da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate?
Controllo:	A.14.01.03	**Protezione delle transazioni dei servizi applicativi** Le informazioni coinvolte nelle transazioni dei servizi applicativi sono 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"?
Obiettivo:	A.14.02	**Sicurezza nei processi di sviluppo e supporto** Obiettivo: Assicurare che la sicurezza delle informazioni sia progettata ed attuata all'interno del ciclo di sviluppo dei sistemi informativi.
Controllo:	A.14.02.01	**Politica per lo sviluppo sicuro** Le regole per lo sviluppo del software e dei sistemi sono state stabilite ed applicate agli sviluppi all'interno dell'organizzazione?

Controllo:	A.14.02.02	**Procedure per il controllo dei cambiamenti di sistema** I cambiamenti ai sistemi all'interno del ciclo di vita sono tenuti sotto controllo attraverso l'utilizzo di procedure formali di controllo dei cambiamenti?
Controllo:	A.14.02.03	**Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative** Quando avvengono dei cambiamenti nelle piattaforme operative, le applicazioni critiche per il business sono state riesaminate e sottoposte a test per assicurare che non ci siano impatti negativi sulle attività operative dell'organizzazione o sulla sua sicurezza?
Controllo:	A.14.02.04	**Limitazioni ai cambiamenti dei pacchetti software** La modifica dei pacchetti software è stata disincentivata e limitata ai cambiamenti necessari? Inoltre, tutti i cambiamenti sono strettamente controllati?
Controllo:	A.14.02.05	**Principi per l'ingegnerizzazione sicura dei sistemi** I principi per l'ingegnerizzazione di sistemi sicuri sono stati stabiliti, documentati, manutenuti e applicati ad ogni iniziativa di implementazione di un sistema informativo?
Controllo:	A.14.02.06	**Ambiente di sviluppo sicuro** Le organizzazioni hanno definito e protetto in modo appropriato ambienti di sviluppo sicuro per lo sviluppo dei sistemi e per le iniziative di integrazione che coprono l'intero ciclo di sviluppo dei sistemi?
Controllo:	A.14.02.07	**Sviluppo affidato all'esterno** L'organizzazione ha supervisionato e monitorato l'attività di sviluppo dei sistemi affidata all'esterno?
Controllo:	A.14.02.08	**Test di sicurezza dei sistemi** I test relativi alle funzionalità di sicurezza sono stati effettuati durante lo sviluppo?
Controllo:	A.14.02.09	**Test di accettazione dei sistemi** Sono stati stabiliti dei programmi di test e di accettazione ed i criteri ad essi relativi per i nuovi sistemi informativi, per gli aggiornamenti e per le nuove versioni?
Obiettivo:	A.14.03	**Dati di test** Obiettivo: Assicurare la protezione dei dati usati per il test.
Controllo:	A.14.03.01	**Protezione dei dati di test** I dati di test sono stati scelti con attenzione, protetti e tenuti sotto controllo?
Obiettivo:	A.15.01	**Sicurezza delle informazioni nelle relazioni con i fornitori** Obiettivo: Assicurare la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.
Controllo:	A.15.01.01	**Politica per la sicurezza delle informazioni nei rapporti con i fornitori** I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori sono stati concordati con i fornitori stessi e documentati?
Controllo:	A.15.01.02	**Indirizzare la sicurezza all'interno degli accordi con i fornitori** Tutti i requisiti relativi alla sicurezza delle informazioni sono stati stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione?

Controllo:	A.15.01.03	**Filiera di fornitura per l'ICT (Information and Comunication Technology)** Gli accordi con i fornitori includono i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT?
Obiettivo:	A.15.02	**Gestione dell'erogazione dei servizi dei fornitori** Obiettivo: Mantenere un livello concordato di sicurezza delle informazioni ed erogazione dei servizi in linea con gli accordi con i fornitori.
Controllo:	A.15.02.01	**Monitoraggio e riesame dei servizi dei fornitori** Le organizzazioni provvedono regolarmente a monitorare, riesaminare e sottoporre a audit l'erogazione dei servizi da parte dei fornitori?
Controllo:	A.15.02.02	**Gestione dei cambiamenti ai servizi dei fornitori** I cambiamenti alla fornitura dei servizi da parte dei fornitori, incluso il mantenimento e il miglioramento delle attuali politiche, procedure e controlli per la sicurezza delle informazioni, sono gestiti tenendo conto della criticità delle informazioni di business, dei sistemi e processi coinvolti e della rivalutazione dei rischi?
Obiettivo:	A.16.01	**Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti** Obiettivo: Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza.
Controllo:	A.16.01.01	**Responsabilità e procedure** Sono state stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni?
Controllo:	A.16.01.02	**Segnalazione degli eventi relativi alla sicurezza delle informazioni** Gli eventi relativi alla sicurezza delle informazioni vengono segnalati il più velocemente possibile attraverso appropriati canali gestionali?
Controllo:	A.16.01.03	**Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni** Viene richiesto a tutto il personale ed ai collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi?
Controllo:	A.16.01.04	**Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni** Gli eventi relativi alla sicurezza sono stati valutati ed è stato deciso se classificarli come incidenti relativi alla sicurezza delle informazioni?
Controllo:	A.16.01.05	**Risposta agli incidenti relativi alla sicurezza delle informazioni** Si risponde agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate?
Controllo:	A.16.01.06	**Apprendimento dagli incidenti relativi alla sicurezza delle informazioni** La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni viene utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri?

Controllo:	A.16.01.07		**Raccolta di evidenze** L'organizzazione ha definito e applicato opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze?
Obiettivo:	A.17.01	**Continuità della sicurezza delle informazioni** Obiettivo: La continuità della sicurezza delle informazioni deve essere integrata nei sistemi per la gestione della continuità operativa dell'organizzazione.	
Controllo:	A.17.01.01		**Pianificazione della continuità della sicurezza delle informazioni** L'organizzazione ha determinato i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri?
Controllo:	A.17.01.02		**Attuazione della continuità della sicurezza delle informazioni** L'organizzazione ha stabilito, documentato, attuato e mantenuto processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa?
Controllo:	A.17.01.03		**Verifica, riesame e valutazione della continuità della sicurezza delle informazioni** L'organizzazione verifica ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse?
Obiettivo:	A.17.02	**Ridondanze** Obiettivo: Assicurare la disponibilità delle strutture per l'elaborazione delle informazioni.	
Controllo:	A.17.02.01		**Disponibilità delle strutture per l'elaborazione delle informazioni** Le strutture per l'elaborazione delle informazioni sono state realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità?
Obiettivo:	A.18.01	**Conformità ai requisiti cogenti e contrattuali** Obiettivo: Evitare violazioni a obblighi cogenti o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza.	
Controllo:	A.18.01.01		**Identificazione della legislazione applicabile e dei requisiti contrattuali** Per ogni sistema informativo e per l'organizzazione in generale sono stati esplicitamente definiti, documentati e mantenuti aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all'approccio stesso dell'organizzazione per soddisfarli?
Controllo:	A.18.01.02		**Diritti di proprietà intellettuale** Sono state attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale potrebbero insistere diritti di proprietà intellettuale e per l'uso di prodotti software proprietari?
Controllo:	A.18.01.03		**Protezione delle registrazioni** Le registrazioni sono protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business?
Controllo:	A.18.01.04		**Privacy e protezione dei dati personali**

		Sono state assicurate la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile?
Controllo:	A.18.01.05	**Regolamentazione sui controlli crittografici** I controlli crittografici sono utilizzati in conformità a tutti gli accordi, la legislazione e i regolamenti pertinenti?
Obiettivo:	A.18.02	**Riesami della sicurezza delle informazioni** Obiettivo: Assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche e alle procedure dell'organizzazione.
Controllo:	A.18.02.01	**Riesame indipendente della sicurezza delle informazioni** L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione (ossia, gli obiettivi di controllo, i controlli, le politiche, i processi e le procedure per la sicurezza delle informazioni) sono stati riesaminati in modo indipendente ad intervalli pianificati oppure quando si verificano cambiamenti significativi?
Controllo:	A.18.02.02	**Conformità alle politiche e alle norme per la sicurezza** I responsabili hanno riesaminato regolarmente la conformità dei processi di elaborazione delle informazioni rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza?
Controllo:	A.18.02.03	**Verifica tecnica della conformità** I sistemi informativi vengono regolarmente riesaminati per conformità con le politiche e con le norme per la sicurezza dell'organizzazione?

F. Framework di Cyber security del NIST

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14

		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4 -1** controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12

			· **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

			• **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	• **CIS CSC** 19, 20 • **COBIT 5** DSS04.04 • **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	• **CIS CSC** 1, 5, 15, 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	• **CIS CSC** 12 • **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	• **CIS CSC** 3, 5, 12, 14, 15, 16, 18 • **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	• **CIS CSC** 9, 14, 15, 18 • **COBIT 5** DSS01.05, DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	• **CIS CSC**, 16 • **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 • **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 • **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
			· **CIS CSC** 1

		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
			· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01

		PR.IP-3: Configuration change control processes are in place	· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Protection processes are improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
			· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02

		PR.IP-12: A vulnerability management plan is developed and implemented	· **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
			· **CIS CSC** 1, 4, 6, 12, 13, 15, 16

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16 · **COBIT 5** DSS01.03, DSS03.05, DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· **COBIT 5** DSS01.04, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· **CIS CSC** 5, 7, 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8
			· **CIS CSC** 7, 8

		DE.CM-5: Unauthorized mobile code is detected	· **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· **CIS CSC** 19 · **COBIT 5** APO01.02, DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to	**RS.RP-1:** Response plan is executed during or after an incident	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5

	ensure response to detected cybersecurity incidents.		· **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4

			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.CO-1: Public relations are managed	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4

	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-2:** Reputation is repaired after an incident	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4